

ACE Management Server 管理者マニュアル

VMware ACE 2.6

このドキュメントは新しいエディションに置き換わるまで、ここで書いてある各商品と後続のすべてのバージョンをサポートします。このドキュメントの最新版をチェックするには、<http://www.vmware.com/jp/support/pubs> を参照してください。

JPN-000169-00

vmware[®]

最新情報を反映したテクニカル ドキュメントは、 ヴィエムウェア Web サイトにてご覧いただけます。

<http://www.vmware.com/jp/support/>

ヴィエムウェア Web サイトでは、最新の製品アップデート情報も提供しています。本ドキュメントに関するコメントがございましたら、次のメールアドレスまでご連絡ください。

docfeedback@vmware.com

Copyright © 2007-2009 VMware, Inc. All rights reserved. 本製品は、米国および国際的な著作権法および知的財産法によって保護されています。VMware 製品には、<http://www.vmware.com/go/patents-jp> に列記する 1 つ以上の特許が適用されます。

VMware は米国およびその他の地域における VMware, Inc の登録商標または商標です。他のすべての名称ならびに製品についての商標は、それぞれの所有者の商標または登録商標です。

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

ヴィエムウェア株式会社
〒 105-0013 東京都港区浜松町 1-30-5
浜松町スクエア 13F
www.vmware.com/jp

目次

本書について 7

1 はじめに 11

- ACE Management Server の特徴 11
- システム要件 13
 - ハードウェア要件 13
 - サポートされているオペレーティング システム 13
 - サポートされている外部データベース 14
 - サポートされているプロキシ 14
 - Web ブラウザの要件 14
 - ライセンス 14

2 ACE Management Server のデプロイの計画 15

- デプロイするコンポーネント 15
 - ホスト システムのオプション 17
 - Windows ホスト 17
 - Linux ホスト 17
 - サーバアプライアンス オプション 17
 - データベース オプション 18
 - Active Directory 認証オプション 19
- キャパシティ プランニングの実行 19
 - データベースのスループットと拡張性 20
 - LDAP のスループット 20
 - ネットワーク バンド幅とポリシー更新頻度 21
 - ACE ポリシーの構成 21
 - ロードバランサー 22
- セキュリティ機能と考慮事項 22
 - SSL 証明書と SSL プロトコルの使用 23
- 企業ファイアウォールの外からの ACE Management Server へのアクセス 24
- デプロイ計画作業シート 26

- 3 ACE Management Server のインストールと構成 29**
 - インストールの準備 29
 - ブラウザでの TLS の構成 30
 - ACE Management Server のインストールとアップグレード 31
 - Windows ホストへの ACE Management Server のインストール 31
 - Linux システムへの ACE Management Server のインストール 32
 - ACE Management Server アプライアンスのインストール 34
 - Apache サービスの起動または再起動の確認 36
 - ACE Management Server の起動と構成 37
 - ACE Management Server へのログイン 38

- 4 ACE Management Server の構成オプション 41**
 - サーバ構成の前提条件 41
 - Active Directory 統合用のユーザーおよびグループの作成 42
 - 外部データベースのセットアップ 43
 - 外部データベース用のシステム DSN エントリの作成 45
 - 許可されるデータベース接続数の拡大 46
 - Linux でのデータベース接続プールの有効化 47
 - サーバアプライアンスと外部データベースとの接続のセットアップ 48
 - カスタムセキュリティ証明書の準備 49
 - 自己署名証明書ファイルのプロパティの表示 50
 - ACE Management Server の構成の開始 50
 - ライセンス情報の表示および変更 50
 - 外部データベースの使用 51
 - アクセス コントロールの作成 52
 - カスタム SSL 証明書のアップロード 53
 - イベントのロギング 54
 - 構成設定の適用 55

- 5 複数の ACE Management Server インスタンスのロード
 バランシング 57**
 - ロードバランシングされた ACE Management Server インスタンスによる標準的な
 セットアップ 57
 - ロードバランシングに必要なサービスのインストール 59
 - すべてのサーバに対する同じ SSL 証明書の使用 59
 - サーバごとの新しい SSL 証明書および SSL キーの作成 61
 - ロードバランサーのインストールと構成 63
 - ACE インスタンスがロードバランサーを使用していることの確認 63

6	ACE インスタンスの管理	65
	サーバが管理する ACE インスタンスの表示	66
	VMware ACE Help Desk アプリケーションの使用	66
	Workstation でのインスタンス ビューの使用	67
	インスタンスの検索	68
	列の見出しによる並べ替えと列の幅の変更	69
	インスタンス ビューでの列の表示、非表示、移動	70
	インスタンス ビューでのカスタム列の作成または削除	70
	インスタンスの詳細の表示	71
	ACE インスタンスの再アクティベーション、アクティベーション解除、 または削除	72
	コピー保護 ID の変更	72
	認証パスワードのリセット	73
	カスタム列の情報の追加	74
7	トラブルシューティングとメンテナンス	75
	構成に関する問題のトラブルシューティング	75
	Linux ACE インスタンスと ACE Management Server との接続の問題	75
	ACE Management Server のポート割り当ての変更	76
	サーバ構成ファイルの削除と新しい管理者パスワードの設定	77
	SSL 証明書のバックアップ コピーのリストア	78
	複数の ACE Management Server インスタンスで SSL を使用するための構成	79
	データベースのバックアップ	80
A	データベース スキーマと監査イベント ログ データ	81
	データベース レポート作成ツールの使用	81
	データベース スキーマ	82
	監査イベント ログのデータのクエリ	87
	用語集	91
	インデックス	95

本書について

本マニュアル『VMware ACE Management Server 管理者マニュアル』では、ACE インスタンスをリアルタイムで管理する VMware ACE Management Server のインストールと使用に関する情報を提供します。ACE Management Server の使用は任意ですが、使用した場合には次のようなメリットがあります。

- ACE パッケージのアクティベーションを管理できます。
- アクティベーションされたこれらのパッケージの認証を管理できます。
- 管理対象 ACE インスタンスに対してポリシーの更新を動的に配信できます。
- Windows ゲスト OS の管理対象 ACE インスタンスに対して、インスタンスのカスタマイズ データを動的に配信できます。

改訂履歴

本マニュアルは、製品のリリースごとに、あるいは必要に応じて改訂されます。改訂版には多少の変更が加えられます。表 1 は、本マニュアルの各バージョンにおける主な変更点を示したものです。

表 1 改訂履歴

リビジョン	説明
20070105	<VMware ACE> <01> ドキュメント初版。

対象読者

本マニュアルは、ACE インスタンスを管理するために ACE Management Server をインストール、アップグレード、または使用する必要のあるすべてのユーザーを対象としています。ACE Management Server は、企業全体にデプロイした仮想マシン上で使用する ACE ポリシーの管理と更新を行うことが必要な ACE 管理者を対象としています。

本書へフィードバック

VMware では、ドキュメントの改善のためにお客様のご意見をお待ちしています。本マニュアルに関するコメントがございましたら、下記の電子メールアドレスまでフィードバックをお寄せください。

docfeedback@vmware.com

スタイル

本書では、表 2 のスタイル規則を使用しています。

表 2 本マニュアルのスタイル規則

スタイル	対象エレメント
青字 (オンラインのみ)	相互参照、Web アドレス、リンク、メールアドレスに使用
LucidaMonoEFO (等倍フォント)	コマンド、ファイル名、ディレクトリ、パスに使用
LucidaMonoEFO (等倍フォント太字)	ユーザー入力を示す場合に使用
[角カッコ]	インターフェイス オブジェクト、ボタンに使用
< 山カッコ >	キー、変数およびパラメータに使用
太字	用語集の用語、見出し語に使用
下線	強調したい箇所に使用
『二重かぎカッコ』	文献名に使用

テクニカル サポートおよびエデュケーション リソース

ここでは、お客様にご利用いただけるテクニカル サポート リソースを紹介します。本マニュアルおよびその他のマニュアルの最新版を参照するには、下記の Web サイトにアクセスしてください。

<http://www.vmware.com/jp/support/pubs>

セルフ サービス サポート

お客様が問題を自身で解決するツールとして、あるいはテクニカル情報として、以下の VMware Technology Network (VMTN) をご利用いただけます。

- **製品情報** <http://www.vmware.com/jp/products/>
- **技術情報** <http://www.vmware.com/jp/vcommunity/technology>
- **ドキュメント** <http://www.vmware.com/jp/support/pubs>
- **VMTN ナレッジベース** <http://kb.vmware.com>
- **ディスカッション フォーラム** <http://www.vmware.com/jp/community>
- **ユーザー グループ** <http://www.vmware.com/vcommunity/usergroups.html>

VMware Technology Network の詳細については、<http://www.vmtn.net> をご覧ください。

オンライン及び電話によるサポート

テクニカル サポート リクエストの提出や、製品および契約情報の確認、製品の登録は、オンラインで行うことができます。詳しくは、<http://www.vmware.com/jp/support> をご覧ください。

該当するサポート契約を結んでいるお客様の場合、迅速な対応が必要な Severity1 の問題に関しては電話でのサポートをご利用ください。詳しくは、http://www.vmware.com/support/phone_support.html をご覧ください。

サポート サービス

当社のサポート サービスがお客様のビジネス ニーズにどのように対応できるかを、<http://www.vmware.com/jp/support/services> にてご検討ください。

VMware プロフェッショナル サービス

VMware エデュケーション サービスでは、広範なハンズオン ラボを行い、ケース スタディの例を学ぶとともに、オンザジョブトレーニングのリファレンス ツールとして使用できるように作成されたコース資料を提供しています。コースは、オンサイト およびトレーニングルームで受講できます。またリアルタイムのオンライン コース もあります。オンサイトでのパイロット プログラムの実施や実装のベスト プラクティスを検討するために、VMware コンサルティング サービスでは、お使いの仮想環境の評価、計画、構築、および管理を支援するサービスを提供しています。エデュケーション サービス、認証プログラム、およびコンサルティング サービスについての情報は、下記の Web サイトを参照してください。

<http://www.vmware.com/jp/services/>

はじめに

システム管理者は VMware ACE Management Server を使用して、VMware ACE インスタンスの管理、インスタンスに対するポリシーの変更の動的な公開、パッケージのテストとデプロイを簡単に行えるようになりました。

この章では、以下のトピックについて説明します。

- [ACE Management Server の特徴](#) (P.11)
- [システム要件](#) (P.13)

ACE Management Server の特徴

ACE Management Server は拡張性と信頼性を提供します。

- 追加のサーバハードウェアやロードバランサーなどのネットワークリソースを追加することで、処理能力を拡張できます。
- テスト環境では、デフォルトの内蔵バックングストアでシンプルかつ効率的なデータベースソリューションを提供できます。本番デプロイ用に ACE Management Server を拡張する際には、外部リレーショナルデータベースマネジメントシステム (RDBMS) を構成して使用できます。
- Windows では、サーバ要求はマルチスレッドプロセスによって処理されます。Linux では、サーバ要求はマルチプロセスによって処理されます。1つのプロセスが失敗した場合は、残りのプロセスが処理を引き継ぎます。

ACE Management Server は Active Directory 統合を提供します。

- Active Directory を使用して、ACE インスタンスのユーザーを認証できます。
- 既存の Active Directory のスキーマを変更する必要はありません。

- Active Directory へのアクセスには LDAP が使用されます。
- Windows ドメイン ユーザー アカウントの状態に関する情報は、分かりやすい有用なメッセージで提供されます。ログイン失敗の理由は「ロックアウト」または「パスワードの期限切れ」として示されます。
- ACE Management Server は、Active Directory のパスワード変更プロキシとして機能します。
- ACE のインスタンスのカスタマイズ機能により、ユーザー独自の命名規則を使用してユーザーをマシンに関連付けることができます。

セキュリティ機能には以下のものがあります。

- HTTPS トラフィックを介し、サーバとクライアントとの間で暗号化通信を行います。
- パスワードは、ハッシュ化された形式でバックストアに安全に保管されます。
- 柔軟なデータベース オプションにより、ACE インスタンスのデータおよびポリシーの保管に内蔵データベースまたは外部 RDBMS を使用できます。

ACE Management Server はインストールと構成が容易です。クライアントのトラフィックは、簡単に入手できる製品を使用してプロキシを設定できます。サーバでは、簡単に入手できる以下のソフトウェア コンポーネントを使用します。

- Apache Web Server 2.0
- デフォルトの SQLite データベース ストア

サーバのセットアップでは、以下に示す業界標準のプロトコルを使用します。

- HTTPS および LDAP
- XML-RPC (メッセージのカプセル化用)

ACE Management Server は拡張性と可用性を提供します。

- 複数の ACE Management Server を作成して使用できます。複数のサーバを使用する場合は、同じデータベースを共有するようにサーバをセットアップして、ロード バランシングやフォールト トレランス性の向上を実現できます。
- Windows ACE Management Server は、Workstation と同じシステム上に配置できます。
- 単一の ACE Management Server の名前 (<https://ace.policyserver.company.com> など) を指定し、DNS ルックアップを使用してホスト名をアドレスに変換できます。DNS サーバが使用できない場合、アドレスはキャッシュされます。また、ユーザーが地理的に異なる複数のオフィス間を移動する場合は、別の ACE Management Server を使用できます。

注意 サーバ名は英語のマシン名またはIPアドレスにする必要があります。他の言語の文字はサポートされていません。

システム要件

以下のセクションでは、ACE Management Server のシステム要件について説明します。

ハードウェア要件

- 最低 800MHz の x86 互換、x86-64 アーキテクチャのプロセッサ
主な互換プロセッサ：
Celeron、Pentium II、Pentium III、Pentium 4、Pentium M (Centrino モバイルテクノロジー搭載コンピュータを含む)、Xeon (Prestonia を含む)、AMD、Athlon、Athlon MP、Athlon XP、Duron、Opteron、AMD64 Opteron、および Athlon 64
- Intel IA-32e CPU (試験的サポート)
- 基本インストールに 40MB のディスク空き容量が必要 (10GB 以上のディスク空き容量を推奨)
- 8 ビット以上のディスプレイ アダプタが必要
- LAN では、オペレーティングシステムがサポートするすべてのイーサネットコントローラをサポート

サポートされているオペレーティングシステム

以下は、ACE Management Server でサポートされているオペレーティングシステムです。

- Windows Server 2003 Web Edition SP1 および SP2、Windows Server 2003 Standard Edition SP1 および SP2、Windows Server 2003 Enterprise Edition SP1 および SP2 (64 ビットおよび R2 Edition を含む)
- Windows XP Professional (64 ビット版を含む)
- Windows 2000 Server Service Pack 4 および Windows 2000 Advanced Server Service Pack 4
- Red Hat Enterprise Linux Advanced Server 4.0、Update 4
- SUSE Linux Enterprise Server 9 Service Pack 3

サポートされている外部データベース

SQLite データベース エンジンが ACE Management Server に内蔵されています。テスト目的の場合はこのデータベースで十分ですが、本番環境では次のいずれかの外部データベースを使用してください。

- **Windows ベースのサーバの場合** Microsoft SQL Server 2000 以降、Oracle Database 10g

Microsoft SQL Server データベースを使用する場合は、ACE Management Server をホストするシステムと同じロケールを使用するシステム上で、データベースをホストする必要があります。たとえば、ACE Management Server が日本語システム上にインストールされている場合は、データベース サーバも日本語システム上にインストールし、日本語照合を使用する必要があります。

- **Linux ベースのサーバの場合** PostgreSQL 7.4 以降、Red Hat Enterprise Linux Advanced Server 4.5 以降

サポートされているプロキシ

ACE Management Server は以下の HTTPS プロキシ ソリューションを使用してデプロイできます。

- Apache Proxy `mod_proxy` を使用
- Zeus Technology Load Balancer 市販のロードバランサーおよびトラフィック管理ソリューション

Web ブラウザの要件

ブラウザベースの ACE Management Server Setup アプリケーションおよび VMware ACE Help Desk アプリケーションには、次のいずれかの Web ブラウザが必要です。

- Mozilla Firefox 1.5.2 以降
- Internet Explorer 6.0 以降

ライセンス

サーバを構成し、Server Setup Web アプリケーションにシリアル番号を入力する必要があります。シリアル番号を入力しないと、Workstation でサーバに接続することはできません。

シリアル番号は、パッケージの登録カードに記載されています。VMware ACE をオンラインで購入した場合は、シリアル番号は電子メールで送られます。Workstation と ACE インスタンスは、ライセンスの有効期限が切れていたり、該当するライセンスが存在しない場合には ACE Management Server に接続できません。

ACE Management Server の デプロイの計画

2

この章では、キャパシティ プランニングやベスト プラクティスなど、VMware ACE Management Server インスタンスをデプロイするためのガイドラインを提供します。この章では、以下のトピックについて説明します。

- [デプロイするコンポーネント](#) (P.15)
- [キャパシティ プランニングの実行](#) (P.19)
- [セキュリティ機能と考慮事項](#) (P.22)
- [企業ファイアウォールの外からの ACE Management Server へのアクセス](#) (P.24)
- [デプロイ計画作業シート](#) (P.26)

デプロイするコンポーネント

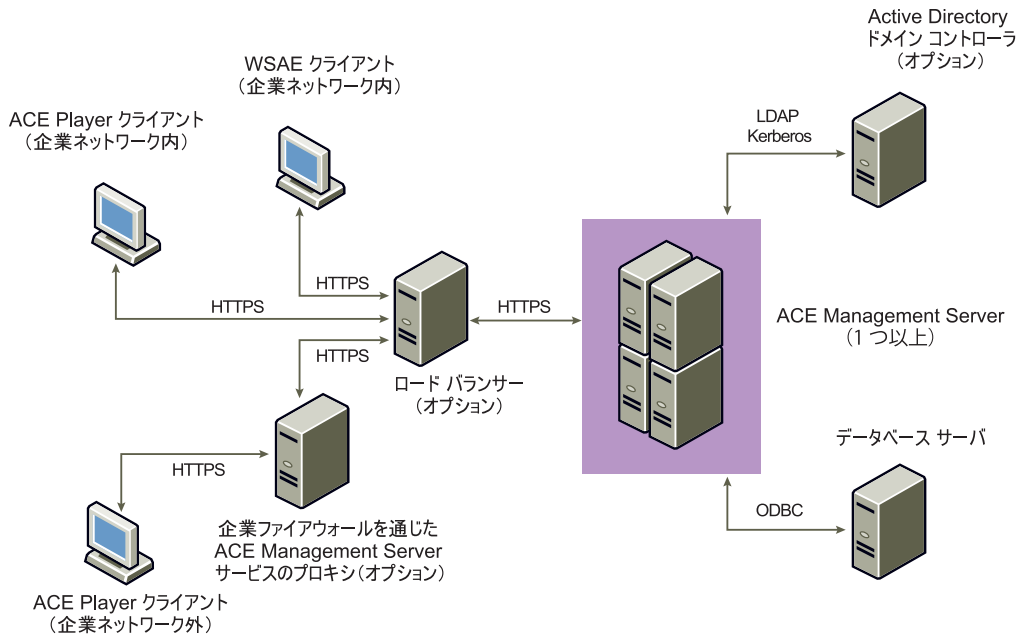
通常、ACE Management Server のデプロイでは、以下のようなコンポーネントが含まれます。

- **1 つ以上の ACE Management Server インスタンス** 同じデータベースインスタンスを使用するように複数のサーバを構成すると、管理できる ACE クライアントの数が増え、高い可用性が保証されます。
- **データベース サーバ** 本番デプロイでは、Windows ホストにインストールした Oracle Database 10g または MS-SQL for ACE Management Server、および Linux ホストにインストールした Postgres for ACE Management Server を使用することをお勧めします。
- **(オプション) Active Directory ドメイン コントローラ** ACE Management Server の Active Directory 統合を有効にするには、ACE Management Server をドメイン コントローラと通信できるように構成する必要があります。

- **(オプション) HTTP ロード バランサー** ロード バランサーを使用すると、ACE Management Server のデプロイ容量を拡張するのに役立ちます。
- **(オプション) HTTP プロキシ** クライアントが企業ファイアウォールの外から ACE Management Server にアクセスする場合は、DMZ (非武装地帯) で HTTPS プロキシを使用することをお勧めします。ACE Management Server は、Apache Proxy および Zeus Technology Load Balancer と共に使用できます。

ACE Management Server のデプロイの例については、[図 1](#) を参照してください。

図 1 ACE Management Server Deployment のデプロイ全体図



ACE Management Server には、利便性と柔軟性の高いセットアップ オプションが用意されてます。

サーバは、Windows または Linux のホストにインストールできます。テスト目的の場合は、サーバをダウンロードし、仮想アプライアンスとして実行することができます。ACE Management Server は独自のセキュリティ証明書と内蔵データベースを備えていますが、必要に応じて、外部データベースや信頼できる認定機関が発行する証明書を使用できます。また、Active Directory を使用して認証できるように ACE Management Server を構成することもできます。

ホスト システムのオプション

ACE Management Server は、Windows または Linux ホストにインストールするか、仮想アプライアンスとしてインストールすることができます。複数の ACE Management Server インスタンスを設定する場合は、すべて同じタイプにする必要があります。

Windows ホスト

Active Directory 統合を計画している場合は、ACE Management Server を Windows ホストにインストールすることをお勧めします。

Windows ACE Management Server は、Windows オペレーティングシステムにバンドルされている WinLDAP ライブラリを使用して Active Directory と統合します。当社内で実施したテスト結果では、Windows で実装した方が Linux で実装した場合よりパフォーマンスが良いことがわかっています。

Linux ホスト

ACE Management Server を Linux にインストールし、Active Directory を使用して認証を行うことができます。ただし、パフォーマンスは Windows ホストに比べて低くなります。本番環境で Linux ホストを使用する計画の場合は、ACE Management Server アプライアンスではなく Linux 用の AMS インストーラを使用してください。サポートされている Linux オペレーティングシステムが物理サーバにインストールされていない場合は、仮想マシンを作成し、サポートされている Linux オペレーティングシステムと ACE Management Server をその仮想マシンにインストールできます。

サーバアプライアンス オプション

ACE Management Server アプライアンスは、事前にインストールおよび構成されている自己完結型の ACE Management Server であり、仮想マシン内に小さな Linux オペレーティングシステムと共にパッケージされています。アプライアンスはテスト環境でのセットアップには便利で手軽ですが、本番環境での使用はお勧めしません。

デフォルトでは、このアプライアンスは DHCP を使用してネットワークの構成を試行します。DHCP を使用しない場合は、ブラウザベースの ACE Management Server Setup アプリケーションを使用して、ネットワーク設定を構成できます。また、アップデートが使用可能になった場合は、同じインターフェイスを使用してアプライアンスを更新できます。

ネットワーク設定の変更およびアプライアンスの更新の入手には、Mozilla 1.52 以降または Internet Explorer 6.0 以降の Web ブラウザが必要です。

データベース オプション

ACE Management Server は以下のデータベース オプションを備えています。

- **内蔵の SQLite データベース** デフォルト モードの ACE Management Server は、内蔵の SQLite 3 データベース エンジンを使用して動作します。SQLite データベース エンジンがサーバのインストール時に初期化され、特別な構成は不要です。この内蔵データベースでは、最大で数 GB のデータを保存できます。

SQLite データベースはファイル ベースであり、複数のプロセス間で効果的に共用できるようには設計されていません。したがって、読み取り操作のためにサードパーティ製ツールを使用してデータベースにアクセスする場合は、ACE Management Server の遅延書き込み処理のトランザクション分離機能を利用できません。

テスト目的の場合は内蔵データベースで十分ですが、本番環境では外部データベースを使用することをお勧めします。

- **サポートされている外部データベース** 本番環境では、サポートされている外部データベースを ODBC 接続を介して ACE Management Server のバッキングストアとして使用します。次の外部データベース エンジンがサポートされています。
 - Windows の場合は、Microsoft SQL Server (SQL Server 2000 または SQL Server 2005) および Oracle Database 10g
 - Linux の場合は、PostgreSQL 7.4 以降

注意 ACE Management Server が DMZ (非武装地帯) にデプロイされている場合は、ファイアウォールで保護された企業ネットワーク内にある外部データベースを使用します。

外部データベースを ACE Management Server と共に使用することには、次のような利点があります。

- オンラインバックアップができるため、データベースをバックアップする際に ACE Management Server をシャットダウンする必要がありません。
- セキュリティ モデルが強化されています。機密データへのアクセス許可を詳細に管理できます。SQLite データベース エンジンで提供されるのは、ファイルシステム ベースのセキュリティです。
- パフォーマンスを詳細にチューニングできます。
- 外部データベース管理ツールを使用できます。

- ロード バランサーを複数の ACE Management Server インスタンスと共に使用できます。バッキングストアとして外部 RDBMS を使用する必要があります。これは、SQLite データベースが、複数のプロセス間で効率的に共用できるように設計されていないためです。

Active Directory 認証オプション

Active Directory 統合には、次のような利点があります。

- ACE インスタンスを実行しているオペレーティング システムを、リモートでドメインに参加させることができます。
- 検索機能を備えているため、特定の個人またはグループを素早く検索できます。
- Active Directory のユーザーおよびグループを使用して、ACE Management Server の機能に対して役割ベースのアクセスを構成できます。

キャパシティ プランニングの実行

ACE Management Server を使用すると、ACE インスタンスと ACE ポリシーをリアルタイムで管理できます。単一の ACE Management Server で対応できるクライアントの数は、次のいくつかの要素によって異なる場合があります。

- データベースのスループットと拡張性
- LDAP のスループット (Active Directory を使用している場合)
- クライアント要求の受信に利用できるネットワーク バンド幅
- ACE ポリシーの構成
- 大規模なデプロイ (5000 クライアント超) 用のロード バランサー

表 1 は、使用しているハードウェアに応じて推奨される対応クライアント数を示しています。推奨されるクライアント数にするとサーバの処理能力に多少の余裕が出るため、インタラクティブクライアントがすぐに応答を受信できるようになり、またサーバが要求の増加に対応できるようになります。

表 1 サポートされるクライアント数

ハードウェア	推奨されるクライアント
2-GHz AMD 搭載双方向サーバ (Opteron 280、4GB RAM)	6,000
2-GHz Intel 搭載双方向デスクトップマシン (4GB RAM)	4,000

データベースのスループットと拡張性

本番デプロイでは、Oracle、MS-SQL、または Postgre をデータベース プラットフォームとして使用することをお勧めします。

ACE Management Server が必要とするストレージスペースの95パーセント以上が、イベント情報の記録に使われます。この情報は、ACE Management Server で実行されたすべてのトランザクションの監査記録です。表 2 は、対応するクライアント数に応じた推奨データベース サイズを示しています。

表の数値は、データベースのアーカイブ期間を 90 日とした場合です。この場合、データベースの記録は 90 日ごとにバックアップされ、イベント ログは 90 日間保管されます。イベント ログを 90 日ごとに消去するように ACE Management Server を構成することができます。

表 2 データベースの推奨ストレージ

クライアント数	推奨データベース サイズ
100	50MB
1,000	500MB
10,000	5,000MB

ほとんどのデータは認証イベントによって生成されます。これは、ACE Management Server への認証をユーザーが試みるたびにイベントが生成されるためです。記録されるイベント情報の数を減らすように ACE Management Server を構成することができます。「[イベントのロギング \(P.54\)](#)」を参照してください。

LDAP のスループット

ACE Management Server は、Active Directory ドメイン コントローラと通信してユーザーの認証情報を検証することができます。ドメイン コントローラ インフラストラクチャは、予想されるクライアント数をサポートするのに必要な LDAP トラフィックを処理します。

LDAP 経由での Active Directory 統合は、Windows ベースの ACE Management Server と Linux ベースの ACE Management Server とで実装方法が異なります。Windows ACE Management Server は、Windows オペレーティングシステムにバンドルされている WinLDAP ライブラリを使用します。Linux ACE Management Server は、サードパーティ製の Kerberos Library および OpenSSL を使用します。VMware が社内でも実施したテスト結果では、Windows で実装した方が Linux で実装した場合よりパフォーマンスが良いことがわかっています。

ネットワークバンド幅とポリシー更新頻度

ACE Management Server と ACE インスタンスが必要とするネットワークバンド幅の値は、構成するポリシー更新頻度によって異なります。表 3 は、10 分のポリシーの更新頻度を使用した場合に必要となるバンド幅の値を示しています。

表 3 ポリシーの更新頻度が 10 分の場合に必要なネットワークバンド幅

クライアント数	必要なバンド幅
100	0.125MB/ 秒
1,000	1.25MB/ 秒
10,000	12.5MB/ 秒

大規模なデプロイ（5000 クライアント超）の場合は、クライアントによるポリシーの更新間隔を長くすることをお勧めします。そうすれば、必要となるバンド幅の値が小さくなるためです。

表 4 は、ポリシーの更新頻度の値を 30 分に設定した場合に必要なバンド幅を示しています。

表 4 ポリシーの更新頻度が 30 分の場合に必要なネットワークバンド幅

クライアント数	必要なバンド幅
100	0.04MB/ 秒
1,000	0.4MB/ 秒
10,000	4MB/ 秒

ポリシー セットが非常に複雑な場合には、必要となるネットワークバンド幅の値も大きくなる場合があります。

ACE Management Server とデータベース サーバとの間に独立したネットワークリンクを設け、ACE Management Server とクライアント間で転送されるトラフィックがデータベースとの間のトラフィックに影響しないようにすることをお勧めします。

ACE ポリシーの構成

ACE ポリシーの構成は、パフォーマンスに影響する可能性があります。以下のいずれかの方法で、ACE Management Server と ACE Player との間で転送されるデータ量を増やすことができます。

- **ホストポリシー** ホストポリシー（ホストのネットワーク検疫など）を有効にすると、ホスト側のデーモンは ACE Management Server からホストポリシーを取得する必要があります。

- **複雑なネットワーク検疫ポリシー** ネットワーク検疫を実行するルールセットが非常に大きなサイズである場合、これらのルールを ACE Management Server からクライアントに転送すると、拡張性に影響する可能性があります。

表 3 および表 4 に示されている値は、平均的なサイズのネットワーク検疫用のルールセットに必要なバンド幅の推定値です。ACE ファイル ディレクトリを調べて `.vmp1` ファイルのサイズを計算すると、ポリシー セットのサイズを確認できます。平均的なポリシー セットは 15KB 以下です。

ロード バランサー

ACE Management Server のクライアント サーバ プロトコルは、HTTPS プロトコル上で構築されます。HTTP ロード バランシングを実行するソフトウェアやハードウェアのソリューションを使用すると、ACE Management Server のデプロイを単一サーバの容量以上の規模に（または可用性の高いデプロイが可能になるまでに）拡大することができます。

エンタープライズレベルの HTTPS ロード バランサーを使用すると、ACE Management Server は直線的に拡張されます。第 5 章「複数の ACE Management Server インスタンスのロード バランシング (P.57)」を参照してください。

セキュリティ機能と考慮事項

デフォルトでは、ACE Management Server は Secure Sockets Layer (SSL) プロトコルを使用して、暗号化された安全な通信を提供します。

セキュリティ機能の概要、およびセキュリティの問題を回避するための ACE Management Server の推奨構成方法について以下に説明します。

- **クライアントとの間で転送するトラフィックを HTTPS で保護** デフォルトでは、ACE Management Server のインストール時に自己署名証明書が作成され、HTTPS トラフィックに使用します。この証明書は安全ですが、独自の証明書とキーペアを使用するように ACE Management Server を構成することもできます。
- **ACE Management Server から Active Directory へのトラフィックを暗号化** サーバが Active Directory サービスと統合されている場合、そのサーバは SSL で保護されたリンクを介してこのサービスと通信します。LDAP トラフィックはアプリケーション層で暗号化されます。認証情報は、検証される際には Kerberos プロトコルによって保護されます。
- **機密性の高い構成オプションを暗号化** 構成ファイルに保管されるパスワードは暗号化されます。

- **データベースのセキュリティ** データベースストアには、暗号化キーなど機密性の高いデータが含まれます。データベースへの侵入を阻止し、データ損失時にデータベースを保護できるようにデータベースのセキュリティを構成してください。データの保護に利用できる機能の詳細については、データベースのマニュアルを参照してください。

SSL は、パブリック キーとプライベート キーのペアを使用してデータを暗号化します。パブリック キーは一般に公開されますが、プライベート キーはメッセージの受信者のみが把握しています。SSL 接続を要求する URL は、**https** で始まります。

ACE Management Server のインストール時に、次の 2 つのファイルが作成されます。

- **server.key** RSA 1024 ビット キーで、これはプライベート キーです。
- **server.crt** 自己署名証明書です。この署名は証明書に埋め込まれているパブリック キーによって検証されます。この公開証明書の有効期間は、サーバがインストールされた日時から 10 年間です。証明書ファイルは PEM 形式でエンコードされます。

デフォルトでは、これらのファイルは VMware ACE Management Server のプログラムディレクトリ内の、**SSL** ディレクトリに保管されます。

ACE インスタンスを実行する VMware Player は、自身が稼動するホスト マシン上に保管されているどの証明書も信頼しません。代わりに、ACE パッケージに含まれる完全な証明書チェーンを信頼します。そのため、ほとんどのセキュリティ ニーズには自己署名証明書の使用で十分に対応できます。

ただし、信頼できる認定機関が発行する証明書を使用することもできます。ACE Management Server インスタンスが複数ある場合は、すべてのインスタンスに対して 1 つの証明書を使用するか、インスタンスごとに異なる証明書を使用することができます。

SSL 証明書と SSL プロトコルの使用

ACE 有効仮想マシンは、ACE Management Server に接続すると、そのサーバのパブリック証明書と、その証明書の検証に必要な証明書チェーンをダウンロードします。サーバ証明書は複数の証明書のチェーンを有している場合があり、検証プロセスが証明書ストア内のルート証明書が信頼された証明書に到達するまで、このチェーンに従って証明書を順次検証していく必要があります。Workstation 管理者のマシン上の ACE 有効仮想マシンによってサーバへの接続が初めて行われると、Workstation のホスト システムに証明書と検証チェーンがダウンロードされます。

ACE 有効仮想マシンによるサーバへの接続時にダウンロードされた証明書のストアまたは集合は、その仮想マシンを使用して作成する各 ACE パッケージに組み込まれます。これは **ACE リソース** ディレクトリに保存されます。この ACE 有効仮想マシンから作成された ACE インスタンスをデプロイして実行する際、VMware Player アプリケーションはパッケージに含まれている証明書を使用して、ACE Management Server への接続を検証します。この検証では、ACE パッケージ内の証明書が、サーバの提供する証明書と一致するかどうかを確認します。これらの証明書が正確に一致しない場合、VMware Player はエラーメッセージを表示してインスタンスを実行しません。

VMware Player はサーバとの通信時に毎回、パッケージに含まれている証明書ストアの整合性をチェックします。VMware Player は、自身が稼動するホストマシン上に保管されているどの証明書も信頼しません。代わりに、ACE パッケージに含まれる完全な証明書チェーンを信頼します。そのため、ほとんどのセキュリティニーズには自己署名証明書の使用で十分に対応できます。

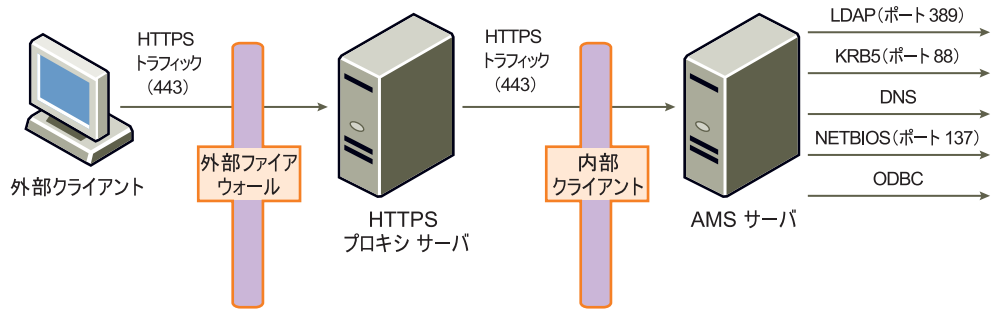
ただし、信頼できる認定機関（内部または商用サービス）により署名された証明書の使用が必要な企業などの場合には、ACE パッケージを使用するために、そのタイプのキーと証明書のペアをセットアップできます。信頼できる認定機関 (CA) とは、パブリックキー証明書（通常は無償）を発行および署名する組織を指します。

企業ファイアウォールの外からの ACE Management Server へのアクセス

ACE Management Server に対するすべてのクライアント要求は、ポート 443 の HTTPS トラフィックとなります。したがって、企業サーバへの HTTPS トラフィックのセキュリティを高めるためにプロキシを使用するソリューションは、すべて ACE Management Server トラフィックのプロキシに使用できます。

ACE Management Server がバックエンドで実行する必要があるデータ接続（LDAP、DNS、ODBC、Kerberos）の数から考えて、DMZ（非武装地帯）で HTTP プロキシを使用することをお勧めします。このプロキシは、ACE Management Server のトラフィックを企業ネットワーク内にある稼働中の ACE Management Server に中継します。

図2 外部アクセス用の推奨デプロイ



ACE Management Server は以下の HTTPS プロキシ ソリューションを使用してデプロイできます。

- Apache Proxy `mod_proxy` を使用
- Zeus Technology Load Balancer 市販のロードバランサーおよびトラフィック管理ソリューション

ACE Management Server へのトラフィックにプロキシを使用する場合、以下の問題を回避してください。

- **SSL ターミネーション** HTTPS プロキシによって SSL 接続が終了してしまった場合は、HTTPS プロキシサーバと ACE Management Server で同じ SSL キーと SSL 証明書を使用する必要があります。または、ACE Management Server 証明書チェーンを使用して、HTTPS プロキシ証明書の検証チェーンを ACE パッケージに埋め込む必要があります。

SSL 接続を終了させるプロキシサーバの一例が Apache Proxy です。また、Zeus のロードバランシング製品は SSL パススルーをサポートしているため、SSL 接続は ACE Management Server 側で終了します。

- **複数の ACE Management Server SSL 証明書** ロードバランシングソリューションの背後で複数の ACE Management Server インスタンスをデプロイする場合は、すべての ACE Management Server インスタンスで同じ SSL キーと SSL 証明書のペアを使用する必要があります。または、ACE Management Server 証明書チェーン機能を使用して、すべての SSL 証明書検証チェーンを ACE パッケージに埋め込むこともできます。
- **DNS 解決** ACE 有効仮想マシンを作成する場合は、ACE Management Server のホスト名を指定する必要があります。このホスト名は、内部クライアントと外部クライアントの両方で適切な IP アドレスに解決されるようにする必要があります。内部クライアントの場合は、ACE Management Server 自身で解決できます。外部クライアントの場合は、HTTPS プロキシサーバで解決できます。

ACE Management Server に到達するトラフィックはプレーン HTTPS トラフィックで、サーバはステータスや情報を持たないため、他の多くの構成をデプロイして ACE Management Server への外部アクセスを提供することができます。デプロイを計画する際は、ACE Management Server をセキュアなトラフィックの Web サーバとみなしてください。

デプロイ計画作業シート

このデプロイ計画作業シートを使用して、本番環境用に選択したサーバシステム、データベース、セキュリティ証明書、およびオプションのコンポーネントを記録してください。

表 2-1. 本番環境用 ACE Management Server の作業シート

コンポーネント	考慮事項	決定内容
Active Directory 統合	ACE Management Server を Windows ホストにインストールした方が、パフォーマンスは向上します。 「 Active Directory 統合用のユーザーおよびグループの作成 (P.42)」も参照してください。	Active Directory を使用しますか。 _____ 使用する場合は、Active Directory データベースに対してクエリを実行するための ACE Management Server のユーザーアカウント名 _____ LDAP サーバの完全修飾ドメイン名 _____
ACE Management Server	複数のサーバを使用する場合は、すべてのサーバを同じプラットフォーム上にインストールする必要があります。 キャパシティ プランニングについては、「 サポートされるクライアント数 (P.19)」を参照してください。	Windows と Linux のどちらのホストを使用しますか。 _____ サーバは何台ですか。 _____
データベースサーバ	データベースサーバは ACE Management Server ホストとの互換性を備えている必要があります。「 サポートされている外部データベース (P.14)」を参照してください。	MSQL、Oracle、PostgreSQL のどのデータベースですか。 _____
ロードバランサー	デプロイが大規模な場合や高可用性を実現する場合には、ロードバランサーを使用します。ロードバランサーは HTTPS をサポートする必要があり、外部データベースを必要とします。「 ロードバランサー (P.22)」を参照してください。	ロードバランサーを使用しますか。 _____

表 2-1. 本番環境用 ACE Management Server の作業シート (続き)

コンポーネント	考慮事項	決定内容
プロキシ	ACE クライアントがファイアウォールの外から ACE Management Server に接続する場合は、プロキシを使用します。「 企業ファイアウォールの外からの ACE Management Server へのアクセス (P.24) 」を参照してください。	プロキシを使用しますか。_____ Apache Proxy と Zeus Technology Load Balancer のどちらを使用しますか。 _____
SSL 証明書	複数のサーバを使用し、サーバごとに異なる SSL 証明書を使用する場合は、証明書を作成または送信する必要があります。 ACE Management Server は、SHA1 アルゴリズムを使用して署名されたパブリック キー証明書のみをサポートしています。「 SSL 証明書と SSL プロトコルの使用 (P.23) 」を参照してください。	自己署名証明書、サードパーティが署名した証明書、内部 CA(信頼できる認定機関)が発行した証明書のうち、どのタイプの証明書を使用しますか。 _____ 証明書の数はどのくらいですか。 _____
ポート	Active Directory の場合は、ポート 389 を使用します。 ACE Management Server アプライアンスの場合は、ポート 8080 を使用します。「 ACE Management Server のポート割り当ての変更 (P.76) 」および「 企業ファイアウォールの外からの ACE Management Server へのアクセス (P.24) 」を参照してください。	ポート 8000 は ACE Management Server の構成用です。 ポート 443 はクライアント要求用です。 どのポートを追加しますか。 _____

ACE Management Server の インストールと構成

3

この章では、以下のトピックについて説明します。

- [インストールの準備](#) (P.29)
- [ACE Management Server のインストールとアップグレード](#) (P.31)
- [Apache サービスの起動または再起動の確認](#) (P.36)
- [ACE Management Server の起動と構成](#) (P.37)
- [ACE Management Server へのログイン](#) (P.38)

インストールの準備

ACE Management Server をインストールする前に、デプロイの計画を立てる必要があります。次の作業を実行してください。

- 1 使用する ACE Management Server インストーラの種類、インストールするサーバの数、および搭載するデプロイ コンポーネントを決めるには、[第 2 章「ACE Management Server のデプロイの計画](#) (P.15)」を参照してください。
- 2 Transport Layer Security (TLS) を使用するよう Web ブラウザを構成するには、「[ブラウザでの TLS の構成](#) (P.30)」を参照してください。

- 3 ホスト システムの時刻をクライアント システムと同期させるには、Network Time Protocol (NTP) を使用してください。
- 4 ACE Management Server を実行するホストの HTTPS ポートを選択するには、[表 3-1](#) を参照してください。

表 3-1. ACE Management Server におけるポート割り当てのデフォルト設定

HTTPS ポート番号	説明
443	ACE Management Server と ACE インスタンスとの間の通信
8000	ACE Management Server Setup (構成) Web アプリケーション ACE Help Desk Web アプリケーション
8080	ACE Management Server Appliance 設定

注意 他の Web サーバがインストールされており、これらのデフォルト ポートのいずれかを使用する場合は、ポートの競合の解消が必要となる場合もあります。

ブラウザでの TLS の構成

ACE Management Server を操作するためには、ご使用の Web ブラウザで Transport Layer Security (TLS) が構成されている必要があります。

ブラウザで TLS を構成するには、以下の手順を実行します。

ブラウザの種類に応じて、次のいずれかの手順を実行します。

- Internet Explorer ブラウザの場合
 - a [ツール]-[インターネット オプション]-[詳細設定] を選択して、[セキュリティ] までスクロールします。
 - b [TLS 1.0 を使用する] チェック ボックスを選択して [OK] をクリックします。
- Mozilla ブラウザの場合
 - a [ツール]-[オプション]-[詳細] を選択します。
 - b [TLS 1.0 を使用する] チェック ボックスを選択して [OK] をクリックします。

ACE Management Server のインストールとアップグレード

ACE Management Server インスタンスを1つ以上インストールし、企業内でACE インスタンスを提供することができます。ACE Management Server インスタンスを複数セットアップする場合は、すべてのインスタンスをWindows ホストとLinux ホストのどちらかにインストールするか、またはアプライアンスとしてインストールする必要があります。

ACE Management Server を2.0から2.5にアップグレードするには、初めてサーバにインストールしたときと同じ手順を使用します。インストーラは、以前のバージョンを検出すると、その旧バージョンをアンインストールしてから新バージョンをインストールします。構成設定は保持されます。

本番デプロイでは、パフォーマンスと安定性を保証するために、使用できるリソースが十分にある専用サーバまたは仮想プラットフォームのどちらかにACE Management Server をインストールすることをお勧めします。システム要件は、ほぼ例外なく、サポートされるACE インスタンスの数と、それらのインスタンスに構成されるサーバとの通信頻度によって決まります。VMware パフォーマンス テストの詳細については、「[キャパシティ プランニングの実行](#) (P.19)」を参照してください。

ただし、クライアント数が少ない場合や非本番環境での評価のサポートについては、デスクトップまたはワークステーション プラットフォーム上でのACE Management Server のテストが行われており、これらのプラットフォームにインストールしても差し支えありません。

Windows ホストへのACE Management Server のインストール

ACE Management Server をWindows ホストにインストールするには、インストールウィザードをダウンロードして実行します。ACE Management Server は次のWindows システムにインストールできます。

- Windows Server 2003
- Windows XP Professional (64ビット版を含む)
- Windows 2000 Server

インストールを開始する前に、「[インストールの準備](#) (P.29)」の説明に従って、時刻が同期され、必要なポートが利用可能になっていることを確認してください。

以下のインストール手順を使用して、ACE Management Server ソフトウェアのインストールまたはアップグレードを行います。

Windows ホストに ACE Management Server をインストールするには、以下の手順を実行します。

- 1 **VMware-ACE-Management-Server.exe** ファイルを当社の Web サイトからダウンロードし、サーバをホストするシステム上にそのファイルを保存します。
このファイルは、Workstation アプリケーションと同じダウンロード場所から、個別のファイルとしてダウンロードして入手できます。
- 2 **VMware-ACE-Management-Server.exe** ファイルをダブルクリックして、インストール ウィザードを開始します。
- 3 インストール ウィザードの指示に従って操作します。
- 4 ファイアウォールが有効に設定されているコンピュータを使用しており、インストールの終了時に、Apache サービスのブロックを解除するかどうかを確認するメッセージが表示された場合は、[ブロックしない]を選択します。
Apache サービスのブロックを解除しないと、ACE Management Server は正しく動作しません。

ACE Management Server をインストールしたら、構成を実行できます。「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。

Linux システムへの ACE Management Server のインストール

ACE Management Server は次の Linux システムにインストールできます。

- Red Hat Enterprise Linux 4
- SUSE Linux Enterprise Server 9 SP3

開始する前に、システムが次の要件を満たしていることを確認してください。

- システムに Apache 2.0 がインストールされて稼働していること (Web サーバの RPM は、Red Hat Enterprise Linux 4 または SUSE Linux Enterprise Server 9 のインストールに付属しています)。
- Apache Web サービスが正常に稼働しており、SSL HTTP 要求を受信していること。
- システム上で **mod_ldap** モジュールおよび **mod_ssl** モジュールが使用可能になっていること。
- Red Hat Enterprise Linux 4 または SUSE Linux Enterprise Server 9 システムに、**curl**、**openldap**、**openssl**、**apache**、および **gdbm** の各パッケージがインストールされていること。

- SUSE Linux Enterprise Server 9 の場合は、**cyrus-sasl-gssapi** パッケージがインストールされていること。このパッケージはデフォルトではインストールされません。
- 外部データベース オプションを使用する場合は、以下のパッケージも必要となります。
 - Red Hat Enterprise Linux 4 **unixODBC**
 - SUSE Linux Enterprise Server 9 **unixODBC**、X11 グラフィカル構成ツールを使用する場合は、このほかに **unixODBC-gui-qt**
- 「[インストールの準備](#) (P.29)」の説明に従って、時刻が同期され、必要なポートが利用可能になっていること。

以下のインストール手順を使用して、ACE Management Server ソフトウェアのインストールまたはアップグレードを行います。

Linux システムに ACE Management Server をインストールするには、以下の手順を実行します。

- 1 **.rpm** ファイルを当社の Web サイトからダウンロードし、サーバをホストするシステム上にそのファイルを保存します。

このファイルは、Workstation アプリケーションと同じダウンロード場所から、個別のファイルとしてダウンロードして入手できます。

- 2 ACE Management Server 用の Red Hat または SUSE Linux の RPM インストーラを実行します。

- **vmware-ace-management-server-<ビルド番号>.i386-rhel4.rpm**

- **vmware-ace-management-server-<ビルド番号>.i386-sles9.rpm**

例:

```
rpm -Uhv vmware-ace-management-server-87693.i386-rhel4.rpm
```

- 3 SUSE Linux Enterprise Server 9 サーバの場合は、LDAP モジュール (**mod_ldap**) がロード用に構成されていることを確認します。

- a テキスト エディタを使って、以下のファイルを開きます。

```
/etc/sysconfig/apache2
```

- b **APACHE_MODULES** 変数に **ldap** 構成オプションを追加します。

- c ファイルを保存し、閉じます。

ACE Management Server をインストールしたら、構成を実行できます。「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。

ACE Management Server アプライアンスのインストール

ACE Management Server アプライアンスは、事前にインストールおよび構成されている自己完結型の ACE Management Server であり、仮想マシン内に小さなオペレーティングシステムと共にパッケージされています。アプライアンスはテスト目的には十分ですが、本番環境では使用しないことをお勧めします。

インストールを開始する前に、「[インストールの準備](#) (P.29)」の説明に従って、時刻が同期され、必要なポートが利用可能になっていることを確認してください。

ACE Management Server アプライアンスをインストールするには、以下の手順を実行します。

- 1 アプライアンスの **.zip** ファイルを当社の Web サイトからダウンロードし、サーバをホストするシステム上にそのファイルを保存します。
- 2 サーバの格納場所にするディレクトリにこのファイルを解凍します。
- 3 Workstation を起動し、[ファイル]-[開く]を選択して開き、**ams_appliance.vmx** ファイルを選択します。
- 4 [パワーオン] ボタンをクリックして、仮想アプライアンスを起動します。
- 5 パスワードのプロンプトで、パスワードを入力して確認します。

ここで設定するパスワードは、root アカウントと network アカウントの両方に使用されます。後でコンソールや Web からアプライアンスの管理操作を実行できるように、このパスワードをメモしておきます。

アプライアンスは、DHCP を使用して自身のネットワークを構成します。

コンソールビューに以下の情報が表示されます。

- 現在のネットワーク設定
- リモートでアプライアンスを管理し、ACE Management Server 自体を構成するための URL

ログイン プロンプトで <Return> キーを押すと、情報が再び表示されます。

- 6 タイムゾーンのプロンプトで、現在の設定を受け入れるか、必要に応じて変更を加えます。

- 7 (オプション) 静的 IP アドレスを使用するようサーバを構成する場合や、プロキシサーバを指定する場合は、アプライアンスの管理と構成アプリケーションを使用して、以下の手順を実行します。
 - a ACE Management Server アプライアンスを稼働させておきます。
 - b **https://<ホスト IP アドレス>:8080** を参照します。
 - c 接続のダイアログ ボックスで、ユーザー名のフィールドに **root** と入力し、パスワードのフィールドに network または root のパスワードを入力します。
 - d ブラウザベースの ACE Management Server Setup アプリケーションの先頭ページで、[ネットワーク] リンクをクリックします。
 - e ネットワーク設定の構成方法を表示するには、Web ページの右上隅にある [ヘルプ] リンクをクリックします。
 - f ネットワーク設定を変更したら、[適用] をクリックします。

- 8 (オプション) 更新の自動ダウンロードを無効にするなど、更新オプションを再構成する場合は、アプライアンスの管理と構成アプリケーションを使用して、以下の手順を実行します。
 - a ACE Management Server アプライアンスを稼働させておきます。
 - b **https://<ホスト IP アドレス>:8080** を参照します。
 - c 接続のダイアログ ボックスで、ユーザー名のフィールドに **root** と入力し、パスワードのフィールドに network または root のパスワードを入力します。
 - d アプライアンスの構成と管理 Web アプリケーションの最初のページで [アップデート] リンクをクリックし、[アプライアンスのアップデート] ページを完成させます。
 - e 更新オプションの構成方法を表示するには、Web ページの右上隅にある [ヘルプ] リンクをクリックします。

- 9 ネットワーク設定または更新設定の構成が完了したら、ACE Management Server Setup Web アプリケーションに移動して、サーバを構成します。

このアプリケーションにアクセスするには、以下のいずれかの方法を使用します。

 - アプライアンスの管理と構成 Web アプリケーションのページで、右上隅にある [ACE にログイン] リンクをクリックします。
 - コマンド プロンプト ウィンドウを閉じてブラウザを開き、ACE Management Server Setup Web アプリケーションの URL を入力します。
https://<ホスト IP アドレス>:8000/

10 [構成] をクリックして Web アプリケーションを開きます。

Apache サービスの起動または再起動の確認

ACE Management Server を Linux ホストにインストールした場合は、Apache サービスが起動していることを確認してからログインを試みます。

また、トラブルシューティングのために、ACE Management Server が使用している Apache サービスを手動で再起動することが必要になる場合もあります。

Apache サービスが起動または再起動されたことを確認するには、以下の手順を実行します。

次のいずれかを実行してください。

- Windows ホストの場合
 - a タスクバーの [Apache] アイコンをクリックします。
 - b 表示されたメニューで [Apache2] を選択します。
 - c 該当するコマンドを以下から選択します。
 - 停止されているサービスを起動するには、[Start] をクリックします。
サービスがすでに起動している場合には、このコマンドは使用できません。
 - 再起動するには、[Stop] をクリックし、次に [Start] をクリックします。
[Restart] ではなく、[Stop] と [Start] をクリックしてください。
- SUSE Linux Enterprise Server 9 ホスト、または ACE Management Server アプリケーションを含む仮想マシンの場合
 - a ホスト上または仮想マシン内でターミナル ウィンドウを開きます。
 - b **root** として次のコマンドを入力します。
/etc/init.d/apache2 status
ステータスが **started** なら、ACE Management Server にログインできません。「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。
 - c 該当するコマンドを以下から選んで入力します。
 - 停止されているサービスを起動するには、以下のコマンドを入力します。
/etc/init.d/apache2 start

- サービスを再起動するには、以下のコマンドを入力します。

```
/etc/init.d/apache2 stop  
/etc/init.d/apache2 start
```

- Red Hat Enterprise Linux 4 の場合

- ホスト上または仮想マシン内でターミナル ウィンドウを開きます。
- root** として次のコマンドを入力します。

```
/etc/init.d/httpd status
```

ステータスが **started** なら、ACE Management Server にログインできます。「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。

- 該当するコマンドを以下から選んで入力します。

- 停止されているサービスを起動するには、以下のコマンドを入力します。

```
/etc/init.d/httpd start
```

- サービスを再起動するには、以下のコマンドを入力します。

```
/etc/init.d/httpd stop  
/etc/init.d/httpd start
```

ACE Management Server の起動と構成

開始前に、以下の前提条件が満たされていることを必要に応じて確認してください。

- ACE Management Server を Linux ホストにインストールした場合、または ACE Management Server アプライアンスを使用している場合は、Apache サーバが稼動していることを確認してください。「[Apache サービスの起動または再起動の確認](#) (P.36)」を参照してください。
- 今回が初めてのログインである場合は、製品のシリアル番号があることを確認してください。シリアル番号は、パッケージの登録カードに記載されています。VMware ACE をオンラインで購入した場合は、シリアル番号は電子メールで送られます。
- 外部データベース、Active Directory 統合、またはカスタム SSL 証明書を使用する場合は、ACE Management Server を構成する前にいくつかのセットアップ作業を行う必要があります。必要に応じて、以下のトピックを参照してください。
 - [Active Directory 統合用のユーザーおよびグループの作成](#) (P.42)
 - [外部データベースのセットアップ](#) (P.43)
 - [カスタム セキュリティ証明書の準備](#) (P.49)

ACE Management Server を起動して構成するには、以下の手順を実行します。

- 1 Web ブラウザを開いて、<https://<ホスト名>:8000> にアクセスします。
 <ホスト名> には、ACE Management Server がインストールされているコンピュータの完全修飾名か、IP アドレスを値として使用できます。
 ACE Management Server が Windows ホストにインストールされており、そのホストを使用して構成を行う場合は、[スタート]-[VMware]-[VMware ACE Management Server] を選択することもできます。
- 2 使用許諾契約書に同意して、[開始] をクリックします。
 構成用のタブが表示されます。これらのタブはログインするたびに表示されますが、初めてログインした場合には、[次へ] や [前へ] などのウィザード ボタンも表示されます。
- 3 各タブで情報を入力して、[次へ] をクリックします。
 デフォルト設定値がなく、変更の必要があるフィールドは、[ライセンス] タブの [シリアル番号] フィールドと [アクセスコントロール] タブの [管理者] パスワードだけです。
 特定のフィールドとタブの詳細については、そのタブで [ヘルプ] をクリックしてください。

ACE Management Server へのログイン

ACE Management Server に初めてログインしたときには、パスワードを設定する必要があります。次にログインしたときには、そのパスワードを入力する必要があります。ただし、Active Directory を使用して認証を行うようにサーバを構成している場合は、Active Directory の認証情報を入力する必要があります。

Workstation と ACE Management Server との間の通信は、セキュアな SSL 接続を介して行われます。

サーバが Active Directory サービスに統合されている場合は、管理者の認証情報を、[表 3-2](#) に示されているいずれかの形式で入力します。

表 3-2. Active Directory サービス使用時のログイン オプション

オプション	説明	例
長い名前 + パスワード + ドメイン名	長い名前とは、<First_name> <Last_name> という形式を指します。	John Doe
長い名前 + パスワード	長い名前とは、<First_name> <Last_name> という形式を指します。 [ドメイン] フィールドは空白のままとします。	John Doe

表 3-2. Active Directory サービス使用時のログイン オプション (続き)

オプション	説明	例
短い名前 + パスワード + ドメイン	短い名前とは、sAMAccountName を指します。	ace (長い名前 ACE User の短縮形)
短い名前 + パスワード	短い名前とは、sAMAccountName を指します。 [ドメイン] フィールドは空白のままとします。	ace (長い名前 ACE User の短縮形)
電子メール アドレス + パスワード	このログイン オプションは、直接接続を介してアクセスするドメインにのみ使用できます。 [ドメイン] フィールドは空白のままとします。	user1@acme.com
NETBIOS DOMAIN NAME ユーザー名 + パスワード	NetBIOS 名は、NetBIOS ネーム サービス (WINS) に登録されているドメインの短縮名です。 [ドメイン] フィールドは空白のままとします。	
ユーザー名 + パスワード +NETBIOS DOMAIN NAME	NetBIOS 名は、NetBIOS ネーム サービス (WINS) に登録されているドメインの短縮名です。	

ACE Management Servers にログインするには、以下の手順を実行します。

- 1 Web ブラウザを開いて、**https://< ホスト名 >:8000** にアクセスします。

< ホスト名 > には、ACE Management Server がインストールされているコンピュータの完全修飾名か、IP アドレスを値として使用できます。

ACE Management Server が Windows ホストにインストールされており、そのホストを使用して構成を行う場合は、[スタート]-[VMware]-[VMware ACE Management Server] を選択することもできます。

- 2 次のいずれかを実行してください。
 - ACE Management Server を構成するには、[構成] をクリックします。
 - このサーバが管理する ACE インスタンスを表示して作業を行うには、[Help Desk] をクリックします。
- 3 ログイン認証情報を入力します。

Active Directory を認証に使用している場合は、表 3-2 を参照してください。マルチドメイン環境では、ドメイン (**eng.com** など) の入力が必要になる場合があります。

ACE Management Server の 構成オプション

4

ACE Management Server をインストールした後、ブラウザベースの ACE Management Server Setup アプリケーションを使用してサーバを構成する必要があります。

この章では、以下のトピックについて説明します。

- [サーバ構成の前提条件](#) (P.41)
- [ACE Management Server の構成の開始](#) (P.50)
- [ライセンス情報の表示および変更](#) (P.50)
- [外部データベースの使用](#) (P.51)
- [アクセスコントロールの作成](#) (P.52)
- [カスタム SSL 証明書のアップロード](#) (P.53)
- [イベントのロギング](#) (P.54)
- [構成設定の適用](#) (P.55)

サーバ構成の前提条件

(LDAP による) Active Directory 統合、外部データベース、またはカスタム SSL 証明書を使用する場合は、ACE Management Server を構成する前にいくつかのセットアップ作業を行う必要があります。

Active Directory 統合用のユーザーおよびグループの作成

Active Directory を使用してユーザー認証を行うには、管理するユーザーを Active Directory グループに追加し、かつクエリ ユーザーを作成する必要があります。クエリ ユーザーは ACE Management Server が LDAP に対してクエリを実行するためのユーザーです。

LDAP を使用するために ACE Management Server を構成する場合は、パフォーマンスに悪影響が及ばないようにするため、以下のガイドラインに従ってください。

- デフォルトのドメインは、LDAP ホストがドメイン コントローラとなっているドメインです。
- クエリ ユーザーはデフォルトのドメイン内のユーザーです。
- 管理ユーザー グループはデフォルトのドメイン内に存在するグループです。

LDAP 経由での Active Directory 統合は、Windows ベースの ACE Management Server と Linux ベースの ACE Management Server とで実装が異なります。Windows と Linux では、Active Directory への接続に使用するライブラリとサポートする外部データベースが異なります。Windows ACE Management Server は、Windows オペレーティングシステムにバンドルされている WinLDAP ライブラリを使用します。Linux ACE Management Server は、サードパーティ製の Kerberos Library および OpenSSL を使用します。VMware が社内でも実施したテスト結果では、Windows で実装した方が Linux で実装した場合よりパフォーマンスが良いことがわかっています。

Active Directory 統合用のユーザーとグループを作成するには、以下の手順を実行します。

- 1 ACE Management Server で LDAP サーバへの接続および照会（クエリ）を行う際に使用するユーザーを作成します。
そのユーザーの `sAMAccountName` の値（`aceuser` など）をメモしておきます。
- 2 ドメインに ACE 管理者グループを作成します。
- 3 ACE 管理者ユーザーを ACE 管理者グループに追加します。
- 4 （オプション） Help Desk グループを作成して、Help Desk ロールを担当するユーザーをそのグループに追加します。

Help Desk Web アプリケーションには、管理者の LDAP 認証情報またはパスワードを使用してログインできます。Help Desk ロールを作成すると、特定のユーザーに対して Help Desk アプリケーションからの Help Desk タスクの実行を許可しつつ、他の管理ツールへのアクセスは許可しないようにすることができます。

外部データベースのセットアップ

開始する前に、以下のいずれかのサポートされているデータベース サーバを持っていることを確認してください。

- **Windows ベースのサーバの場合** Microsoft SQL Server 2000 以降、Oracle Database 10g。

Microsoft SQL Server データベースを使用する場合は、ACE Management Server をホストするシステムと同じロケールを使用するシステム上で、データベースをホストする必要があります。たとえば、ACE Management Server が日本語システム上にインストールされている場合は、データベース サーバも日本語システム上にインストールし、日本語照合を使用する必要があります。

- **Linux ベースのサーバの場合** PostgreSQL 7.4 以降、Red Hat Enterprise Linux Advanced Server 4.5 以降。

データベースを Linux ホストにインストールする前に、**unixODBC** RPM パッケージがその Linux システムにインストールされていることを確認してください。そのパッケージを、ご使用の Linux ディストリビューション向けにリリースされた最新バージョンに更新することをお勧めします。**unixODBC** パッケージは、Linux システム上で稼働するプログラムに ODBC API を提供します（Windows の ODBC API に類似しています）。

このパッケージには、他のプログラムに ODBC Driver Manager API を提供する **libodbc** 共有ライブラリ、構成ユーティリティのセット、および良く知られているデータベース用の ODBC ドライバが含まれています。Red Hat Enterprise Linux と SUSE Linux Enterprise Server 9 のいずれの場合も、PostgreSQL 用の ODBC ドライバが **unixODBC** バイナリ ディストリビューションパッケージに含まれています。

また、**unixODBC-gui-qt** パッケージがインストールされていることを確認してください（このユーティリティは Red Hat Enterprise Linux **unixODBC** パッケージに含まれています）。このパッケージは、データソース名（DSN）の作成に **ODBCConfig** X11 グラフィカル構成ツールを使用するために必要です。

外部データベースをセットアップするには、以下の手順を実行します。

- 1 データベース サーバをホストにインストールします。

外部データベースは ACE Management Server と同じサーバ上にインストールする必要はありませんが、同じプラットフォーム上にインストールする必要があります。たとえば、ACE Management Server が Windows ホスト上にインストールされている場合は、データベース サーバも Windows ホスト上にインストールする必要があります。

適切なアクセス権が付与されている場合、ACE Management Server はデータベース スキーマを自動的に作成します。

- 2 データベースを構成します。

専用のデータベースと、このデータベースに対するフルアクセス権（テーブルの作成権限を含む）を持つユーザー アカウントを持っていることを確認します。このデータベースのユーザーに対して不要な権限を与えないでください。たとえば、RDBMS が管理している他のデータベースに対する読み取り権限または書き込み権限などを与えないようにします。

データベース内のテーブルにはすべて、**PolicyDb_** という接頭部で始まる名前と、**PdbIns_** または **PdbLf_** という接頭部のインデックスが付けられています。データベースの数が限られている場合には、ACE Management Server にデータベースへの DSN を提供することで、データベースを他のアプリケーションと共有させることができます。

- 3 （オプション）ACE Management Server がネットワーク経由（TCP ソケット接続）でデータベースに接続する場合は、以下の設定が行われていることを確認してください。

- TCP 接続がデータベース構成オプションで有効に設定されていること。
- データベース サーバまたは ACE Management Server ホスト上で、TCP 接続がファイアウォールの設定によってブロックされていないこと。
- PostgreSQL データベースを使用する場合は、ネットワーク経由でデータベースに接続する許可がユーザーごとに構成されていること。この許可は、ご使用のデータベースのルート フォルダに格納されている **pg_hba.conf** ファイルで構成します。

- 4 （オプション）ACE Management Server のマシン上で、構成されたユーザー認証情報によるサーバから構成済みデータベースへの接続を検証するために、コマンドラインまたはグラフィカル SQL ツールを実行します。

たとえば、SQL Server の場合は **sqlcmd.exe**、Oracle の場合は **sqlplus.exe**、Postgres の場合は **psql** といったツールを使用できます。データベースの構成および検証方法については、各データベースのマニュアルを参照してください。

5 ACE Management Server のマシンで、システム DSN エントリを作成します。

外部データベース用のシステム DSN エントリの作成

DSN の構成に必要な情報は、DSN 名、サーバの IP アドレスまたはホスト名、およびデータベース名です。DSN の構成では、ユーザー名やパスワードを指定する必要はありません。ユーザー名とパスワードは、後で ACE Management Server Setup アプリケーションを使用する際に指定します。

ユーザー DSN ではなく、必ずシステム DSN を作成してください。ユーザー DSN を作成した場合、作成者自身のユーザー アカウントにしか認識されません。ACE Management Server はローカル システム アカウントで実行されるため、サーバはユーザー DSN を検出または使用することができません。

Windows データベース用のシステム DSN エントリの作成

ホストが 32 ビットと 64 ビットのどちらの場合でも、32 ビットシステム用の DSN エントリを作成します。

開始する前に ODBC ドライバが正しいことを確認するには、ご使用のオペレーティングシステムとデータベースのマニュアルを参照してください。

Windows データベース用のシステム DSN エントリを作成するには、以下の手順を実行します。

- 1 次のいずれかを実行してください。
 - 32 ビット ホストの場合は、[コントロールパネル]-[管理ツール]-[データ ソース (ODBC)] を選択して、ODBC データ ソース プラグインを使用します。
 - 64 ビット ホストの場合は、%WINDIR%\syswow64\odbcad32.exe に移動し、そのプログラムを使用して 32 ビット サブシステム用のシステム DSN エントリを作成します。

ACE Management Server は、Windows 64 ビット システム上での SQL Native Client ドライバを使用する ODBC をサポートしていません。

- 2 DSN 名、サーバの IP アドレスまたはホスト名、およびデータベース名を含むエントリを作成します。
- 3 (オプション) DSN セットアップ ウィザードで接続をテストするオプションが表示された場合は、データベース ユーザーの認証情報で正しく接続できることを確認してください。
- 4 データベース DSN、ユーザー名、およびパスワードをメモしておきます。

これで、ブラウザベースの ACE Management Server Setup アプリケーションを使用してこのデータベースに接続できるようになりました。

Linux データベース用のシステム DSN エントリの作成

Linux システムでは、テキスト エディタまたは **ODBCConfig** グラフィカル (X11) ユーティリティを使用してシステム DSN エントリを作成します。**ODBCConfig** ユーティリティは、Windows の ODBC データ ソース コントロール パネル プラグインに類似しています。

開始する前に、ODBC ドライバが正しいことを確認します。

- Red Hat Enterprise Server の場合は、ドライバは `/usr/lib/libodbcpsql.so` にあります。
- SUSE Linux Enterprise Server 9 の場合は、ドライバは `/usr/lib/unixODBC/libodbcpsql.so.2` にあります。**unixODBC** パッケージの DSN 構成は、`/etc` ディレクトリ (SUSE Linux Enterprise Server の場合は `/etc/unixODBC`) に保管されます。

ACE Management Server アプライアンスを使用している場合は、「[サーバアプライアンスと外部データベースとの接続のセットアップ](#) (P48)」を参照してください。

DSN の作成には `odbc.ini` ファイルを、ドライバおよび一般的な ODBC システムの構成には `odbcinst.ini` ファイルを使用します。

Linux データベース用のシステム DSN エントリを作成するには、以下の手順を実行します。

- 1 root として **ODBCConfig** ユーティリティを使用して、システム DSN エントリを作成します。

また、サーバアドレスおよびデータベース名も DSN 設定に構成する必要があります。

unixODBC の使用については、[unixODBC Project の Web ページ](#)を参照してください。

ODBCConfig ユーティリティは、`odbc.ini` ファイルと `odbcinst.ini` ファイルに変更を加えます。

- 2 データベース DSN、ユーザー名、およびパスワードをメモしておきます。

これで、ブラウザベースの ACE Management Server Setup アプリケーションを使用してこのデータベースに接続できるようになりました。

許可されるデータベース接続数の拡大

サーバのパフォーマンスを最適化するために、ACE Management Server では、クライアントからの受信接続を待機する、複数の並列スレッド (Windows の場合) またはプロセス (Linux の場合) を開始します。通常、各クライアント接続はデータベース トランザクションを実行するため、データベース接続を開く必要があります。

ACE Management Server は、クライアント接続のために、自身が実行する並列スレッドまたは並列プロセスと同じ数のデータベース接続を通常必要とします。サーバにおいて使用可能なデータベース接続がなくなると、クライアントには接続エラーが返されるようになります。

以下の表は、Apache 構成ファイルの格納場所と一般的なデフォルト接続数を示しています。

プラットフォーム	場所	クライアント接続
Windows	C:\Program Files\VMware\VMware ACE Management Server\Apache2\conf\httpd.conf	250 (WinNT MPM セクション)
Red Hat Enterprise Linux	/etc/httpd/conf/httpd.conf	256 (prefork MPM セクション)
SUSE Linux	/etc/apache2/server-tuning.conf	150 (prefork MPM セクション)
ACE Management Server アプライアンス	/etc/httpd/apache2.conf	20 (prefork MPM セクション)

Red Hat Enterprise Linux への PostgreSQL データベースのデフォルト インストールではリモート接続が 100 までしか許可されておらず、この数は、同じプラットフォーム上で Apache サーバがデフォルトで開始する並列スレッドの数を下回っています。大量のクライアントがサーバに要求を送信する（アクティブなクライアント数が 100 を超える）と予測される場合は、この数値を変更します。

許可されるデータベース接続数を増やすには、以下の手順を実行します。

- 1 ACE Management Server ホスト上の Apache 構成ファイルを調べて、同時に開始できる並列スレッドまたは並列プロセスの数を確認します。
- 2 Apache サーバと同じ接続数が許可されるようにデータベースを構成します。
詳しくは、データベースのマニュアルを参照してください。

Linux でのデータベース接続プールの有効化

Linux ホスト上でデータベース接続のプールを有効にすると、高負荷の状況でパフォーマンスを大幅に改善できます。ACE Management Server は、要求のたびに新たにデータベース接続を開くのではなく、データベース接続を再利用できます。

Linux プラットフォーム上のサーバのパフォーマンスを最適化する場合には、ODBC ドライバマネージャでデータベース接続のプールを有効にします（デフォルトでは無効に設定されています）。

Windows プラットフォームでは、ODBC 接続のプールはデフォルトで有効です。

Linux 上でデータベース接続のプールを有効にするには、以下の手順を実行します。

- 1 root ユーザーとして ODBCConfig ユーティリティを開始します。
- 2 [Advanced] タブをクリックします。
- 3 [Connection Pooling] チェック ボックスを選択します。

サーバアプライアンスと外部データベースとの接続のセットアップ

ACE Management Server アプライアンスには、PostgreSQL データベース サーバが含まれていません。しかし、外部データベース サーバをアプライアンスと共に使用できます。

サーバアプライアンスと外部データベースとの接続をセットアップするには、以下の手順を実行します。

- 1 サーバアプライアンスの初回実行時に作成したパスワードを使用して、サーバアプライアンスのコンソールに **root** としてログインします。
- 2 **/etc/odbc.ini** ファイルをテキスト エディタで開きます。

例:

```
vaos# vi /etc/odbc.ini
```

このファイルには、**postgres_dsn** という ODBC DSN の設定が含まれています。

- 3 先頭の 2 行を除き、**postgres_dsn** ファイルのすべての行のコメント化を解除します。
行のコメント化を解除するには、各行の先頭にあるシャープ記号 (#) を削除します。
- 4 プレースホルダ <...> を、PostgreSQL データベース サーバの DSN 名または IP アドレス、およびこのサーバ内のデータベース名に置き換えます。
- 5 デフォルトのポート番号を使用するか、異なるポート番号を設定します。
- 6 ファイルを保存します。

この作業を完了すると、**postgres_dsn** が ACE Management Server Setup アプリケーションの [データベース] タブのドロップダウンメニューに表示されるようになります。

カスタム セキュリティ証明書の準備

カスタム SSL 証明書（独自の自己署名証明書、サードパーティが署名した証明書、内部 CA（信頼できる認定機関）が発行した証明書のいずれか）を使用する場合は、証明書、キー、および証明書チェーンファイル（CA の場合）を提供する必要があります。これらのファイルは PEM 形式でエンコードされている必要があります。

これらのファイルを作成または入手したら、ACE Management Server Setup アプリケーションの [カスタム SSL 証明書] タブを使用して、これらのファイルを ACE Management Server にアップロードします。

VMware ACE で SSL 証明書を使用する方法については、「[SSL 証明書と SSL プロトコルの使用](#) (P.23)」を参照してください。

カスタム セキュリティ証明書を準備するには、以下の手順を実行します。

- 1 必要なファイルを作成または入手します。
 - 独自の自己署名証明書を使用する場合は、**openssl** ユーティリティを使用して自己署名証明書を新規作成します。
 - サードパーティ CA または内部 CA が署名した証明書を使用する場合は、該当する CA によって署名された SSL 証明書と、証明書の検証チェーンファイルを入手します。

チェーンファイルは、作成または入手した新しい SSL 証明書を検証するうえで必要な、各証明書の連結を示したものです。証明書チェーンを入手するためのステップは、使用するホスト OS、および CA 証明書の入手元に応じて異なります。
 - プライベート キーファイル。SSL は、パブリック キーとプライベート キーのペアを使用してデータを暗号化します。パブリック キーは一般に公開されますが、プライベート キーはメッセージの受信者のみが把握しています。
- 2 ファイル名を以下のように変更します。
 - プライベート キーファイルの名前を **server.key** に変更します。
 - 証明書ファイルの名前を **server.crt** に変更します。
 - 証明書チェーンファイルの名前を **chain.crt** に変更します。

これで、ACE Management Server Setup アプリケーションを使用して証明書ファイルをアップロードできるようになりました。

自己署名証明書ファイルのプロパティの表示

このファイルは、VMware ACE Management Server のプログラム ディレクトリ内の、SSL ディレクトリに保管されます。

自己署名証明書ファイルのプロパティを表示するには、以下の手順を実行します。

次のいずれかを実行してください。

- Windows ホストの場合は、`server.crt` ファイルの格納場所に移動して、このファイル名をダブルクリックします。
- Linux ホストの場合は、以下のコマンドを使用します。

```
openssl x509 -in /var/lib/vmware/acesc/ssl/server.crt -text
```

有効期限が切れた証明書の置き換えについては、「[カスタム セキュリティ証明書の準備 \(P.49\)](#)」を参照してください。証明書に変更を加えて無期限にすることはしないでください。

ACE Management Server の構成の開始

(LDAP による) Active Directory 統合、外部データベース、またはカスタム SSL 証明書を使用する場合は、ACE Management Server を構成する前にいくつかのセットアップ作業を行う必要があります。「[サーバ構成の前提条件 \(P.41\)](#)」を参照してください。

[開始] タブに表示されるテキストは、最初の構成をすでに行ったかどうかによって、以下のように異なります。

- このページで [このサーバはまだ構成されていません] と表示される場合は、[開始] をクリックして構成セットアップ ウィザードでの作業を完了させる必要があります。
- このページで [このサーバは構成されています] と表示される場合は、ウィザードのボタンである [次へ] と [前へ] は表示されません。タブをクリックすると、他のタブに移動することができます。

ライセンス情報の表示および変更

ACE Management Server のシリアル番号を入力したら、[ライセンス] タブを使用して有効期限（設定されている場合）を確認します。

シリアル番号は、パッケージの登録カードに記載されています。VMware ACE をオンラインで購入した場合は、シリアル番号は電子メールで送られます。

ACE Management Server をインストールしたシステム上に、有効なサーバライセンスが複数存在する場合は、このページには 1 ライセンスだけが表示されます。

[ライセンス] タブを使用して、シリアル番号、ユーザー名、または会社名を追加または変更することができます。

このタブの情報を変更する場合は、[適用] または [キャンセル] をクリックしなければ、他のタブに移動することができません。

外部データベースの使用

内蔵データベースは、SQLite データベースです。本番環境では、外部データベースを使用することをお勧めします。

内蔵 データベースはサーバのインストール時に初期化され、特別な構成は不要です。このデータベースはテスト用であり、複数のプロセス間で効果的に共用できるようには設計されていません。

外部データベースを使用するよう ACE Management Server を構成するには、そのデータソースにアクセスするためのシステム DSN と認証情報を作成する必要があります。「[外部データベースのセットアップ](#) (P.43)」を参照してください。

以下の情報を使用して、[データベース] タブのフィールドへの入力を完了します。

- **データソース名 (DSN)** ACE Management Server マシンでシステム DSN エントリを作成したときに使用したデータソース名です。
- **ユーザー名 および パスワード** このデータベースに対するフルアクセス権 (テーブルの作成権限を含む) を持つユーザー アカウントの認証情報です。

データベース接続の認証情報を入力すると、セットアップアプリケーションは既存のデータベースがあるかどうかを確認します。



要注意 認証情報の入力後に「**互換性のあるスキーマが存在します。スキーマを再初期化して既存のデータを上書きしますか**」というメッセージが表示されたら、既存のデータベース内にデータをすべて削除する場合を除いて、[既存のインスタンスを使用] を選択します。後でデータベースを再初期化する場合は、この構成アプリケーションをもう一度開いて、このページに戻ることができます。

既存のスキーマに互換性がない場合、スキーマの使用やアップグレードはできません。既存のスキーマとデータを上書きすると、新しいスキーマが作成されます。既存のスキーマとデータを上書きしなかった場合は、構成アプリケーションが終了します。

サーバを以前のリリースからアップグレードする場合、データベーススキーマは自動的にアップグレードされます。この場合、以前のデータは失われません。このアップグレードは、セットアップアプリケーションを再実行しなくても、アップグレードされたサーバの初回実行時に行われます。

[データベース] タブの情報を変更する場合は、[適用] または [キャンセル] をクリックしなければ、他のタブに移動することができません。

アクセスコントロールの作成

[アクセスコントロール] タブで、ローカル Administrator ロールと Help Desk ロールを作成するか、Active Directory を使用してこれらのロールを持つユーザーを認証することができます。

ドメインアカウントを使用して認証できるように ACE Management Server を構成する前に、ユーザーとグループを作成して ACE Management Server が LDAP サーバに接続できるようにする必要があります。「[Active Directory 統合用のユーザーおよびグループの作成 \(P.42\)](#)」を参照してください。

以下の情報を使用して、認証用のフィールドへの入力を完了します。

- **ローカルアカウント** Administrator ロールのパスワードを指定し、そのパスワードを忘れてたりなくしたりした場合は、サーバの構成ファイルを削除する必要があります。このファイルを削除すると、サーバの設定が初期状態に戻ります。サーバを再構成し、管理者パスワードを再設定する必要があります。

「[サーバ構成ファイルの削除と新しい管理者パスワードの設定 \(P.77\)](#)」を参照してください。

- **ドメインアカウント (LDAP)** Active Directory を使用して認証を行う場合は、ACE Management Server が使用するホストと認証情報を指定してドメインコントローラに接続し、ドメインコントローラに対してクエリを実行します。
 - **ホスト名** IP アドレスや親ドメイン名のないホスト名 (`ldap` など) ではなく、完全修飾ドメイン名 (`ldap.vmware.com` など) を入力します。
 - **クエリユーザー sAMAccountName およびクエリユーザーのパスワード** この目的で Active Directory に作成したユーザーアカウントのパスワードと短い名前を使用します。
 - **クエリユーザードメイン** LDAP ホストがドメインコントローラとなっているドメインにする必要があります。
 - **管理グループ DN および Help Desk グループ DN** (オプション) グループを区別する目的で Active Directory に作られたグループ名を入力します (`cn=Users`、`dc=simplecorp`、`dc=com` など)。

このオプションが有効に設定されていない場合、Help Desk アプリケーションにログインするユーザーはすべて ACE 管理者グループのメンバーである必要があります。

- **Help Desk ロールまたはグループ DN** Help Desk ロールを作成すると、特定のユーザーが Help Desk アプリケーションから Help Desk タスクを実行できるようになります。このロールのユーザーは、他の管理ツールにはアクセスできません。ただし、Help Desk Web アプリケーションには、管理者の LDAP 認証情報またはローカルの管理者パスワードを使用してログインできます。

[アクセスコントロール] タブの情報を変更する場合は、[適用] または [キャンセル] をクリックしなければ、他のタブに移動することができません。

カスタム SSL 証明書のアップロード

ACE Management Server でカスタム SSL 証明書（独自の自己署名証明書か、サードパーティまたは内部 CA（信頼できる認定機関）が署名した証明書のいずれか）を使用するには、[カスタム SSL 証明書] タブを使用して、PEM 形式でエンコードされたファイルをアップロードします。

カスタム SSL 証明書をアップロードする前に、証明書ファイルを作成して名前を変更する必要があります。「[カスタム セキュリティ証明書の準備](#) (P.49)」を参照してください。

デフォルトでは、ACE Management Server のインストール時に、次の 2 つのファイルが作成されます。

- **server.key** この RSA 1024 ビット キーはプライベート キーです。
- **server.crt** この自己署名証明書の有効期間は、サーバがインストールされた日時から 10 年間です。この署名は証明書に埋め込まれているパブリック キーによって検証されます。証明書ファイルは PEM 形式でエンコードされます。

ACE インスタンスを実行する際、VMware Player アプリケーションは、ホスト上ではなくパッケージ内にある完全な証明書チェーンを使用して ACE Management Server への接続を検証します。そのため、ほとんどのセキュリティ ニーズには自己署名証明書の使用で十分に対応できます。VMware ACE でセキュリティ証明書を使用する方法については、「[SSL 証明書と SSL プロトコルの使用](#) (P.23)」を参照してください。

[証明書のアップロード] をクリックすると、指定したファイルと場所を示すサマリ ページがこのタブに表示されます。バックアップファイルの場所はメモしておきます。[適用] をクリックしたときに新しいファイルが無効であることが判明した場合に、このバックアップの使用が必要になる場合があるためです。「[SSL 証明書のバックアップ コピーのリストア](#) (P.78)」を参照してください。

カスタム SSL 証明書をアップロードしたら、新しい証明書とキー ファイルが使用されるようにするため、既存の ACE 有効仮想マシンを更新する必要があります。そのためには、Workstation を使用してアップデート パッケージを作成します。新しいパッケージをデプロイすると、ACE インスタンスは、新しい証明書ファイルと証明書チェーンを受け取ります。

イベントのロギング

サーバは、データベースを変更するイベントのログ エントリを収集します。[ログ] タブで、ロギングのレベル、およびログ エントリの消去オプションを設定できます。

ACE Management Server は以下のログ カテゴリを使用します。

- **ACE 管理** インスタンスの作成、更新、および破棄に関するイベントをログに記録します。
- **パッケージ管理** パッケージの作成と更新、インスタンスのカスタマイズ、およびパッケージの削除に関するイベントをログに記録します。
- **ポリシー管理** ポリシー セットの更新と公開、ユーザー アクセス制御の変更、および ACE 管理者によるインスタンスパスワードの設定に関するイベントをログに記録します。
- **インスタンス管理** インスタンスのライフサイクル イベント（作成、コピー、失効、再有効化、および削除）をログに記録します。また、ユーザーまたは管理者によるインスタンスパスワードの変更、インスタンスごとの有効期限の変更、インスタンスのゲスト OS またはホスト OS の情報の変更、およびインスタンスのカスタム フィールドの設定を記録します。デバッグ レベルを使用すると、アクティブなインスタンスからのポリシー更新要求など、一般的なほとんどのトラブルシューティングをログに記録できます。インスタンスの検証の失敗は、デバッグ レベルでのみログに記録されます。
- **認証** 管理またはヘルプデスクの認証の試行（標準レベル）、インスタンスの認証（通知レベル）、リモート LDAP パスワードの変更など、すべての認証要求に関するイベントをログに記録します。このカテゴリのロギングは必要最小限のレベルに設定することをお勧めします。このカテゴリでは膨大な量のエントリが生成される可能性があるためです。

各カテゴリについて、以下のいずれかのロギング レベルを選択できます。

- **なし** このイベントのログ エントリを作成しません。
- **クリティカル** クリティカルなログ イベントには、ACE 有効仮想マシンに関連付けられたすべてのパッケージ、インスタンス、およびポリシーを削除するイベントなどが該当します。
- **標準** ほとんどの照会に対しては、このレベルの詳細情報で十分に回答できます。
- **通知** 影響が限定されている、破壊的ではないイベントのエントリです。
- **デバッグ** サーバにおけるすべてのクライアント アクセスのエントリです。特定のイベント タイプについて詳細なレコードを記録するため、他のログ レベルと比べて膨大な量のログ エントリが作成されます。インスタンスの状態などの、すべての通知トランザクションをログに記録します。

[イベント ログの消去] 機能を使用して、保持するログ情報の量を設定します。消去のメンテナンス プロセスは、約 6 時間ごとに実行されます。

[ログ] タブの情報を変更する場合は、[適用] または [キャンセル] をクリックしなければ、他のタブに移動することができません。

構成設定の適用

いずれかのタブで [適用] をクリックすると、[再起動] ページが表示されます。構成設定が反映されるようにするには、サーバを再起動する必要があります。

[後で再起動] をクリックした場合は、内容を変更していないタブも含め、任意のタブで [適用] をクリックするといつでもサーバを再起動できます。

複数の ACE Management Server インスタンスのロード バランシング

5

何千ものクライアントがある場合は、複数の VMware ACE Management Server インスタンスを互いに連携させるように構成できます。2 台以上のサーバをセットアップし、ロード バランサーとともに使用することができます。

この章では、以下のトピックについて説明します。

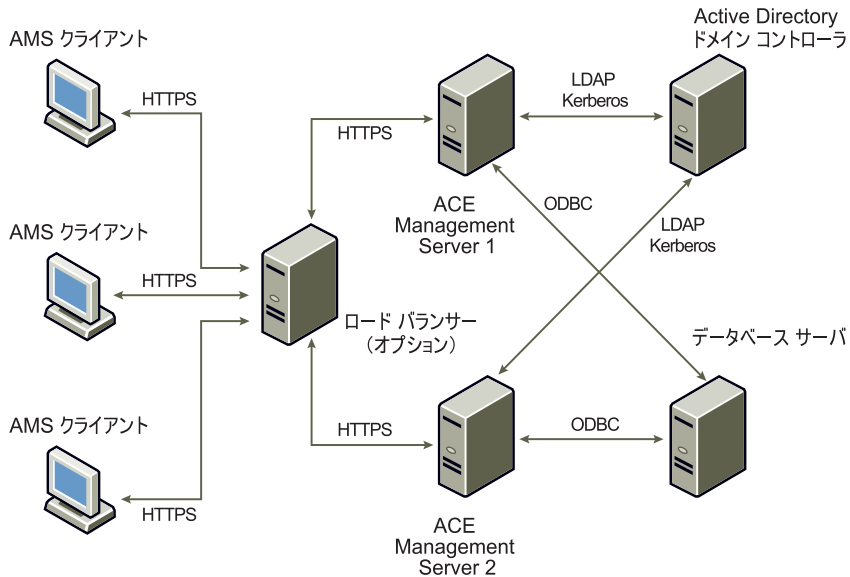
- [ロード バランシングされた ACE Management Server インスタンスによる標準的なセットアップ](#) (P.57)
- [ロード バランシングに必要なサービスのインストール](#) (P.59)
- [すべてのサーバに対する同じ SSL 証明書の使用](#) (P.59)
- [サーバごとの新しい SSL 証明書および SSL キーの作成](#) (P.61)
- [ロード バランサーのインストールと構成](#) (P.63)
- [ACE インスタンスがロード バランサーを使用していることの確認](#) (P.63)

ロード バランシングされた ACE Management Server インスタンスによる標準的なセットアップ

単一の ACE Management Server でもあらかじめ設定した数のクライアントを処理できますが、ロード バランシングを使用すると、さらに多くのサーバを ACE Management Server に追加できます。複数のサーバをロード バランシング グループに追加すると、対応できるクライアント数が直線的に増加します。たとえば、1 台のサーバで 2000 クライアントに対応できる場合、ロード バランシングされたサーバを 2 台使用すると、4000 クライアントまで対応可能になります。

図 1 は、ロード バランシングを使用するための単純なデプロイトポロジを示しています。

図 1 2 台の ACE Management Server インスタンスの連携



図のようなセットアップを使用するには、以下の準備が必要となります。

- ACE Management Server プロセスをホストする 2 台以上のマシン (または仮想マシン)
- ACE Management Server のデータをホストする外部データベース
- トラフィックを管理するロード バランシング ソリューション

ロード バランシングに必要なサービスのインストール

サービスには、複数の ACE Management Server インスタンス、1 個の外部データベース、および Workstation が含まれます。

ロード バランシングに必要なサービスをインストールするには、以下の手順を実行します。

- 1 ACE Management Server パッケージを 2 台以上のマシン（または仮想マシン）にインストールします。

「[ACE Management Server のインストールとアップグレード](#) (P.31)」を参照してください。

- 2 ACE Management Server ごとに、同じ外部データベースにアクセスするように構成します。

「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。

インストールした両方の ACE Management Server が同じデータ ストアを識別できるようにする必要があります。そうすれば、どちらの ACE Management Server も、クライアントのクエリを処理し、対応可能なクライアントの数を拡大することが可能になります。

- 3 両方の ACE Management Server が正しく動作していることを確認するには、以下のように、Workstation を起動して各 ACE Management Server に直接接続します。
 - a Workstation で [ファイル]-[ACE Management Server への接続] を選択します。
 - b ACE Management Server がインストールされているマシンの IP またはホスト名を入力し、必要に応じて [ポート] フィールドの番号を変更して、[OK] をクリックします。

各 ACE Management Server インスタンスで [インスタンス ビュー] ウィンドウに同じデータが表示できれば、セットアップは成功です。テスト用の ACE を作成してプレビューした場合は、どちらのサーバでもプレビューのインスタンスが表示されます。

すべてのサーバに対する同じ SSL 証明書の使用

ロード バランシング ソリューションでは、SSL 証明書と SSL キーを ACE Management Server 間でコピーできます。



要注意 この手順では、証明書ファイル（.crt ファイル）と照合キーファイル（.key ファイル）の両方をアップロードすることになります。両方をアップロードしないと、2 番目の ACE Management Server の Apache **httpd** サービスがフリーズすることがあります。フリーズした場合は、ACE Management Server のアンインストールと再インストールが必要になります。

すべてのサーバで同じ SSL 証明書を使用するには、以下の手順を実行します。

- 1 1 番目の ACE Management Server の ACE Management Server Setup アプリケーションにログインします。
- 2 [カスタム SSL 証明書] タブをクリックして、SSL 証明書と SSL キーのディレクトリファイルがある場所を探します。
 - Windows の場合、これらのファイルは **C:\Program Files\VMware\VMware ACE Management Server\ssl** にあります。
 - Linux の場合、これらのファイルは **%var%lib%vmware%acesc%ssl** にあります。

証明書ファイルは **server.crt** です。キー ファイルは **server.key** です。

- 3 これらのファイルを 2 番目の ACE Management Server にコピーします。

ACE Management Server 仮想アプライアンスを使用している場合は、以下のよう
に、**scp** (secure copy) コマンドを使用して証明書ファイルとキー ファイルを
コピーします。

 - a コマンド プロンプトを開きます。
 - b 以下のコマンドを入力します。

```
scp user@<ホスト>:<ファイル> user@<ホスト>:<ファイル>
```

また、Workstation を使用して仮想アプライアンスを実行している場合は、共有フォルダを有効にし、その共有フォルダ機能を介して仮想マシンからファイルをコピーすることができます。共有フォルダについての詳細は、『Workstation ユーザー マニュアル』を参照してください。

- 4 2 番目の ACE Management Server の ACE Management Server Setup アプリケーションにログインします。
- 5 [カスタム SSL 証明書] を使用して、以下の手順でファイルをアップロードします。
 - a [サーバのプライベート キー] フィールドでキー ファイルを指定します。
 - b [サーバのパブリック証明書] フィールドで証明書ファイルを指定します。
 - c [証明書のアップロード] をクリックします。

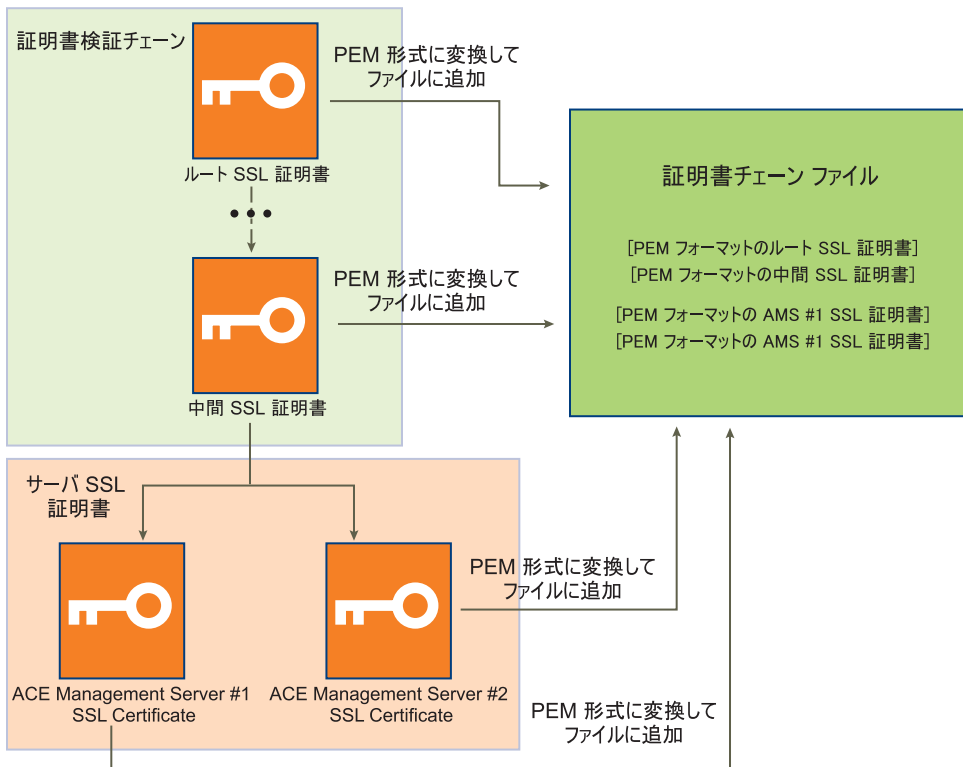
d [適用] をクリックし、[再起動] をクリックします。

サーバごとの新しい SSL 証明書および SSL キーの作成

各 ACE Management Server で同じ SSL 証明書と SSL キーを使用したくない場合は、サーバごとに新しい SSL 証明書と SSL キーを作成する必要があります。

SSL 証明書を信頼できる認定機関から入手する場合は、証明書チェーンを作成する必要があります。図 5-1 は、チェーンに含める証明書の種類を示しています。

図 5-1. 証明書チェーン ファイルの作成



サーバごとに新しい SSL 証明書および SSL キーを作成するには、以下の手順を実行します。

- 1 SSL 証明書と SSL キーのペアを必要な数だけ（サーバファームのサーバごとに 1 ペア）作成します。

そのための手順は、使用するツールによって異なります。証明書とキーの作成方法については、お使いのプラットフォームのマニュアルを参照してください。各証明書には、固有の共通名とシリアル番号が付けられている必要があります。

- 2 お使いの証明書で検証用の証明書チェーンが必要な場合は、証明書ごとに証明書チェーンファイルを作成します。

証明書チェーンファイルはテキストファイルで、（チェーンのルート証明書を含む）リーフ証明書の検証に必要な（PEM 形式の）証明書がすべて含まれます。

- a 信頼できる認定機関から検証チェーンをダウンロードします。
- b 証明書チェーンファイルを作成する前に、すべての証明書を PEM 形式にする必要があります。

PEM 形式に変換するには、オンラインで入手できるオープンソースの SSL ツールを使用します。

- c PEM 形式にエンコードされた各証明書を 1 つのファイルに連結して、証明書チェーンファイルを作成します。

- どちらの証明書も自己署名証明書である場合は、両方の証明書が連結されたファイルを証明書チェーンファイルにする必要があります。
- どちらの証明書も同じ信頼できる認定機関から入手した場合は、それらの証明書の検証チェーンだけが含まれるファイルをチェーンファイルにし、そのチェーンを同じにする必要があります。
- 証明書を入手した信頼できる認定機関が異なる場合は、両方の証明書検証チェーンを含むファイルをチェーンファイルにする必要があります。

たとえば、2 つの ACE Management Server インスタンスを使用している場合は、2 つの証明書チェーンファイルを用意します。

- 3 すべての証明書チェーンファイルを 1 つのファイルに連結します。
可能であれば、重複エントリを削除します。
- 4 サーバの SSL 証明書を PEM 形式に変換します。
- 5 PEM 形式に変換したサーバの SSL 証明書を証明書チェーンファイルに追加します。

- 6 [カスタム SSL 証明書] タブで、SSL 証明書ファイル、SSL キー ファイル、および証明書チェーン ファイルを以下のようにアップロードします。
 - a [サーバのプライベート キー] フィールドでキー ファイルを指定します。
 - b [サーバのパブリック証明書] フィールドで証明書ファイルを指定します。
 - c [証明書のアップロード] をクリックします。
 - d [適用] をクリックし、[再起動] をクリックします。

サーバファーム内のすべての ACE Management Server に対してこの作業を実行し、ファイルを各 ACE Management Server にアップロードします。

ロード バランサーのインストールと構成

ACE Management Server は、クライアントとの通信に HTTPS を使用します。HTTPS をサポートするどのようなロード バランシング ソリューションも、ACE Management Server と共に使用できます。

ロード バランサーをインストールしたら、ポート 443 (HTTP over SSL) をロード バランシング用に構成します。ポート 8080 とポート 8000 はロード バランシング用に構成しないでください。この 2 つのポートは他の構成のために使用されます。ポート 8080 は仮想アプライアンスの構成用ポートで、ポート 8000 は ACE Management Server の構成用ポートです。

ACE インスタンスがロード バランサーを使用していることの確認

複数の ACE Management Server インスタンスをロード バランサーと共に動作するよう構成し、必要な SSL 証明書をインストールしたら、確認作業を行います。ACE インスタンスがロード バランサーのアドレスを使用して ACE Management Server に接続できることを確認します。

開始する前に Workstation を再起動し、ACE Management Server への接続が確立したときに Workstation が SSL 証明書をダウンロードできるようにしておきます。

ACE インスタンスがロード バランサーを使用していることを確認するには、以下の手順を実行します。

- 1 ACE 有効仮想マシンを作成します。
- 2 ポリシー エディタを開きます。
- 3 [ポリシーの更新頻度] を選択します。
- 4 [オフラインの使用を無効にする] を選択します。

- 5 [OK] をクリックします。
- 6 1 番目の ACE Management Server をロード バランシング構成から削除して、すべてのトラフィックが 2 番目の ACE Management Server に向かうようにします。
- 7 ACE インスタンスをプレビューします。
このプレビューによって、ACE Management Server 上にインスタンスが作成されます。
- 8 ACE Player を閉じます。
- 9 2 番目の ACE Management Server をロード バランシング構成から削除して、1 番目の ACE Management Server を構成に追加し直します。
すべてのトラフィックが 1 番目の ACE Management Server に向かいます。
- 10 同じ ACE Management Server を再度プレビューし、インスタンスを作成し直すか再利用するかを選択するプロンプトが表示されたら、[既存のインスタンスを使用] を選択します。
インスタンスの起動に成功した場合は、両方のサーバが同じ SSL 証明書を使用しています。

ACE インスタンスの管理

ACE Management Server をインストールおよび構成した後は、以下のことが可能になります。

- 特定の ACE Management Server で管理されている ACE インスタンスを表示できません。
- インスタンスを無効化 / 再有効化できます。
- インスタンスのユーザーによって報告された ACE インスタンスのさまざまな問題に対処できます。

この章では、以下のトピックについて説明します。

- [サーバが管理する ACE インスタンスの表示](#) (P.66)
- [インスタンスの検索](#) (P.68)
- [列の見出しによる並べ替えと列の幅の変更](#) (P.69)
- [インスタンスビューでの列の表示、非表示、移動](#) (P.70)
- [インスタンスビューでのカスタム列の作成または削除](#) (P.70)
- [インスタンスの詳細の表示](#) (P.71)
- [ACE インスタンスの再アクティベーション、アクティベーション解除、または削除](#) (P.72)
- [コピー保護 ID の変更](#) (P.72)
- [認証パスワードのリセット](#) (P.73)
- [カスタム列の情報の追加](#) (P.74)

サーバが管理する ACE インスタンスの表示

サーバの ACE インスタンスを表示および管理する場合、VMware ACE Help Desk の [インスタンス] ページを使用するか、Workstation でサーバのインスタンス ビューを使用することができます。

どちらのユーザー インターフェイスでも、インスタンスの再アクティベーション、インスタンスの有効期限の変更、ユーザー パスワードの再設定（ユーザーが忘れた場合）など、ACE インスタンス関連の一部の問題に対処できます。

VMware ACE Help Desk はブラウザ ベースのアプリケーションであるため、Workstation をインストールしていないコンピュータでも使用できます。また、Help Desk を使用して限定的な Help Desk ロールを作成できます。このロールを持つユーザーは、エンド ユーザーから報告された一部の問題に対処することができますが、ACE Management Server の構成設定を変更することはできません。

Workstation のインスタンス ビューを利用すると、VMware ACE Help Desk で実行可能なすべてのタスクに加え、他のいくつかのタスクを実行できます。たとえば、インスタンス ビューでカスタム列を作成したり、作成した検索を保存したりすることができます。

VMware ACE Help Desk アプリケーションの使用

ACE 管理者と Help Desk 担当者は VMware ACE Help Desk Web アプリケーションを介して ACE インスタンスにアクセスできます。Help Desk を使用すると、インスタンスの再アクティベーション、インスタンスの有効期限の変更、およびユーザー パスワードの再設定（ユーザーが忘れた場合）を行うことができます。

VMware ACE Help Desk アプリケーションを使用するには、以下の手順を実行します。

- 1 Web ブラウザを開いて、**https://<ホスト名>:8000** にアクセスします。
<ホスト名> には、ACE Management Server がインストールされているコンピュータの完全修飾名か、IP アドレスを値として使用できます。

ACE Management Server が Windows ホストにインストールされており、そのホストを使用して構成を行う場合は、[スタート]-[VMware]-[VMware ACE Management Server] を選択することもできます。

- 2 [Help Desk] リンクをクリックします。
- 3 ログイン情報を入力します。

以下の情報を使用して、このウィンドウに表示されているフィールドへの入力を完了します。

- [ユーザー名]および[パスワード] Help Desk ロールが作成されている場合は、そのロールの認証情報を入力します。作成されていない場合は、ACE Management Server の管理者の認証情報を入力します。
- [ドメイン] マルチドメイン環境では、ドメイン (**eng.com** など) の入力が必要になることがあります。

VMware ACE Help Desk の [インスタンス] ページが開きます。このページには、そのサーバが管理しているすべてのインスタンスのサマリ表が含まれています。

Workstation でのインスタンス ビューの使用

ACE 管理者は、インスタンス ビューを介して ACE インスタンス にアクセスできます。インスタンス ビューを使用すると、インスタンスの再アクティベーション、インスタンスの有効期限の変更、およびユーザー パスワードの再設定（ユーザーが忘れた場合）を行うことができます。

Workstation のインスタンス ビューを利用すると、VMware ACE Help Desk で実行可能なすべてのタスクに加え、他のいくつかのタスクを実行できます。インスタンス ビューでカスタム列を作成したり、作成した検索を保存したりすることができます。

インスタンス ビューを使用するには、管理者の認証情報が必要になります。

インスタンスの状態は、以下の3種類のいずれかです。



アクティブ インスタンスはアクティブで、すぐに使用できます。



アクティベーション解除済み このインスタンスは、意図的にアクティベーション解除されています。再度使用するためには、再アクティベーションする必要があります。



ポリシーによりブロック インスタンスはアクティブですが、有効期限やコピー保護などのポリシーに違反しているために、ブロックされています（実行できません）。詳細については、このインスタンスのサーバログを参照してください。

[有効期間開始日] 列と [有効期間終了日] 列は、そのインスタンスの有効期間を示しています。このインスタンスは、[有効期間終了日] の日付までで有効期限切れとなります。インスタンスに有効期限が設定されていない場合、これらの列は空白になります。

Workstation でインスタンスビューを使用するには、以下の手順を実行します。

- 1 Workstation のメニューバーで、[ファイル]-[ACE Management Server への接続] を選択します。
- 2 完全修飾ホスト名または IP アドレスを指定して、[OK] をクリックします。
ほとんどの場合、デフォルトのポート番号を変更する必要はありません。
- 3 ログインウィンドウに必要な情報を入力します。
以下の情報を使用して、このウィンドウに表示されているフィールドへの入力を完了します。
 - [ユーザー名]および[パスワード] ACE Management Server の管理者の認証情報を入力します。
 - [ドメイン] マルチドメイン環境では、ドメイン (**eng.com** など) の入力が必要になることがあります。

インスタンスの検索

検索機能を使用すると、ACE Management Server データベースに対してクエリを実行して、特定の ACE インスタンスを 1 つ以上見つけることができます。検索条件には、OR ではなく AND の処理が適用されます。

開始前に、次のいずれかの作業を行います。

- ACE Management Server の VMware ACE Help Desk にログインします。
- Workstation のウィンドウから ACE Management Server に接続します。

ACE インスタンスを検索するには、以下の手順を実行します。

- 1 [検索] をクリックし、データベースのクエリが実行されるときに適用される条件を指定します。
以下の情報を使用して、特定の検索条件を指定します。
 - [アクティベーション方法] パスワード、Active Directory ユーザー、アクティベーション キーなどのアクティベーション方法です。該当するアクティベーション方法がない場合は、この列には「N/A」と表示されます。
 - [ACE 仮想マシン名] ACE インスタンスの作成元となった ACE 有効仮想マシンの名前です。

- [ゲスト名] (Windows ゲストのみ) インスタンスのカスタマイズ機能を使用した場合に、カスタマイズ中にユーザーのマシンで解決されるコンピュータ名です。ここでは NetBIOS 名が報告されますが、名前の長さは最長 15 文字です。実際のコンピュータ名がこの制限を越える長さである場合も、名前は常に NetBIOS 名として表示されます。
 - [カスタム]列 作成したカスタム列は、[ゲスト MAC アドレス]条件のすぐ下に表示されます。
 - [完全一致のみ] この値は大文字と小文字が区別されます。
 - [名前を付けて保存] (Workstation のインスタンスビューのみで利用可能) 保存された検索は各サーバの専用となります。保存された検索を編集または削除するには、[保存された検索]ドロップダウンメニューで保存された検索の名前を選択してから[オプション]をクリックします。
- 2 [検索]をクリックします。
検索結果では、インスタンスの総数が表のすぐ下に表示されます。
 - 3 多数の検索結果を表示するには、次のいずれかを行います。
 - VMware ACE Help Desk の場合は、[インスタンス]表の下部にあるステータスバーの右側にある矢印をクリックして前後に移動します。
 - Workstation のインスタンスビューの場合は、スクロールダウンします。
 - 4 全体リストに戻るには、以下のいずれかを実行します。
 - VMware ACE Help Desk の場合は、[検索]ボタンの下にある[すべてのインスタンスに戻る]リンクをクリックします。
 - Workstation のインスタンスビューの場合は、[検索をクリア]をクリックします。

列の見出しによる並べ替えと列の幅の変更

選択した列の内容に応じて、表のインスタンスをアルファベットまたは数字の昇順/降順で並べ替えることができます。

列の見出しによる並べ替えを行い、列の幅を変更するには、以下の手順を実行します。

- 1 並べ替える列の見出しをクリックします。
再びクリックすると、逆の順序（昇順または降順）で並べ替えが行われます。
- 2 列の幅を変更するには、列の境界線をクリックして、新しい幅の位置までドラッグします。

インスタンス ビューでの列の表示、非表示、移動

列の並べ替えとサイズ変更は VMware ACE Help Desk でも Workstation のインスタンス ビューでも実行できますが、列の表示、非表示、および移動は Workstation のインスタンス ビューだけで実行できます。

あるサーバで列を変更しても、他のサーバには影響しません。

インスタンス ビューで列を表示、非表示、および移動するには、以下の手順を実行します。

- 1 Workstation で ACE Management Server に接続してログインします。
「[Workstation でのインスタンス ビューの使用](#) (P.67)」を参照してください。
- 2 列の表示または非表示を切り替えるには、列の見出し行を右クリックして、表示または非表示にする列を選択するか選択解除します。

非表示になっていた列を表示すると、その列は表の右側に追加されます。
- 3 列を移動するには、列の見出しをクリックして新しい位置にドラッグしてから、マウスのボタンを離します。

インスタンス ビューでのカスタム列の作成または削除

カスタム列を使用して、ACE Management Server が管理するインスタンスについて追加のカテゴリ情報を表示することができます。たとえば、[ヘルプ チケット] 列を追加し、エンド ユーザーの要求に ID 番号を付けて記録することができます。

カスタム列は、Workstation のインスタンス ビューでのみ作成できます。インスタンス ビューの表で、最大 9 個のカスタム列を追加したり、削除したり、名前を変更したりすることができます。

インスタンス ビューでカスタム列を作成または削除するには、以下の手順を実行します。

- 1 Workstation で ACE Management Server に接続してログインします。
「[Workstation でのインスタンス ビューの使用](#) (P.67)」を参照してください。
- 2 列の見出し行を右クリックして、[カスタム列の追加] を選択します。
- 3 新しい列の名前を [名前] テキスト ボックスに入力して、[OK] をクリックします。
- 4 カスタム列の名前を変更するか、カスタム列を削除するには、カスタム列の見出しを右クリックして、コンテキスト メニューからコマンドを選択します。

カスタム列を作成したら、各 ACE インスタンスの [インスタンスの詳細] ページを使用して、表示する情報を追加します。「[カスタム列の情報の追加](#) (P.74)」を参照してください。

インスタンスの詳細の表示

[インスタンスの詳細] ページには、概要ページに表示される情報と同じ情報がすべて表示されるほか、ACE インスタンスのポリシー設定に関する情報が含まれます。

[インスタンスの詳細] ページでは、概要ページと同じように、インスタンスの再アクティベーションとアクティベーション解除、またはインスタンスの有効期限の変更を実行できます。また、以下の作業は、[インスタンスの詳細] ページでのみ実行できます。

- コピー保護 ID の変更
- 認証パスワードのリセット
- カスタム列の情報の追加

インスタンスの詳細を表示するには、以下の手順を実行します。

- 1 インスタンスの行をクリックして、インスタンスを選択します。
- 2 表の上部にある [詳細の表示] アイコンをクリックするか、インスタンスの行をダブルクリックします。
- 3 VMware ACE Help Desk を使用しているときにネットワーク アクセスについての詳細を表示するには、[ゾーン]、[ホスト アクセス]、または [ゲスト アクセス] の下にあるリンクをクリックします。

そのゾーンまたはそのタイプのネットワーク アクセスの [ゾーンの詳細] ページまたは [ルールの詳細] ページを表示できます。

[すべての場所] または [他のすべての場所] のゾーン設定は、その名のとおり [ゾーンの詳細] ページにはリンクされません。

ACE インスタンスの再アクティベーション、アクティベーション解除、または削除

インスタンスを再アクティベーションまたはアクティベーション解除することによって、インスタンスへのアクセスをただちに許可または拒否できます。インスタンスをアクティベーション解除した後で、サーバが管理するインスタンスのリストからそのインスタンスを削除できます。

開始前に、次のいずれかの作業を行います。

- ACE Management Server の VMware ACE Help Desk にログインします。
- Workstation のウィンドウから ACE Management Server に接続します。

ACE インスタンスの再アクティベーション、アクティベーション解除、または削除を行うには、以下の手順を実行します。

- 1 インスタンスの行をクリックして、インスタンスを選択します。
- 2 [インスタンス] ページの左上にある [アクティベーションの解除] アイコンまたは [再アクティベーション] アイコンをクリックします。
- 3 [再アクティベーション] をクリックした場合は、プロンプトが表示されたときに有効期限をリセットします。
- 4 (オプション) [アクティベーションの解除] をクリックした場合は、[削除] をクリックしてインスタンスの行を削除します。
- 5 [OK] をクリックします。

コピー保護 ID の変更

コピー保護された ACE インスタンスをエンドユーザーがコピーまたは移動しようとすると、新しいコピー保護 ID を含むエラーメッセージがユーザーに表示されます。エンドユーザーがその ID を管理者に送信した後で、管理者はその ID を使用して元の ID を置き換えることができます。

開始前に、次のいずれかの作業を行います。

- ACE Management Server の VMware ACE Help Desk にログインします。
- Workstation のウィンドウから ACE Management Server に接続します。

[コピー保護 ID] フィールドは常にアクティブになっているので、いつでも ID を変更できます。



要注意 アクティブなインスタンスに対してコピー保護 ID を変更すると、元のインスタンスは実行できなくなります。

コピー保護 ID を変更するには、以下の手順を実行します。

- 1 インスタンスの行をクリックして、インスタンスを選択します。
- 2 表の上部にある [詳細の表示] アイコンをクリックするか、インスタンスの行をダブルクリックします。
- 3 次のいずれかを実行してください。
 - VMware ACE Help Desk の場合は、[コピー保護 ID] フィールドの英数字のストリングを新しい ID で置き換え、ページ上部にある [保存] アイコンをクリックします。
 - Workstation の場合は、[ポリシー] タブをクリックし、コピー保護 ID を新しい ID に置き換えて [OK] をクリックします。

認証パスワードのリセット

インスタンスのパスワードを、ユーザーが指定したパスワードでリセットすることができます。新しいパスワードには、少なくとも 1 つの文字を含める必要があります。

認証パスワードをリセットするには、以下の手順を実行します。

- 1 インスタンスの行をクリックして、インスタンスを選択します。
- 2 表の上部にある [詳細の表示] アイコンをクリックするか、インスタンスの行をダブルクリックします。
- 3 [パスワードのリセット] をクリックし、新しいパスワードを指定します。
Workstation のインスタンス ビューで、このボタンは [ポリシー] タブに表示されます。
- 4 新しいパスワードを、電子メール メッセージでユーザーに送信します。

カスタム列の情報の追加

カスタム列を追加するには Workstation のインスタンス ビューを使用する必要がありますが、カスタム列のフィールドに情報を追加する作業は、Workstation のインスタンス ビューでも VMware ACE Help Desk でも実行できます。

開始前に、必要に応じて、Workstation のインスタンス ビューでカスタム列を作成します。「[インスタンス ビューでのカスタム列の作成または削除 \(P.70\)](#)」を参照してください。

カスタム列に情報を追加するには、以下の手順を実行します。

- 1 インスタンスの行をクリックして、インスタンスを選択します。
- 2 表の上部にある [詳細の表示] アイコンをクリックするか、インスタンスの行をダブルクリックします。
- 3 次のいずれかを実行してください。
 - VMware ACE Help Desk の場合は、1 つ以上のフィールドにカスタム値を入力して、ページ上部にある [保存] アイコンをクリックします。
 - Workstation の場合は、[カスタム] タブをクリックし、1 つ以上のフィールドにカスタム値を入力して [OK] をクリックします。

トラブルシューティングとメンテナンス

7

この章では、以下のトピックについて説明します。

- [構成に関する問題のトラブルシューティング](#) (P.75)
- [複数の ACE Management Server インスタンスで SSL を使用するための構成](#) (P.79)
- [データベースのバックアップ](#) (P.80)

構成に関する問題のトラブルシューティング

構成に関してよく起こる問題は、接続の問題とポートの競合の解決、および ACE 管理者パスワードのリセットです。

Linux ACE インスタンスと ACE Management Server との接続の問題

Linux ホスト上の ACE インスタンスがサーバに接続できない場合は、ファイアウォールまたはプロキシの設定でポート 443 の HTTPS トラフィックをブロックまたは再ルーティングしていないかどうかを確認します。

デフォルトでは、VMware Player から ACE Management Server への HTTPS トラフィックはポート 443 にルーティングされます。VMware Player からサーバへのトラフィックをそのポートに送信できるようにするには、ファイアウォールを無効にするか、またはプロキシ設定をオフにします。

ACE Management Server のポート割り当ての変更

ACE Management Server は、Apache 2.0 プラットフォーム上で稼働するモジュールです。サーバが接続を待機するポートを変更するには、Apache の構成ファイルを手動で編集する必要があります。

ACE Management Server のポート割り当てを変更するには、以下の手順を実行します。

- 1 テキスト エディタを使用して、ACE Management Server コンポーネントの HTTP 構成ファイルを開きます。

サーバのオペレーティング システムによって、ファイルの場所は以下のいずれかになります。

- **Windows** C:\Program Files\VMware\VMware ACE Management Server\Apache2\conf\httpd.conf
- **Red Hat Enterprise Linux 4** /etc/httpd/conf.d/acesc.conf
- **SUSE Linux Enterprise Server 9 SP3** /etc/apache2/conf.d/acesc.conf

VMware ACE Management Server を別の場所にインストールした場合、このパスは異なります。ご使用のサーバで設定されたパスを使用してください。

- 2 このファイル内で、**Listen 443** と記載された行のエントリを検索して、ポート番号を変更します。

サーバが構成用に使用しているポート 8000 と ACE Management Server アプライアンスが使用しているポート 8080 は使用できません。

- 3 仮想サーバ構成で、ポート 443 と記述されたセクション ヘッダを検索します。この行は、以下のように記述されています。

```
<VirtualHost -default_:443>
```

- 4 セクション ヘッダのポート番号を必要なポート番号に変更します。たとえば、ポート 8443 に変更するには、**443** を **8443** に変更します。

- 5 ファイルを保存します。
- 6 Apache サービスを停止し、再開します。

手順については、「[Apache サービスの起動または再起動の確認](#) (P.36)」を参照してください。

ACE 有効仮想マシンを作成する際に、ACE Management Server との通信に使用するポートを指定できます。

サーバ構成ファイルの削除と新しい管理者パスワードの設定

管理者パスワードをなくりたり忘れてたりした場合は、構成ファイルを削除してサーバを再構成する必要があります。その構成作業の一環として、新しいパスワードを設定します。

サーバの構成ファイルを削除して、新たに管理者パスワードを設定するには、以下の手順を実行します。

- 1 ACE Management Server の構成ファイルの格納場所に移動します。

サーバのオペレーティングシステムによって、ファイルの場所は以下のいずれかになります。

 - **Windows** C:¥Program Files¥VMware¥VMware ACE Management Server¥conf¥acesc.conf
 - **Linux** /var/lib/vmware/acesc/conf/acesc.conf
- 2 ファイルのコピーを新しい場所に保存して、サーバを再構成するときにファイルを参照できるようにします。
- 3 元の構成ファイルを削除します。
- 4 ACE Management Server Setup アプリケーションを起動してサーバを再構成し、[アクセスコントロール] タブでパスワードを指定します。

「[ACE Management Server の起動と構成](#) (P.37)」を参照してください。
- 5 ACE Management Server Setup アプリケーションを使用して、以下のいずれかの作業を続けます。
 - これが初めてのサーバ構成である場合は、[次へ]をクリックします。
 - サーバを再構成している場合は、[適用]をクリックしてから、[再起動]または[後で再起動]をクリックします。

[後で再起動]をクリックした場合は、サーバを再起動して構成の変更内容を有効にする必要があります。内容を変更していないタブも含め、任意のタブで[適用]をクリックするとサーバを再起動できます。

SSL 証明書のバックアップ コピーのリストア

誤った証明書ファイルをアップロードした場合、[適用]をクリックしてから [再起動]をクリックすると ACE Management Server Setup アプリケーションが失敗し、Apache サービスを再起動できなくなります。この問題を解決するには、該当する証明書のバックアップ証明書ファイルをリストアします。

SSL 証明書のバックアップ コピーをリストアするには、以下の手順を実行します。

- 1 バックアップが保存されている ACE Management Server ディレクトリに移動します。

ファイル名には以下の形式が使用されています。

<certificate_filename>.<日付>-<時刻>

ここで、<certificate_filename> 値は以下のいずれかです。

- **server.crt** サーバのパブリック証明書
- **server.key** サーバのプライベート キー
- **chain.crt** 証明書チェーン

ファイル名の <日付> 部分は、YYYYMMDD (年、月、日) 形式です。

ファイル名の <時刻> 部分は、HHMMSS (時、分、秒) 形式です。

たとえば、**server.crt.20070216-095344** のようなファイル名になります。

- 2 **ssl/<ファイル名>.crt** としてファイルを正しい格納場所に保存し、Apache サーバを手動で再起動します。

「[Apache サービスの起動または再起動の確認](#) (P.36)」を参照してください。

- 3 ACE Management Server Setup アプリケーションを起動し、[カスタム SSL 証明書] タブを使用してバックアップ コピーをアップロードします。

「[ACE Management Server の起動と構成](#) (P.37)」

複数の ACE Management Server インスタンスで SSL を使用するための構成

以下のシナリオで、複数の ACE Management Server インスタンスを構成して SSL を使用することができます。

- 1つ以上のプロキシ サーバによって保護された複数のサーバの場合
 - 各サーバが独自の SSL キーおよび SSL 証明書を持つことができます (ACE Management Server とプロキシ サーバ)。
 - **cert_chain** ファイル (証明書チェーン ファイル) には、証明書ファイルと、プロキシ サーバが使用している SSL 証明書の検証チェーンが含まれている必要があります。この **cert_chain** ファイルを、各 ACE Management Server に配置します。
 - 自己署名証明書を使用する場合、実際に証明となるのは検証チェーンです。チェーン ファイルには、各プロキシが使用するそれぞれの自己署名証明書が含まれます。
 - また、各サーバとプロキシに対して、同一のキーおよび証明書を使用することもできます。この場合、**cert_chain** ファイルを作成する必要はありません。
 - 各証明書には、固有の共通名が付けられている必要があります。
- DNS ラウンド ロビンを使用する複数のサーバの場合
 - 各サーバが独自の SSL キーおよび SSL 証明書を持つことができます (ACE Management Server とプロキシ サーバ)。
 - **cert_chain** ファイル (証明書チェーン ファイル) には、証明書ファイルと、サーバが使用するすべての証明書の検証チェーンが含まれている必要があります。この証明書チェーン ファイルを、各 ACE Management Server に配置します。
 - 自己署名証明書を使用する場合、実際に証明となるのは検証チェーンです。チェーン ファイルには、各サーバが使用するそれぞれの自己署名証明書が含まれます。
 - 各サーバに対して、同一のキーおよび証明書を使用できます。この場合、**cert_chain** ファイルを作成する必要はありません。

「[複数の ACE Management Server インスタンスのロード バランシング \(P.57\)](#)」も参照してください。

データベースのバックアップ

外部データベースを使用する場合は、そのデータベース システムに適したバックアップ方式とリカバリ方式を使用します。必要な場合に ACE Management Server のデータベースを素早くリカバリできるように、データベースを定期的にバックアップします。

内蔵データベースを使用する場合は、`ntbackup` や `dd` などの標準のファイルバックアップツールを使用できます。データは以下のいずれかの場所に保管されています。

- **Windows** `C:%Program Files%VMware%VMware ACE Management Server%db%acesc.bin`
- **Linux** `/var/lib/vmware/acesc/db/acesc.bin`

本番環境で内蔵データベースを使用する場合は、サーバを停止し、バックアップを行う別の場所にファイルをコピーしてから、サーバを再起動します。SQLite はデータベースであるため、バックアップのためのコピー中に ACE Management Server のプロセスによってデータベース ファイルが変更される可能性があります。このため、不整合な状態のデータベース スナップショットが作成されてしまう可能性があります。ただし、通常はファイルのサイズが大きくないため、迅速にコピーされることから、この問題はほとんど発生しません。

オープン データベースをバックアップするための他の方法としては、次のような方法が SQLite のコミュニティで推奨されています。

- **sqlite3** コマンドライン ツールを使用して、SQLite データベースにログインします。`.dump` コマンドを使用して、実行結果を別のファイルとして保管し、そのファイルをバックアップします。SQL スクリプトによってデータベースが再作成されます。
- Windows システムの Volume Shadow Copy メカニズムまたは Linux の LVM ボリューム スナップショット（および SQLite のクラッシュ リストア機能）を使用して、データベース ディレクトリ全体（ジャーナル ファイルがある場合はこれも含む）をバックアップします。Windows XP SP1 以降のオペレーティング システムの場合は、データベース ディレクトリに対して `ntbackup` を使用します。
- **sqlite3** コマンドライン ツールを使用して、SQLite データベースにログインします。`BEGIN EXCLUSIVE` コマンドを使用してデータベース ファイルをコピーしてから、`COMMIT` コマンドを使用します。

VRM データベース内のデータに対して、社内独自の管理ツールやレポート作成ツール、または自動化スクリプトを使用する場合には、「[データベーススキーマと監査イベント ログ データ](#) (P.81)」を参照してください。

データベーススキーマと監査 イベントログデータ



この付録では、データベースに格納されているデータの形式と、データへの最適なアクセス方法について説明します。この付録では、以下のトピックについて説明します。

- [データベースレポート作成ツールの使用](#) (P.81)
- [データベーススキーマ](#) (P.82)
- [監査イベントログのデータのクエリ](#) (P.87)

データベースレポート作成ツールの使用

サードパーティ製のデータベース管理ツールやレポート作成ツールを、VMware ACE Management Server データベースと共に使用することができます。レポート作成ツールを使用すると、システム状態に関するカスタムのレポートを作成できます。また、レポート作成ツールを使用すると、Event テーブルに格納される管理者やユーザーのアクションの監査証跡を調査できます。たとえば、最新ではない ACE ポリシーセットを含むアクティブなインスタンスがないかどうかを検索したり、認証の失敗が多発していないかどうかを検索したりすることが可能です。

データベースに格納されるデータは、RDBMS のアクセスコントロールメカニズムによって保護されます。レポート作成ツールで使用するデータベースユーザーアカウントに対しては、データへの必要以上に高いアクセスレベルを許可しないでください。許可すると、VMware ACE システムのセキュリティが脅かされる可能性があります。

たとえば、レポート作成ツールでは通常、データベースへの書き込みアクセス権は不要です。代わりに、そのレポート作成ツール用に読み取り専用の独立したアカウントを作成できます。また、ユーザーのパスワード、インスタンスのカスタマイズに関するデータ（ドメイン管理者のログイン情報が含まれる可能性があります）、インスタンスのディスクの暗号化キーなど、機密情報が含まれるデータベースフィールドへの読み取りアクセスは許可しないようにしてください。内蔵のSQLite データベースは認証をサポートしていないため、アクセスは読み取り専用権限またはすべての動作を実行する権限を提供するファイルベースのセキュリティによってのみ保護されます。

データベーススキーマ

ACE Management Server のデータベースは、ACE Management Server の主要な構成オブジェクト（ACE、パッケージ、インスタンス、アクセス ポリシー、ランタイム ポリシー、およびイメージのカスタマイズ設定などのユーザー別データ）のテーブルで構成されています。管理者やユーザーのアクションはデータベースの Event テーブルに監査ログとして記録され、発生する可能性のあるイベント タイプは EventType テーブルに一覧されています。

データベーススキーマに関して、以下の点に注意してください。

- 内部システム情報やインデックスが格納される一部のテーブルは、リストされていません。
- ブール値は、TRUE または FALSE という文字列型の値として格納されます。
- タイムスタンプは、1970 年 1 月 1 日の午前 0 時から起算したマイクロ秒数を表わす、10 進形式の 64 ビット数値文字列として格納されます。
- 他の日付および時刻は、1970 年 1 月 1 日の午前 0 時から起算した秒数を表わす 10 進形式の文字列として格納されます。
- ACE、パッケージ、インスタンス、アクセス、およびユーザー データの各レコードは、データベースからは削除されません。これらのレコードは削除済みフィールドが TRUE に設定され、削除済みとしてマークされます。これにより、監査を行う場合に以前の情報を調査できます。
- ACE ポリシー セットのゲスト OS およびホスト OS の部分は、サイズが 2000 バイト未満の場合は、PolicyDb_RuntimePolicy テーブル内のそれぞれのフィールドに文字列として格納されます。ポリシー コンポーネントが 2000 バイト以上の場合は、文字列が 2000 バイトのチャンクに分割されて PolicyDb_LongField テーブルに格納されます。この場合、RuntimePolicy テーブル内のそれぞれの ExtKey フィールドの値には、LongField テーブル内の対応する文字列の系列をポイントする外部キーが含まれます（テーブルの定義の注記を参照してください）。

データベーススキーマスクリプトを以下に記載します。

```

/* サービス情報の名前 - 値ペア (例: DB スキーマのバージョン番号) */
CREATE TABLE PolicyDb_MetaInfo (
    name VARCHAR(128),           /* 名前 / 値ペアの名前 */
    value VARCHAR(1024),        /* 名前 / 値ペアの値 */
    PRIMARY KEY(name));

/* このテーブルはゲストおよびホストのポリシー セットのデータ (2K のチャンクに分割) を保持し
   ます */
/* キーのフィールドをインデックス順にすべて選択し、ストリングを一緒に追加して、*/
/* ポリシー セットを復元します */
CREATE TABLE PolicyDb_LongField (
    longFieldKey VARCHAR(128),   /* long フィールドの系列の固有 ID */
    longFieldIndex INTEGER,      /* 系列のインデックス */
    longFieldValue VARCHAR(2000), /* フィールドの値チャンクは最大 2000 文字 */
    sessionExpires VARCHAR(21), /* セッション BLOB 格納用のオプションのフィールド */
    PRIMARY KEY (longFieldKey, longFieldIndex));

/* ACE Master データ */
CREATE TABLE PolicyDb_Ace (
    aceUID VARCHAR(128),         /* 固有 ID (プライマリ キー) */
    aceName VARCHAR(128),       /* この ACE の名前 */
    activePolicySetVersion INTEGER NOT NULL, /* アクティブ RT ポリシーに対するソフト外部
   キー */
    aceTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
    aceTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
    deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
    PRIMARY KEY(aceUID));

/* パッケージ データ */
CREATE TABLE PolicyDb_Package (
    packageUID VARCHAR(128),     /* 固有 ID (プライマリ キー) */
    aceUID VARCHAR(128) NOT NULL, /* 所属先の ACE */
    pkgName VARCHAR(128),        /* UI として表示される名前 */
    pkgUseValidDates VARCHAR(7)
        DEFAULT 'FALSE' NOT NULL, /* 有効期限を使用、または常に有効 */
    pkgValidDateStart VARCHAR(21) NOT NULL, /* パッケージの有効期限開始日。 */
    pkgValidDateEnd VARCHAR(21) NOT NULL, /* パッケージの有効期限終了日。 */
    pkgDisabled VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* パッケージが無効化されているか */
    pkgProtectionKey VARCHAR(1024), /* パッケージの配布に使用されるキー */
    pkgPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* プレビュー パッケージか */
    pkgTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
    pkgTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
    deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
    PRIMARY KEY(packageUID),
    FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

```

```

/* Access Control オブジェクトのデータ ( ACE Master に関連付けられた、リストの単一項目 ) */
CREATE TABLE PolicyDb_Access (
    accessPK VARCHAR(128), /* 固有 ID (プライマリ キー) */
    aceUID VARCHAR(128), /* このアクセス ポリシーの対象の ACE (FK) */
    identityData VARCHAR(128), /* 内部表記、AD 統合を使用する場合の SID、 */
    /* トークンの値がここに格納される。 */
    accVersion INTEGER NOT NULL, /* Access オブジェクトのバージョン番号 */
    identityType INTEGER NOT NULL, /* AD ユーザー、グループ、またはトークンの値 */
    identityName VARCHAR(128), /* AD 統合を使用する場合の UI に表示されるユーザー / グループ名 */
    accUseInstanceLimit VARCHAR(7)
        DEFAULT 'FALSE' NOT NULL, /* この ID に対してインスタンス数を制限するか ? */
    accInstanceLimit INTEGER NOT NULL, /* 許可される ACE インスタンスの最大数 */
    accTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
    accTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
    deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 ( 廃棄 ) されたか */
    PRIMARY KEY(accessPK),
    FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Instance オブジェクトのデータ */
CREATE TABLE PolicyDb_Instance (
    instanceUID VARCHAR(128), /* VM インスタンス ID (プライマリ キー) */
    packageUID VARCHAR(128) NOT NULL, /* 所属先のパッケージ */
    aceUID VARCHAR(128) DEFAULT '' NOT NULL, /* 所属先の ACE Master */
    creatorIdName VARCHAR(128) NOT NULL, /* アクティベーションしたユーザーの表示名 */
    creatorIdData VARCHAR(256), /* アクティベーションしたユーザーの完全修飾名 */
    creatorAuthType INTEGER NOT NULL, /* アクティベーション時のアクセス チェックの種類 */
    activationDate VARCHAR(21) NOT NULL, /* アクティベーションされた日時 */
    lastPolicyCheck VARCHAR(21) NOT NULL, /* PLayer がサーバに対して最後に呼び出しを行った日時 */
    revocationDate VARCHAR(21) NOT NULL, /* インスタンスがアクティベーション解除された日時 */
    replacementDate VARCHAR(21) NOT NULL, /* コピー保護が理由で置き換えられた日時 */
    /* ポリシー */
    inheritsExpiration
        VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* Use expiration info from Policy Set */
    insUseValidDates
        VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* 有効期限を使用、または常に有効 */
    insValidDateStart VARCHAR(21) NOT NULL, /* インスタンスの有効期限開始日 */
    insValidDateEnd VARCHAR(21) NOT NULL, /* インスタンスの有効期限終了日 */
    insPassword VARCHAR(128), /* AD を使用しない場合のログイン パスワード */
    /* このインスタンスの認証用 */
    hostName VARCHAR(128), /* VM が稼働しているホスト PC の名前 */
    hostIp VARCHAR(128), /* VM が稼働しているホストの IP アドレス */
    insProtectionKey VARCHAR(1024), /* インスタンスの VM ディスクの暗号化キー */
    copyProtectionId VARCHAR(1024), /* コピーの場所を格納 */
    insPreview VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* プレビュー インスタンスか */
    guestIpAddress VARCHAR(128) DEFAULT '', /* レポートされた VM の IP アドレス */
    guestMacAddress VARCHAR(128) DEFAULT '', /* 割り当てられた VM の MAC アドレス */
    guestMachineName VARCHAR(128) DEFAULT '', /* ゲスト ( VM ) OS のホスト名 */
    guestConfigStatus INTEGER DEFAULT 0, /* ゲストの自動構成の */

```

```

/* 実行状況 */
guestConfigMsg VARCHAR(512), /* ゲストの自動構成のメッセージ */
insTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
insTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
insCustom1 VARCHAR(255), /* ユーザー定義フィールド */
insCustom2 VARCHAR(255), /* ユーザー定義フィールド */
insCustom3 VARCHAR(255), /* ユーザー定義フィールド */
insCustom4 VARCHAR(255), /* ユーザー定義フィールド */
insCustom5 VARCHAR(255), /* ユーザー定義フィールド */
insCustom6 VARCHAR(255), /* ユーザー定義フィールド */
insCustom7 VARCHAR(255), /* ユーザー定義フィールド */
insCustom8 VARCHAR(255), /* ユーザー定義フィールド */
insCustom9 VARCHAR(255), /* ユーザー定義フィールド */
PRIMARY KEY(instanceUID),
FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* MAC アドレス プール (将来使用するために予約済み) */
CREATE TABLE PolicyDb_MacPool (
  macPoolUID VARCHAR(128), /* プライマリ キー */
  aceUID VARCHAR(128) NOT NULL, /* この MAC プールが使用される ACE */
  macPoolName VARCHAR(128), /* ユーザーに表示される名前 */
  description VARCHAR(128), /* MAC プールの名前および説明 */
  rangeStart VARCHAR(21) NOT NULL, /* MAC プールの開始アドレス */
  rangeEnd VARCHAR(21) NOT NULL, /* MAC プールの終了アドレス */
  lastAssigned VARCHAR(21) NOT NULL, /* 最後に割り当てられたアドレス */
  mp1TsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
  mp1TsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
  deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
  PRIMARY KEY(macPoolUID),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* インスタンスのカスタマイズ データ */
CREATE TABLE PolicyDb_UserData (
  userDataPK VARCHAR(516), /* プライマリ キー */
  aceUID VARCHAR(128), /* このユーザー データが定義されている ACE */
  packageUID VARCHAR(128), /* このユーザー データが使用されているパッケージ */
  activator VARCHAR(128), /* ユーザー */
  udataName VARCHAR(128), /* ユーザー データ エントリ名 */
  udataType INTEGER NOT NULL, /* 日付の属性 */
  udataValue VARCHAR(2048), /* ユーザー データ エントリの値 */
  udtTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
  udtTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
  deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID),
  FOREIGN KEY(packageUID) REFERENCES PolicyDb_Package(packageUID),
  PRIMARY KEY(userDataPK));

```

```

/* ACE Master のポリシー セット */
CREATE TABLE PolicyDb_RuntimePolicy (
  aceUID VARCHAR(128), /* 所属先の ACE */
  policyVersion INTEGER, /* この ACE の RT ポリシーのバージョン */
  clientPolicyData VARCHAR(2000), /* ゲスト OS のランタイム ポリシー */
  clientPolicyDataExtKey VARCHAR(128), /* 長すぎる場合は LongField テーブルに格納 */
  hostPolicyData VARCHAR(2000), /* ホスト OS のランタイム ポリシー (NQ) */
  hostPolicyDataExtKey VARCHAR(128), /* 長すぎる場合は LongField テーブルに格納 */
  expirationType INTEGER NOT NULL, /* 有効期限のタイプ (enum) */
  expValue_1 VARCHAR(21) NOT NULL, /* 有効期限の値 (タイプに応じて変化) */
  expValue_2 VARCHAR(21) NOT NULL, /* 有効期限の値 (タイプに応じて変化) */
  cacheLifetime VARCHAR(21) NOT NULL, /* サーバへのアクセスなしで使用できる期間 */
  rtpInstType INTEGER NOT NULL, /* インスタンス化の認証チェックのタイプ */
  rtpAuthType INTEGER NOT NULL, /* ランタイムの認証チェックのタイプ */
  rtpUseInstanceLimit VARCHAR(7)
    DEFAULT 'FALSE' NOT NULL, /* この ACE に対してインスタンス数を制限するか ? */
  rtpInstanceLimit INTEGER NOT NULL, /* 許可される ACE インスタンスの最大数 */
  rtpUsePerUserInstanceLimit VARCHAR(7)
    DEFAULT 'FALSE' NOT NULL, /* ユーザーあたりのインスタンス数を制限す
    るか ? */
  rtpPerUserInstanceLimit INTEGER NOT NULL, /* ユーザーあたりの ACE インスタンスの最大数 */
  copyPolicy INTEGER DEFAULT 0 NOT NULL, /* VM インスタンスがコピーされた場合の動作 */
  published VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* 公開済みポリシー (更新はロックされ
    ている) */
  rtpTsCreated VARCHAR(21) DEFAULT 0 NOT NULL, /* 作成時のタイムスタンプ */
  rtpTsLastModified VARCHAR(21) DEFAULT 0 NOT NULL, /* 最終更新時のタイムスタンプ */
  deleted VARCHAR(7) DEFAULT 'FALSE', /* このエントリが削除 (廃棄) されたか */
  PRIMARY KEY (aceUID, policyVersion),
  FOREIGN KEY(aceUID) REFERENCES PolicyDb_Ace(aceUID));

/* ACE Management Server 情報 - 将来使用するために予約済み */
CREATE TABLE PolicyDb_AcescServer (
  serverHostname VARCHAR(128), /* サーバ コンピュータのホスト名 */
  serverPort INTEGER, /* サーバが待機している TCP ポート番号 */
  secure VARCHAR(7) DEFAULT 'FALSE' NOT NULL, /* HTTPS が有効化されているかどうか */
  sslCertificateExtKey VARCHAR(128), /* SSL 証明書データ、格納されている */
  /* LongField テーブルへのキー */
  sslCertificateChainExtKey VARCHAR(128), /* SSL 証明書チェーンのデータ、 */
  /* 格納されている LongField テーブルへのキー */
  PRIMARY KEY (serverHostname, serverPort));

/* 監査イベント ログのイベント タイプのルックアップ テーブル */
CREATE TABLE PolicyDb_EventType (
  eventType INTEGER, /* イベント タイプ コード (PK) */
  eventMessage VARCHAR(1024), /* このイベント タイプの表示可能メッセージ */
  eventCategory INTEGER, /* イベント カテゴリ コード */
  eventCategoryName VARCHAR(128), /* イベント カテゴリの表示可能名 */
  eventLogLevel INTEGER, /* イベント ログのレベル */
  PRIMARY KEY (eventType));

```

```

/* 監査イベント ログのデータ */
CREATE TABLE PolicyDb_Event (
    eventUID INTEGER, /* テーブルのプライマリ キー ( 順次 ) */
    eventTs VARCHAR(21), /* イベントが作成されたタイムスタンプ ( マイクロ秒
        単位 ) */
    loginName VARCHAR(128), /* アクティベーションしたユーザーのログイン
        ユーザー名 */
    aceUID VARCHAR(128), /* イベントの影響を受ける ACE の UID */
    packageUID VARCHAR(128), /* イベントの影響を受けるパッケージの UID */
    instanceUID VARCHAR(128), /* イベントの影響を受けるインスタンスの UID */
    policyVersion INTEGER, /* イベントの影響を受ける ACE ポリシーのバージョン */
    eventCategory INTEGER, /* EventType で定義されたイベント カテゴリ */
    eventType INTEGER, /* EventType で定義されたイベント タイプ */
    sessionID VARCHAR(128), /* ACE Server のセッション ID */
    clientIP VARCHAR(128), /* クライアント マシンの IP アドレス ( 予約済み ) */
    serverIP VARCHAR(128), /* ACE Server の IP アドレス ( 予約済み ) */
    turnaroundTime VARCHAR(21), /* サーバ側の実行時間 ( ミリ秒 ) */
    handlerName VARCHAR(128), /* ClientLib ハンドラの名前 ( デバッグ ) */
    returnCodeText VARCHAR(128), /* クライアントに返されたテキスト エラー コード */
    messageParams VARCHAR(1024), /* タブ区切り形式のイベント データ リスト */
    prevEventUID INTEGER UNIQUE, /* 以前に記録されたイベントの UID */
    eventSignature VARCHAR(128), /* サーバ キーにより署名された、イベントの署名 */
    FOREIGN KEY(eventType) REFERENCES PolicyDb_EventType(eventType),
    FOREIGN KEY(prevEventUID) REFERENCES PolicyDb_Event(eventUID),
    PRIMARY KEY (eventUID));

```

監査イベント ログのデータのクエリ

ACE Server コンポーネントを使用すると、サーバが実行するすべてのトランザクションの監査記録を作成できます。このシステムを使用して、使用状況、セキュリティ違反、ポリシーのエラー、パフォーマンスなどを監視できます。

ACE Server コンポーネントのイベント ログ インフラストラクチャは、パフォーマンスが低下してシステムに影響を及ぼすことなく、必要に応じて詳細なロギングを提供できる十分な柔軟性を備えています。

イベント ログ メカニズムでは十分な情報が収集され、以下の疑問への回答を得ることができます。

- どのユーザーがインスタンスをアクティベーションしたか。
- インスタンスはいつアクティベーションされたか。
- どのユーザーがインスタンスをアクティベーション解除したか。
- どのユーザーがコピー保護ポリシーをオフにしたか。
- ポリシーに対して、いつ、どのような変更が加えられたか。
- どのユーザーが認証に失敗しているか。

このメカニズムでは、必ずしもこれらの疑問への回答を直接的に得られるわけではありませんが、管理者に対して、イベント ログを参照して回答を得ることのできる十分なデータを提供します。ログに記録されるデータは、以下の要件を満たしています。

- 処理された各トランザクションについての詳細な情報を提供する。
- 複数のサーバを使用している場合に、イベント ログのデータの収集を一元化する。
- ログ収集対象のトランザクション タイプを管理者が選択できる。
- 必要に応じて、収集するログ情報の量を増やしたり、減らしたりするように構成できる。

この監査記録の一部は、すでに本製品の他の機能において、目に見える形で使用されています。たとえば、インスタンス ビューには、最後にポリシーの**取得**操作が行われた日時や有効期限などが表示されます。イベント ログ メカニズムでは、たとえば、どの管理者がどのポリシーを変更したか、どの管理者がどの ACE インスタンスを削除したか、などの難しい疑問点に対する回答を得ることができます。

表 A-1 は、ログ エントリに格納されるデータを示しています。

表 A-1 ログ エントリのデータ

データ	説明
監査ログ イベント ID (PK)	増分する整数
ログのタイムスタンプ	1970 年 1 月 1 日の午前 0 時から起算したマイクロ秒の値を、10 進形式のストリングとして格納
ログオン ユーザー名	
影響を受ける ACE の UID (FK)	
影響を受けるパッケージの UID (FK)	
影響を受けるインスタンスの UID (FK)	
影響を受けるポリシー セットのバージョン	
イベント カテゴリ	Auth、AceAdmin、PkgAdmin、PolicyAdmin、InstAdmin
イベント タイプのコード (FK)	PolicyDb_EventType テーブルを参照
セッション ID	デバッグ
受信 IP アドレス	将来使用するために予約済み
サーバ IP アドレス	将来使用するために予約済み
処理にかかった時間	サーバで費やされた時間 (マイクロ秒)

表 A-1 ログ エントリのデータ (続き)

データ	説明
処理のハンドラ名 (デバッグ)	
戻りコードのテキスト	成功、失敗、特定のエラー
メッセージパラメータ	タブ区切り形式のリスト
無許可でのレコードの削除や挿入を防ぐための、直前のイベントの UUID	ログの整合性
レコードが変更されたかどうかを示すための、サーバキーを使用したイベントレコードのハッシュ	ログの整合性

ACE、パッケージ、インスタンスの各 UID、およびポリシーのバージョンは、ACE Server オブジェクトのスペース内でのログ イベントの座標を提供します。これは、システムの状態とイベントを関連付けるうえで役立ちます。データベース クエリ ツールを使用すると、特定の ACE インスタンスに影響を及ぼしたすべての ACE 管理 イベントを、そのイベントが作成された時点から削除された時点まで追跡できます。

あらゆるイベントに対して、すべて座標が存在するわけではありません。たとえば、パッケージの有効期限の更新がログに記録される場合、インスタンスの UID フィールドは設定されません。これは、パッケージ内の全インスタンスに影響を受けるためです。

データベース内の他の場所で永続的に格納されているデータが不変のデータである場合は、ログ エントリ内には複製されません。たとえば、新しいポリシーが公開された場合、そのポリシー テキスト全体がログ エントリに組み込まれることはありません。その代わりに、ポリシーのバージョン番号が参照されるため、必要な場合に PolicyDb_RuntimePolicy テーブルと PolicyDb_Access テーブルからイベントの完全なデータを復元できるようになります。

注意 ACE Management Server では、パスワードや暗号化キーなどの機密データはログに記録しません。

イベント タイプ コードはルックアップテーブル PolicyDb_EventType に関連付けられています。このテーブルには、各イベント タイプごとのテキスト メッセージのテンプレート、カテゴリ、およびイベントのログ レベルが含まれています。メッセージには、パラメータのプレースホルダ (**%s**) が含まれている場合があります。この場合、ログ エントリの [メッセージパラメータ] フィールドには、これらのパラメータの値のリスト (タブ区切り形式) が含まれます。たとえば、タイプ 4110 のインスタンス管理イベントでは、メッセージは次のようになります。

4110 -> "Instance Set Guest Info が要求されました。IP アドレス = %s、MAC アドレス %s、構成メッセージ ¥"%s¥"、マシン名 ¥"%s¥"、構成ステータス %s"

この例では、[メッセージパラメータ]フィールドの表示は次のようになります。

10.17.0.3 00:0C:29:1A:2B:3C OK ACETest 0

実際のパラメータによって、メッセージテンプレート内の%s プレースホルダが置き換えられます。

ACE Management Server のイベント ログには、改ざん証拠機能が試験的に組み込まれています。イベント ログ内のすべてのレコード（最初の1件を除く）には直前のイベントへの固有の参照がなければならず、さらに、この機能はデータベースの外部キーと固有制約によって強化されています。後続の各レコードには値が1ずつ増分された固有 ID が付けられるため、欠落しているレコードがある場合はすぐに分かります。データベースへの直接アクセス権を持つユーザーがレコードを変更、追加、または削除する場合には、そのユーザーは、直前のイベントのポインタか、残りのイベントレコード内の他のデータのいずれかを変更する必要があります。各レコード内のデータはサーバキーによってハッシュ化され、[eventSignature] フィールドに格納されます。

イベントのカテゴリ、カテゴリごとのイベント ログのレベルの構成、および古いイベントの消去によるテーブルサイズの抑制については、「[イベントのログギ](#) (P.54)」を参照してください。

用語集

ACE Management Server

ACE インスタンスのアクティベーションと追跡、および ACE インスタンス用の動的ポリシーのホスティングを行うために、ACE 管理者がインストールして使用できるサーバです。

ACE インスタンス

ACE 管理者が作成し、仮想権利マネジメント (VRM) ポリシーへの関連付けを行い、パッケージしてユーザーにデプロイする仮想マシンです。

ACE 有効仮想マシン

ACE 管理者が作成する仮想マシン テンプレートです。この仮想マシンは、さまざまなポリシー、デバイス、およびデプロイ設定で構成できます。構成後、これをベースとして使用して、ACE ユーザーに送信するパッケージを作成できます。VMware ACE の以前のバージョンでは、このテンプレートは ACE Master と呼ばれていました。

VMware Player

ユーザーが ACE インスタンスを実行するために使用できる、シンプルなアプリケーションです。

VMware Tools

ゲスト OS のパフォーマンスと機能性を向上させるユーティリティおよびドライバのパッケージです。VMware Tools の主な機能は、ゲスト OS の種類によって多少異なりますが、SVGA ドライバ、マウス ドライバ、VMware Tools コントロールページなどが含まれ、フォルダの共有、仮想ディスクの圧縮、ホストとの時刻同期、VMware Tools スクリプト、および ACE インスタンスの実行中のデバイスの接続または切断といった機能をサポートします。

Workstation

ACE パッケージの作成、デプロイ、更新、および ACE インスタンスの管理を行うために、管理者が使用するプログラムです。従来の「VMware ACE Manager」または「VMware Workstation ACE Edition」です。

アクティベーション

パッケージの保護および ACE インスタンスのランタイム認証ポリシーの設定を含む、ACE インスタンスのセットアップステップの 1 つです。アクティベーションが正常に完了すると、パッケージされた仮想マシンは、ポリシーおよび他の設定が適用されて ACE インスタンスとなります。アクセス コントロール ポリシーのアクティベーション設定によって、インストールされた ACE パッケージにアクセスしてこれを ACE インスタンスに変更できるユーザーが決まります。「[認証](#)」も参照。

インスタンスのカスタマイズ

ACE インスタンスをカスタマイズして、他のすべてのインスタンスとは異なるインスタンスにする作業を指します。インスタンスのカスタマイズ プロセスは、Microsoft Sysprep ユーティリティのアクションを自動化します。また、ACE 管理者に対して、企業の VPN ネットワークに対する ACE インスタンスの自動リモートドメイン参加プロセスのセットアップに必要な機能を提供します。

仮想マシン

ゲスト OS と関連アプリケーションソフトウェアの実行が可能な、仮想化された x86 PC 環境です。ポリシーおよびその他の設定が関連付けられた ACE 有効仮想マシンは、ACE インスタンスと呼ばれます。「[ACE インスタンス](#)」も参照。

管理対象 ACE インスタンス

ACE Management Server が管理する ACE インスタンスです。「[ACE Management Server](#)」も参照。

ゲスト OS

ACE インスタンス内で実行されるオペレーティングシステムです。「[ホスト OS](#)」も参照。

公開

ACE インスタンスがポリシーの更新スケジュールに従ってポリシーを受信できるように、ACE Management Server 上でポリシーを使用可能にするプロセスです。「[ポリシー](#)」も参照。

スタンドアロン ACE インスタンス

ACE Management Server によって管理されない ACE インスタンスです。スタンドアロン ACE インスタンスのポリシーや他の設定に対する変更はすべて、管理者がユーザーに更新を配布することによって行われます。

デプロイ設定

インスタンスのカスタマイズの設定など、パッケージに関連付けられたルールおよび設定のセットです。これらの設定は、パッケージ作成後には変更できません。デプロイ設定を変更するには、新たにパッケージを作成する必要があります。

認証

インスタンスの保護を含む、ACE インスタンスのセットアップステップの1つです。認証ステップが正常に完了すると、ユーザーはインスタンスを実行できます。「[アクティベーション](#)」も参照。

パッケージ

ユーザーに配布する、インストール可能なバンドルです。フルパッケージには、ACE 有効仮想マシンの構成ファイル、仮想ディスク ファイル、ポリシー、パッケージ インストーラ、およびリソース ファイルが含まれます。また、ACE インスタンスの実行に使用される VMware Player アプリケーションも含まれます。

プレビュー

管理者が使用できる操作および表示モードの1つで、ユーザーのマシン上で ACE インスタンスを実行した場合の状態をプレビューするために使用します。管理者はこの機能を使用することで、パッケージ作成およびデプロイのステップを実行せずに、ポリシーや構成の設定の効果を確認できます。

ホスト OS

ホスト マシン上で実行される OS です。「[ゲスト OS](#)」も参照。

ホスト コンピュータ

VMware Player ソフトウェアがインストールされている物理コンピュータです。ACE インスタンスをホスティングします。

ホットフィックス

ユーザーのパスワードの再設定を行ったり、期限切れの仮想マシンを更新したり、コピー保護機能が適用されている仮想マシンを新しい場所から実行できるようにする、インストール可能なファイルです。

ポリシー

ACE インスタンスの機能を制御する公式なガイドライン セットです。ポリシーは、Workstation のポリシー エディタで設定します。「[公開](#)」も参照。

インデックス

A

- ACE Management Server
 - Linux ホスト上の ACE インスタンスの接続に関する問題の解決 75
 - Active Directory ユーザーとグループの作成 42
- ACE インスタンス
 - Linux ホスト上の、サーバへの接続に関する問題の解決 75
- ACE Management Server
 - Active Directory 統合 19
 - Active Directory ユーザーとグループの作成 41、42
 - Linux システムへのインストール 32
 - Windows システムへのインストール 31
 - インストール 31
 - インストール オプション 31
 - 外部データベース オプション 18
 - 監査イベント ログのデータのクエリ 82
 - 構成 41
 - 手動での停止と起動 36
 - 使用 65
 - シリアル番号 50
 - データベース スキーマ 82
 - データベースのバックアップ 80
 - デフォルトのポート割り当て 31
 - 特徴 11
 - 内蔵データベース 18
 - ハードウェア要件 13
 - ポート割り当ての変更 76
 - ライセンス 50
 - ログイン 38
- ACE Management Server のインストール 31
- ACE Management Server の再起動 55
- ACE Management Server の使用 65
- ACE Management Server のポート 76
- ACE Management Server へのログイン 38
- ACE Management Server 用 SQLite データベース 18
- ACE Management Server 用データベース 18
- ACE インスタンス
 - セキュリティ証明書 23
 - ログ イベント 54
- ACE インスタンスのアクティベーション解除 72
- ACE インスタンスの再アクティベーション 72
- Active Directory
 - ACE Management Server で使用するグループの作成 42
 - ACE Management Server で使用するユーザーの作成 42
 - ACE Management Server との統合 19
 - ログイン オプション、ACE Management Server 38

H

- Help Desk
 - [インスタンス] ページ 66
 - 高度なインスタンス クエリ 68
 - 使用 66
- Help Desk アプリケーションのトラブルシューティング 66
- Help Desk でのインスタンスの検索 68
- Help Desk の [インスタンスの詳細] ページ 71

L

- LDAP
 - Active Directory を参照

S

- SSL 証明書、使用 22、23
- SSL プロトコル、使用 22、23

V

- VMware Player
 - Linux ホスト上の ACE Server の接続に関する問題の解決 75
- VMware コミュニティ フォーラム
 - アクセス 9

い

- イベントのロギング 54
- インスタンス ビュー
 - 詳細 71
- インスタンスの詳細の表示 71
- インスタンスの詳細、表示 71
- [インスタンスの詳細] ページ 71
- インスタンス クエリ 68
- インスタンスの並べ替え 69
- インスタンスのパスワードのリセット 73

インスタンス ビュー

- カスタム フィールド 70
- 列のカスタマイズ 70
- インスタンス ビューのカスタム フィールド 70
- [インスタンス] ページ 66

か

- 監査イベント ログのデータ、クエリ 87

こ

- 構成
 - ACE Management Server インスタンス 41
- コピー保護 ID の変更 72
- コピー保護、ID の変更 72

さ

- [再起動] ページ 55
- [再起動] ページの構成 55

し

- 時刻の同期 (注) 30
- 手動での Apache サービスの停止と起動 36
- 証明書、セットアップ 49

せ

- セキュリティ、SSL 22、23

て

- データベース
 - ACE 用 18
 - 外部 18
 - バックアップ 80

な

- ナレッジベース
 - アクセス 9

は

パスワード、リセット

ACE Management Server の
管理者パスワード 77

ACE インスタンス 73

ほ

ポート割り当て、デフォルト 31

ゆ

有効期限、変更 72

ユーザー グループ

アクセス 9

ら

ライセンス、ACE Management
Server 50

れ

列の見出し、並べ替え方法 69

