CHAPTER 1

ACS 5.3 展開の概要

ACS 5.3 展開モデルは ACS 4.x と似ており、単一のプライマリ ACS サーバと複数のセカンダリ ACS サーバから構成され、設定の変更はプライマリ ACS サーバで行います。これらの設定はセカンダリ ACS サーバに複製されます。

すべてのプライマリおよびセカンダリ ACS サーバで AAA 要求を処理できます。プライマリ ACS サーバは Monitoring and Report Viewer のデフォルトのログ コレクタでもありますが、任意の ACS サーバをログ コレクタに設定することができます。

1 台の ACS サーバで管理できますが、複数の ACS サーバを使用して、AAA 要求の処理の冗長性を備えることをお勧めします。ACS 5.3 は外部ログ用の syslog のサポートと、自動およびバッチ設定プロビジョニング用のインターフェイスを備えています。

ACS 展開は、セカンダリ サーバを追加することによって、AAA 要求の処理容量の増加に合わせて拡大できます。大規模な展開では、セカンダリ サーバを特定機能専用にすることができます。たとえば、プライマリ ACS サーバを設定の変更専用に使用し、AAA 要求の処理に使用しないようにすることもできます。セカンダリ ACS サーバをログ コレクタとしてのみ指定することができます。

大規模環境では、ロード バランサを使用して、展開内の ACS サーバ間で AAA 要求を分散し、AAA クライアント管理を簡単にして、高可用性を実現できます。

ACS サーバは一般にデータセンターや地域のサイトなどのユーザ クラスタの近くに配置します。

その他の展開情報については、『*Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3*』の「Understanding the ACS Server Deployment」を参照してください。

表 1-1 にさまざまな ACS サーバの役割について説明します。

表 1-1　　ACS サーバの役割

ACS サーバの役割	役割の説明
プライマリ	プライマリ ACS サーバで実行した設定の変更は、展開内のすべてのセカンダリ ACS サーバに複製されます。プライマリ サーバとして使用できる ACS サーバは一度に 1 台だけです。
セカンダリ	ACS プライマリ サーバからの設定の変更を受け取るすべての ACS サーバはセカンダリ サーバです。
ログ コレクタ	Monitoring and Report Viewer のログ コレクタでもある ACS プライマリまたはセカンダリ サーバ。展開に配置できるログ コレクタは 1 台だけです。 他の ACS 展開（この展開と同期されないサーバ）は ACS ログをこのサーバに送信できません。

次の項では、ACS 4.x と ACS 5.3 の展開の違い、および ACS 5.3 を展開する場合のいくつかの考慮事項について説明します。

Windows と Linux ベースのアプリケーション

ACS 3.x および 4.x リリースは Windows サーバ プラットフォームにインストール可能な Windows ベースのアプリケーションとして使用できます。これらのアプリケーションは ACS Solution Engine と呼ばれるアプライアンスでも使用できます。このアプライアンスは ACS と Windows オペレーティング システムが事前ロードされているハードウェア プラットフォームです。

ACS 5.3 は Linux フレーバーのアプリケーションで Linux オペレーティング システムにパッケージされています。アプリケーションとオペレーティング システム パッケージはアプライアンスに同梱されており、VMware ESX Server 上の仮想マシンにもインストールできます。

ACS for Windows と ACS Solution Engine には機能と展開の違いがありますが、ACS 5.3 ハードウェア アプライアンスと仮想マシンにインストールされた ACS 5.3 には機能の違いがありません。ACS 5.3 ハードウェア アプライアンスと ACS 5.3 仮想マシンから構成される展開もサポートされます。

レプリケーション

ACS 3.x および 4.x は緩いレプリケーション モデルを提供します。ACS 3.x および 4.x レプリケーション モデルの特性を次に示します。

- 設定ブロックは ACS 設定の論理領域を表します。たとえば、ユーザとユーザグループ、ユーザグループのみ、ネットワーク デバイス、配布テーブル、インターフェイス設定、インターフェイス セキュリティ設定、パスワード検証設定、EAP-FAST 設定、ネットワーク アクセス プロファイル、ログ設定などです。
- プライマリ サーバからセカンダリ サーバに 1 つ以上の設定ブロックを複製するオプション。
- 設定の変更のサイズに関係なく、ブロック全体が複製されます。
- カスケード レプリケーション。これは、セカンダリ ACS サーバがレプリケーションの更新を別の ACS サーバにプッシュする機能です。
- レプリケーションは手動またはスケジュールに従って起動できます。
- TACACS+ パスワードの更新は、プライマリ サーバでのみ受け取ります。

この緩いレプリケーション モデルでは、プライマリ サーバとセカンダリ サーバ間で複製されたブロックが同期されますが、設定の他の部分は異なることがあり、ローカル環境に合わせてカスタマイズできます。

ACS 5.3 のレプリケーション モデルは単純で効率的かつ堅牢です。ACS 5.3 レプリケーション モデルの特性を次に示します。

- プライマリ サーバとセカンダリ サーバ間の完全同期。
- 透過的で即座のレプリケーション。
- 設定の変更のみが複製されます。
- 設定の変更はプライマリ サーバでのみ実行できます。
- カスケード レプリケーションはありません。
- 欠落した更新の自動リカバリ。
- セカンダリ サーバをプライマリ サーバにプロモートする機能。
- TACACS+ パスワードの更新は任意の ACS インスタンスで受け取ることができます。

ACS 5.3 ネットワーク アクセス ポリシー設定で地域固有のアクセス ポリシーを実装する必要があります。これは、ACS 5.3 の設定がプライマリ サーバとセカンダリ サーバで完全に同期され、直接セカンダリ サーバに対して設定を変更することができないためです。

ID ストア

ACS 3.x および 4.x と 5.3 の ID ストアのサポートに関する主な違いは、ACS 5.3 では、データベースへの認証に ODBC がサポートされないことと、TACACS+ 要求のプロキシ転送がサポートされないことです。ACS 5.3 では、認証に次の ID ストアがサポートされます。

- ACS 内部ストア
- Active Directory
- LDAP ディレクトリ
- 次を使用したワンタイム パスワード サーバ
  - RSA SecurID インターフェイス
  - RADIUS インターフェイス
- RADIUS による他のストアへのプロキシ転送（RADIUS プロキシ）

ロギング

ACS 5.3 では、Monitoring and Report Viewer 機能が ACS に含まれます。ACS 5.3 展開では、ACS サーバがレポートおよび監視機能のログ コレクタとして指定されます。その他のすべての ACS サーバは指定されたログ コレクタにログ メッセージを送信します。

ACS は外部サーバへのログ用に syslog をサポートしています。

ACS 5.3 は Monitoring and Report Viewer からユーザ認証情報を取得するための Cisco Wireless Control System（WCS）の Web サービス インターフェイスを備えています。

設定

ACS 5.3 では、設定のプライマリ モードは Web ベースのユーザ インターフェイスです。ACS 5.3 にはシステム タスクとファイルベースの設定の更新を実行できるコマンドライン インターフェイス（CLI）もあります。

CLI には、コンソール ポート、キーボード、ビデオ、マウス（KVM）、SSH からアクセスできます。内部 ACS ユーザ向けにパスワード変更アプリケーションを開発するための Web サービス インターフェイスが提供されています。

表 1-2 に ACS でサポートされる内部ユーザとネットワーク デバイスの数を示します。ユーザとネットワーク デバイスは一般的に使われ、広く読み込まれる ACS オブジェクトです。

表 1-2　内部ユーザとデバイスの設定の容量

ACS オブジェクト	設定の容量
内部ユーザ	300,000
ネットワーク デバイス	50,000

ライセンス

ACS の 3.x および 4.x リリースには、キーまたはライセンス ファイルを適用する必要がありませんでした。しかし、5.x リリースにはライセンス ファイルの適用が必要です。ACS 5.3 ライセンスは、http://cisco.com/go/license で入手できます。

表 1-3 に使用可能な ACS 5.3 ライセンスを示します。

表 1-3　使用可能な ACS 5.3 ライセンス

ライセンス	説明
Base Server	各 ACS インスタンスに 1 つ。
Large Deployment	ACS のネットワーク デバイス数（IP アドレスに基づく）が 500 を超える場合、各 ACS 展開に 1 つ。 Default Network Device を設定すると、デバイス数に影響します。

サーバの展開の推奨事項

表 1-4 に ACS 3.x および 4.x から ACS 5.3 へのコンポーネントのマッピングを示します。

表 1-4　コンポーネントのマッピング

ACS 3.x および 4.x コンポーネント	ACS 5.3 コンポーネント	変更点
ACS for Windows	VMware ESX の VM または 1120/1121 アプライアンス	ACS 5.3 Windows オプションはありません。ACS 5.3 は VMWare またはサポート対象のアプライアンスで実行できるアプリケーションです。
ACS Solution Engine（1111、1112、1113）	VMware ESX の VM または 1120 または 1121 アプライアンス	ACS 1111、1112、および 1113 プラットフォームは ACS 5.3 をサポートしていません。ACS 4.2 は 1120 で実行できます。
ACS Remote Agent	該当なし	ACS 5.3 では Remote Agent は必要ありません
ACS View 4.0	VMware ESX の VM または 1120/1121 アプライアンス	ACS 5.3 には ACS View 機能が組み込まれています。

ACS 5.3 の展開のガイドライン

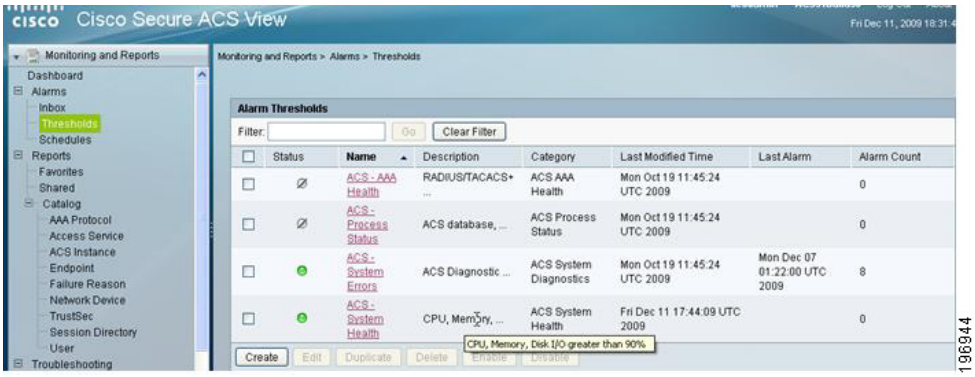
- ほとんどの場合に、1 対 1 の ACS サーバ置換が適切です。

  ACS 5.3 の認証パフォーマンスは以前のバージョンと同じです。
- 冗長性を提供するために、少なくとも 2 つの ACS インスタンスを展開します。
- 認証パフォーマンスを拡張するには、ACS サーバを追加します。

  1 台の ACS サーバでその AAA クライアントと、バックアップ AAA サーバとしてそれに依存するすべての AAA クライアントのピークの認証レートを処理できることを確認します。
- 展開環境を拡大するために、AAA 要求のみを処理するセカンダリ ACS サーバを使用することができます。プライマリは設定の更新とログの収集にのみ使用します。

  ログ コレクタには最も強力なハードウェアを使用します。たとえば、1120 アプライアンスよりも 1121 アプライアンスを使用します。
- ロード バランサを使用して、AAA 要求を受け取り、AAA クライアントの管理を簡単にし、耐障害性を向上して、ACS 認証容量を有効に利用します。
- 実行中のリソースの使用状況を監視します。これは、図 1-1 に示すように、Monitoring and Report Viewer の ACS システム健全性アラームしきい値を有効にすることによって実行できます。

図 1-1　　ACS 5.3 のアラームしきい値



パフォーマンス

ログ コレクタとして動作しない単一の ACS 5.3 サーバは 1 秒あたり 100 を超える認証を処理できます。AAA 要求を処理する単一の ACS サーバでピーク時間の負荷を管理できることを確認する必要があります。ピーク時間は、一般にユーザの始業時やネットワーク機器の再起動時に発生します。これにより、大量の認証要求が作成されます。

たとえば、15 分間に 50,000 人の社員がネットワークに均等にログインします。これは、ピーク認証レートとして、1 秒あたり約 56 の認証に換算されます。この場合、ログ コレクタとして動作しない単一の ACS サーバでこのピーク認証レートをサポートできます。

表 1-5 に、最小レートが 1 秒あたり 100 認証として、さまざまな期間での 1 台の ACS サーバでサポートできる認証数を示します。

表 1-5　　さまざまな期間での認証

1 秒	100 認証
60 秒	6,000 認証
5 分	30,000 認証
15 分	90,000 認証
1 時間	360,000 認証

ACS 認証パフォーマンスに影響する要因は、設定サイズ、ポリシーの複雑さ、外部サーバとの通信、認証プロトコルの複雑さなどたくさんあります。

表 1-6 にさまざまな認証環境での ACS のパフォーマンスを示します。このパフォーマンス データは、複雑な設定を使用する ACS をテストした場合に観察された低い範囲の認証レートを示しています。簡単な設定の場合はパフォーマンスが高くなります。

表 1-6　低い範囲の ACS 5.3 認証パフォーマンス（認証数/秒）

認証タイプ	ID ストア		
	内部	AD	LDAP
PAP	500	100	800
CHAP	500	500	該当なし
TACACS+	400	160	1200
MSCHAP	500	300	該当なし
PEAP-MSCHAP	200	100	該当なし
PEAP-GTC	200	100	300
EAP-TLS	200	180	270
LEAP	330	280	該当なし
FAST-MSCHAP	120	120	該当なし
FAST-GTC	130	110	190
MAC 認証バイパス	750	該当なし	2000

（注）　上の数値は、該当する EAP モジュールに高速再接続およびセッション再開が使用されていることを前提としています。

ACS サーバを Monitoring and Report Viewer のログ コレクタとしても使用する場合、認証パフォーマンスは約 50 % 低下します。

CSACS 1121 アプライアンスでは、表 1-6 に示す数値よりもパフォーマンスが約 10 % ～ 15 % 向上します。

仮想マシンでのパフォーマンスは、仮想マシンのオーバーヘッドのため、実際の 1120 アプライアンスよりも低くなります。CPU リソースを増やすと、仮想マシンのパフォーマンスが向上します。

仮想マシン環境での最小要件は 1121 アプライアンスと似ています。仮想マシン環境の詳細については、『*Installation and Upgrade Guide for the Cisco Secure Access Control System 5.3*』を参照してください。