

ACS サーバの展開について

この章では、ACS サーバの考えられる展開方法とそのコンポーネントの概要について説明します。

この章の内容は、次のとおりです。

- [展開シナリオ、1 ページ](#)
- [ACS サーバの設定について、5 ページ](#)

展開シナリオ

ここでは、ACS を使用する次の 3 つの展開シナリオについて説明します。

- [小規模 ACS 展開、1 ページ](#)
- [中規模 ACS 展開、2 ページ](#)
- [大規模 ACS 展開、3 ページ](#)

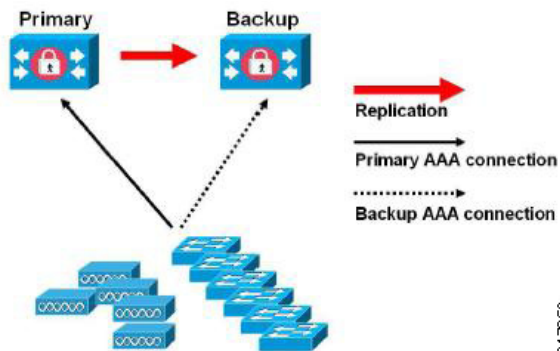
小規模 ACS 展開

最も基本的な ACS の展開は、[図 1 \(1 ページ\)](#) に示すように、2 台のサーバで構成されます。第 1 のサーバは、ネットワークのすべての設定、認証、ポリシー要件を満たすプライマリ サーバです。

第 2 のサーバは、AAA クライアントとプライマリ サーバ間の接続が失われた場合にバックアップサーバとして使用されます。プライマリ ACS サーバからセカンダリサーバへのレプリケーションを使用して、セカンダリサーバがプライマリサーバと同期している状態を保ちます。

小規模なネットワークでは、この構成により、プライマリとセカンダリの RADIUS または TACACS サーバを、すべての AAA クライアントで同じように設定できます。

図 1 小規模 ACS 展開



組織内のユーザと AAA クライアントの数の増加に応じて、ACS の展開方法を基本的な設計から変更し、[図 2 \(2 ページ\)](#) に示す分割 ACS 展開設計を使用することを推奨します。

分割 ACS 展開

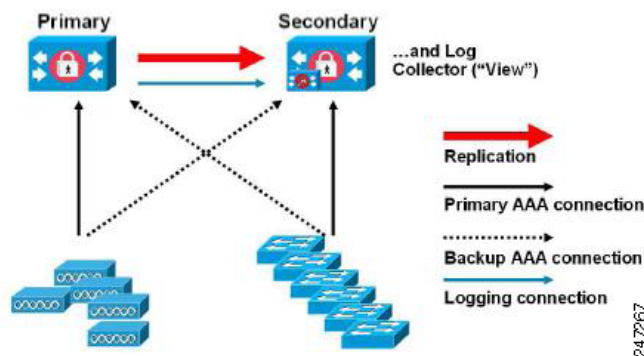
分割 ACS 展開では、小規模 ACS 展開と同様にプライマリ サーバとセカンダリ サーバを使用しますが、AAA の負荷を 2 台のサーバに分散し、AAA フローを最適化します。AAA 接続に問題が発生した場合は、各サーバが両方のサーバのすべての負荷を処理しますが、通常運用時には、どちらのサーバも認証要求のすべての負荷を処理しません。

サーバのこの特性により、各 ACS システムへの負荷が最適化され、正常動作を通じてセカンダリ サーバの動作状態を知ることができます。

この配置のもう 1 つの利点は、各サーバを、デバイスの管理やネットワークの許可など特定の運用のために使用しながら、障害時にすべての AAA 機能を実行できることです。

2 台の ACS システムが、AAA クライアントからの認証要求の処理とアカウントリングデータの収集を行うため、一方のシステムをログコレクタとして使用することを推奨します。図 2(2 ページ) では、セカンダリ ACS サーバをログコレクタとして使用しています。

図 2 分割 ACS 展開

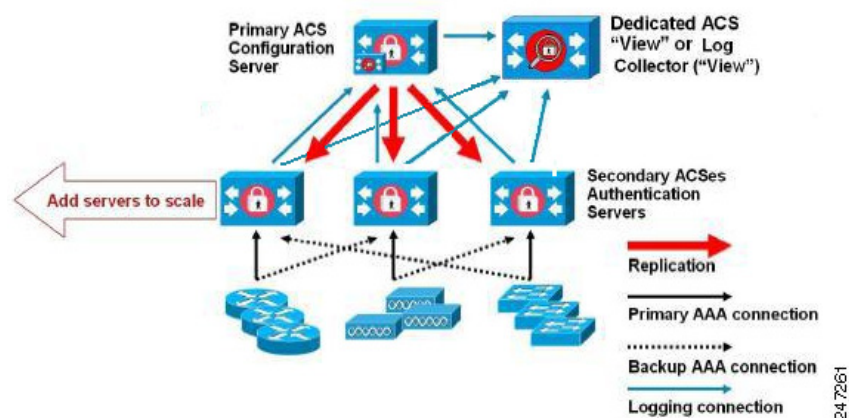


この設計のもう 1 つの利点は、図 3(3 ページ) に示すように拡張が可能なことです。

中規模 ACS 展開

ローカルネットワークの成長に応じて、さらに ACS サーバをシステムに追加する必要があります。このシナリオでは、プライマリ サーバを昇格させて構成サービスを実行し、セカンダリ サーバを AAA 機能で使用することを検討します。ログトラフィック量が増大した場合は、セカンダリ サーバの 1 台を専用の中央ログコレクタサーバとして使用する必要があります。ACS 5.8 は、展開では 1 個の追加 ACS インスタンスをサポートします。ACS 5.8 メディア展開では、14 個の ACS インスタンスをサポートします。実際のプライマリ インスタンスを降格させる場合に、この追加 ACS インスタンスをプライマリ インスタンスにプロモート可能な専用インスタンスとして指定できます。

図 3 中規模 ACS 展開



大規模 ACS 展開

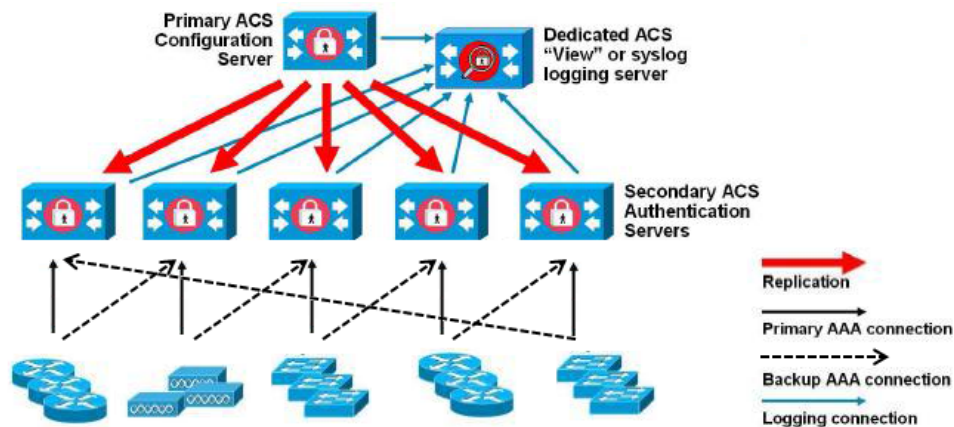
図 4(4 ページ) に示すような大規模 ACS 展開では、集中化されたロギングを使用することを強く推奨します。ACS 5.8 は、展開では 1 個の追加 ACS インスタンスをサポートします。ACS 5.8 の大規模な展開では、22 個の ACS インスタンスをサポートします。実際のプライマリ インスタンスを降格させる場合に、この追加 ACS インスタンスをプライマリ インスタンスにプロモート可能な専用インスタンスとして指定できます。使用率の高いネットワークでは、大量の syslog トラフィックが生成される可能性があるため、専用のロギング サーバ(モニタリングおよびレポート サーバ)を使用することが推奨されます。ACS は 発信ログ トラフィックに対して syslog メッセージを生成するため、RFC-3164 に準拠した任意の syslog サーバを使用して発信ロギング トラフィックを収集できます。

このタイプのサーバでは、すべての ACS サーバに対して、ACS が備えているレポート機能とアラート機能を使用できます。これには特別なライセンスが必要です(『User Guide for Cisco Secure Access Control System 5.8』を参照してください)。ACS サーバのインストールの詳細については、ACS サーバのインストール、2 ページを参照してください。

モニタリングおよびレポートサーバと汎用 syslog サーバの両方にログを送信するようにサーバを設定することも検討してください。汎用 syslog サーバを追加することにより、モニタリングおよびレポート サーバがダウンした場合に、バックアップが提供されます。

注: ACS 5.8 は、ACS インスタンス数が 22 を超える大規模導入をサポートしていません。

図 4 大規模 ACS 展開



247254

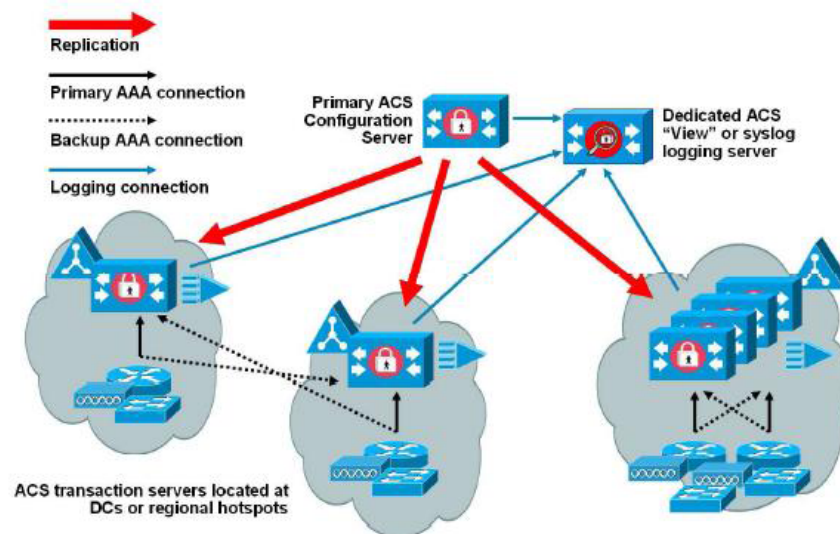
分散 ACS 展開

分散 ACS 展開は、世界中にキャンパスがある組織で有効です。ホーム キャンパスにプライマリ ネットワークがある場合もありますが、さまざまな地域のキャンパスに、小規模から大規模の LAN が存在することもあります。

AAA パフォーマンスを最適化するために、これらの各リモート キャンパスには独自の AAA インフラストラクチャを配置します。図 5(4 ページ)を参照してください。一貫性のある同期された AAA ポリシーを維持するためには、集中化された管理モデルを使用する必要があります。

集中化された構成でも、プライマリ ACS サーバと個別のモニタリングおよびレポート サーバを使用する必要があります。しかし、各リモート キャンパスには固有の要件があります。

図 5 分散 ACS 展開



247258

リモート サイトがあるネットワークを計画する際に検討すべき要素としては、次のものがあります。

- 中央または外部データベース (Microsoft Active Directory (AD) または Lightweight Directory Access Protocol (LDAP)) を使用しているかどうかを確認します。最適化のために、ACS がアクセス可能な、外部データベースの同期されたインスタンスを各リモート サイトに配置する必要があります。
- AAA クライアントの場所も重要な留意事項です。ネットワークの遅延による影響や、WAN 障害によってアクセスできなくなる可能性を減らすために、ACS サーバは、できるだけ AAA クライアントの近くに配置する必要があります。

- ACS では、バックアップなどの一部の機能にコンソールからアクセスできます。各サイトで端末を使用することを検討します。これにより、ネットワークの外部から各サーバに対するセキュアなコンソール アクセスが可能になります。
- 小規模なりモート サイトが近くにあり、他のサイトへの信頼できる WAN 接続がある場合は、近くのサイトにある ACS サーバをローカル サイトのバックアップ サーバとして使用し、冗長性のある構成とすることもできます。
- 外部データベースにアクセスできるようにするには、すべての ACS ノードで DNS を適切に設定する必要があります。

ACS サーバの設定について

ここでは、各種 ACS サーバの役割と、その設定方法についての概要を説明します。ロールのサーバへの割り当てと設定の詳細については、『*User Guide for Cisco Secure Access Control System 5.8*』を参照してください。

この項の構成は、次のとおりです。

- プライマリ サーバ、5 ページ
- セカンダリ サーバ、5 ページ
- ログ収集サーバ、6 ページ

インストール手順は、どの ACS サーバでも同様です。

ACS (CSACS-1121 アプライアンス モデル) の設置については、[CSACS-1121 を使用した Cisco Secure Access Control System のインストールと設定、1 ページ](#) を参照してください。ACS (Cisco SNS-3415 アプライアンス モデル) の設置については [Cisco SNS-3415 および Cisco SNS-3495 を使用した Secure Access Control System のインストールと設定、1 ページ](#) を、ACS (VMware ESX) の設置については [VMware 仮想マシンへの ACS のインストール、1 ページ](#) を参照してください。ACS の導入時は、必ずプライマリ サーバを最初に設置してください。

プライマリ サーバ

ACS 展開では、1 つのインスタンスだけが ACS プライマリとなり、構成機能を提供するとともに、レプリケーションのソースとなります。

ACS プライマリ サーバでは、ACS の展開に必要なすべてのシステム設定を行うことができます。ただし、ライセンスとローカル証明書は、各 ACS セカンダリ サーバで個別に設定する必要があります。

セカンダリ サーバ

プライマリ サーバを除く他のすべてのインスタンスはセカンダリ サーバとして機能します。

セカンダリ ACS サーバは、プライマリ サーバからすべてのシステム設定を受け取ります。ただし、次のものは各セカンダリ サーバで設定する必要があります。

- ライセンス: 展開内の各 ACS セカンダリ サーバに対し、固有の基本ライセンスをインストールします。
- 新しいローカル証明書: セカンダリ サーバでローカル証明書を設定するか、プライマリ サーバからローカル証明書をインポートします。
- ログ収集サーバ: プライマリ サーバとセカンダリ サーバのいずれかを、ACS のログ収集サーバとして設定できます。セカンダリ ACS サーバをログ収集サーバとして設定することを推奨します。

注: セカンダリ サーバのインストール先を選択する場合、プライマリ サーバとセカンダリ サーバの間でネットワーク アドレスは変換できません。

セカンダリ サーバを ACS 環境の一部とするためには、アクティベーションを行う必要があります。管理者は、セカンダリ サーバのアクティベーションを行うか、自動アクティベーションを設定する必要があります。デフォルトでは、アクティベーションは自動に設定されます。

セカンダリ サーバは、アクティベーションが行われると、設定とレプリケーションの更新がプライマリ サーバと同期されます。

ログ収集サーバ

プライマリ サーバまたはいずれかのセカンダリ サーバがログ収集サーバとして機能できます。

ログ収集サーバは、展開内のプライマリ サーバとすべての ACS セカンダリ サーバからログを受信します。ACS セカンダリ サーバのうちの 1 台をモニタリングおよびレポート サーバとして割り当て、このセカンダリ サーバを AAA アクティビティから除外することを推奨します。

3 つの主なロギング カテゴリは、監査、アカウントिंग、および診断です。

ロギング カテゴリと設定の詳細については、『*User Guide for Cisco Secure Access Control System 5.8*』を参照してください。