



AAA の RSA SecurID サーバー

ここでは、AAA で使用する RSA SecurID サーバーの設定方法について説明します。RSA SecurID サーバーは、通信に SDI プロトコルを使用することから、SDI サーバーとも呼ばれます。管理接続、ネットワークアクセス、および VPN ユーザーアクセスの認証に RSA SecurID サーバーを使用できます。

- [RSA SecurID サーバーについて \(1 ページ\)](#)
- [AAA の RSA SecurID サーバーのガイドライン \(1 ページ\)](#)
- [AAA の RSA SecurID サーバーの設定 \(2 ページ\)](#)
- [AAA の RSA SecurID サーバーのモニタリング \(4 ページ\)](#)
- [AAA の RSA SecurID サーバーの履歴 \(5 ページ\)](#)

RSA SecurID サーバーについて

RSA SecurID サーバは、認証に直接使用することも、認証の第 2 要素として間接的に使用することもできます。後者の場合は、SecurID サーバーと RADIUS サーバーの間で SecurID サーバーとの関係を設定し、RADIUS サーバーを使用するように ASA を設定します。

一方、SecurID サーバーに対して直接認証する場合は、SDI プロトコルの AAA サーバグループを作成します。これは、それらのサーバーとの通信に使用されるプロトコルです。

SDI を使用する場合は、AAA サーバグループを作成するときにプライマリ SecurID サーバーを指定するだけで済みます。ASA からサーバーに最初に接続したときに、すべての SecurID サーバーのレプリカをリストした `sdiconf.rec` ファイルを取得します。以降にプライマリサーバが応答しない場合、それらのレプリカが認証に使用されます。

さらに、ASA を認証エージェントとして RSA Authentication Manager に登録する必要があります。ASA を登録していないと認証の試行は失敗します。

AAA の RSA SecurID サーバーのガイドライン

- シングルモードで最大 200 個のサーバグループ、またはマルチモードでコンテキストごとに 8 つのサーバグループを持つことができます。

- 各グループには、シングルモードで最大 16 台、マルチモードで最大 8 台のサーバーを含めることができます。ユーザーがログインすると、コンフィギュレーション内で指定されている最初のサーバーから順に、サーバーが応答するまでこれらのサーバーが 1 つずつアクセスされます。

AAA の RSA SecurID サーバーの設定

ここでは、RSA SecurID サーバーグループの設定方法について説明します。管理アクセスや VPN を設定するときに、これらのグループを使用できます。

RSA SecurID AAA サーバーグループの設定

認証に RSA SecurID サーバーとの直接通信を使用する場合は、最初に少なくとも 1 つの SDI サーバーグループを作成し、各グループに 1 つ以上のサーバーを追加する必要があります。RADIUS サーバーとプロキシ関係が確立された SecurID サーバーを使用する場合は、ASA で SDI AAA サーバーグループを設定する必要はありません。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから、[SDI] サーバータイプを選択します。

ステップ 5 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバが非アクティブになると、グループ内のすべてのサーバが再アクティブ化されます。このアプローチでは、障害が発生したサーバに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 6 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。デッドタイムは、ローカ

ルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。

ステップ 7 次のサーバーを試す前にグループ内の AAA サーバーでの AAA トランザクションの失敗の最大数を指定します。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 8 [OK] をクリックします。

SDI サーバーグループへの RSA SecurID サーバーの追加

SDI サーバーグループを使用する前に、少なくとも 1 つの RSA SecurID サーバーをグループに追加する必要があります。

SDI サーバーグループのサーバーは、ASA との通信に認証およびサーバー管理プロトコル (ACE) を使用します。

手順

ステップ 1 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 サーバーを追加するサーバーグループを選択します。

ステップ 3 [Servers in the Selected Group] 領域で、[Add] をクリックします。

サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 4 [Interface Name] で、認証サーバーが存在するインターフェイス名を選択します。

ステップ 5 グループに追加するサーバーの名前または IP アドレスを入力します。

ステップ 6 サーバーへの接続試行のタイムアウト値を指定します。

Specify the timeout interval (1-300 seconds) for the server; the default is 10 seconds. For each AAA transaction the ASA retries connection attempts (based on the retry interval) until the timeout is reached. 連続して失敗したトランザクションの数が AAA サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー (設定されている場合) への要求の送信を開始します。

ステップ 7 再試行間隔を選択します。システムはこの時間待機してから接続要求を再試行します。1〜10 秒の範囲で選択できます。デフォルトは 10 秒です。

ステップ 8 サーバー ポートを指定します。サーバーポートは、デフォルトのポート番号である 5500 か、ASA で RSA SecurID サーバーとの通信に使用する TCP ポートの番号です。

ステップ 9 [OK] をクリックします。

SDI ノードシークレットファイルのインポート

RSA Authentication Manager (SecurID) サーバーによって生成されたノードシークレットファイルを手動でインポートできます。

手順

ステップ 1 RSA Authentication Manager サーバーからノードシークレットファイルをエクスポートします。詳細については、RSA Authentication Manager のドキュメントを参照してください。

ステップ 2 **[Configuration] > [Device Management] > [Users/AAA] > [AAA SDI]** の順に選択します。

ステップ 3 **[Upload]** をクリックし、RSA Authentication Manager からエクスポートして解凍されたノードシークレットファイルを選択してシステムにアップロードします。

ステップ 4 **[Import Node Secret for SDI]** で、次の情報を入力します。

- **[Server IP]** : ノードシークレットが属する RSA Authentication Manager サーバーの IP アドレスまたは完全修飾ホスト名。
- **[Password]** : エクスポート時にファイルを保護するために使用されるパスワード。
- **[File Name]** : **[Browse]** をクリックし、アップロードした解凍済みノードシークレットファイルを選択します。

AAA の RSA SecurID サーバーのモニタリング

次のコマンドを使用して、RSA SecurID 関連情報をモニターおよびクリアできます。コマンドは **[Tools] > [Command Line Interface]** ウィンドウで入力します。

- **[Monitoring] > [Properties] > [AAA Servers]**

このウィンドウに AAA サーバーの統計情報が表示されます。

- **show aaa-server**

AAA サーバーの統計情報を表示します。サーバーの統計情報をクリアするには、**clear aaa-server statistics** コマンドを使用します。

- **show running-config aaa-server**

システムに設定されている AAA サーバーを表示します。AAA サーバー コンフィギュレーションを削除するには、**clear configure aaa-server** コマンドを使用します。

- **show aaa sdi node-secrets**

インポートされたノードシークレットファイルがある RSA SecurID サーバーを表示します。ノードシークレットファイルを削除するには、**clear aaa sdi node-secret** コマンドを使用します。

AAA の RSA SecurID サーバーの履歴

機能名	プラットフォーム リリース	説明
SecurID サーバー	7.2(1)	AAA の SecurID サーバーの管理認証でのサポート。以前のリリースでは、SecurID は VPN 認証でサポートされていました。
AAA の IPv6 アドレス	9.7(1)	AAA サーバーに IPv4 または IPv6 アドレスを使用できるようになりました。
グループごとの AAA サーバー グループとサーバーの制限が増えました。	9.13(1)	より多くの AAA サーバー グループを設定できます。シングルコンテキストモードでは、200 個の AAA サーバー グループを設定できます（以前の制限は 100）。マルチコンテキストモードでは、8 個設定できます（以前の制限は 4）。 さらに、マルチコンテキストモードでは、グループごとに 8 台のサーバーを設定できます（以前の制限はグループごとに 4 台のサーバー）。シングルコンテキストモードのグループごとの制限の 16 は変更されていません。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。
SDI AAA サーバーグループで使用するノードシークレットファイルの RSA Authentication Manager からの手動インポート。	9.15(1)	SDI AAA サーバーグループで使用するために RSA Authentication Manager からエクスポートしたノードシークレットファイルをインポートできます。 次の画面が追加されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA SDI]。

翻訳について

このドキュメントは、米国シスコ発行ドキュメントの参考和訳です。リンク情報につきましては、日本語版掲載時点で、英語版にアップデートがあり、リンク先のページが移動/変更されている場合がありますことをご了承ください。あくまでも参考和訳となりますので、正式な内容については米国サイトのドキュメントを参照ください。