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 SecureID 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

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 サーバー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 サーバー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 個のサーバーグループ、またはマルチモードでコンテキストごとに 8 つのサーバー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 SDI AAA サーバーグループを作成し、AAA サーバーグループ コンフィギュレーション モードを開始します。

aaa-server *server_group_name* **protocol sdi**

例：

```
ciscoasa(config)# aaa-server watchdog protocol sdi
```

ステップ 2 （オプション）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。

max-failed-attempts *number*

例：

```
ciscoasa(config-aaa-server-group)# max-failed-attempts 2
```

number 引数の範囲は 1 ～ 5 です。デフォルトは 3 です。

ローカルデータベースを使用してフォールバック方式（管理アクセス専用）を設定すると、グループ内のすべてのサーバーが応答しないか応答が無効である場合にグループは応答なしと見なされ、フォールバック方式が試行されます。サーバー グループで、追加の AAA 要求によるアクセスがない、非応答と見なされる時間が 10 分間（デフォルト）続くと、ただちにフォールバック方式が使用されます。非応答時間をデフォルトから変更するには、次のステップの **reactivation-mode** コマンドを参照してください。

フォールバック方式として設定されていない場合、ASAは引き続きグループ内のサーバーにアクセスしようとします。

ステップ 3 （任意）グループ内で障害の発生したサーバーを再度アクティブ化する方法（再アクティブ化ポリシー）を指定します。

reactivation-mode {**depletion** [**deadtime** *minutes*] | **timed**}

例：

```
ciscoasa(config-aaa-server-group)# reactivation-mode depletion deadtime 20
```

depletion キーワードを指定すると、グループ内のすべてのサーバーが非アクティブになって初めて、障害の発生したサーバーが再度アクティブ化されます。これは、デフォルトのモードです。

deadtime *minutes* キーワードと引数のペアは、グループ内の最後のサーバーをディセーブルにしてから次にすべてのサーバーを再度イネーブルにするまでの経過時間を、0 ～ 1440 分の範囲で指定します。デフォルトは 10 分です。

timed キーワードを指定すると、30 秒のダウン時間の後、障害が発生したサーバーが再度アクティブ化されます。

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 RSA SecurID サーバーを SDI サーバーグループに追加します。

aaa-server *server_group* [**(***interface_name***)**] **host** *server_ip*

例：

```
ciscoasa(config-aaa-server-group)# aaa-server servergroup1 outside host 10.10.1.1
```

インターフェイスを指定しない場合、ASA ではデフォルトで**内部**インターフェイスを使用します。

IPv4 または IPv6 アドレスを使用できます。

ステップ 2 サーバーへの接続試行のタイムアウト値を指定します。

timeout *seconds*

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 interval defined on the **retry-interval** command）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 **max-failed-attempts** コマンドで指定された制限に達すると、AAA サーバーは非アクティブ化され、ASA は（設定されている場合は）別の AAA サーバーへの要求の送信を開始します。

例：

```
ciscoasa(config-aaa-server-host)# timeout 15
```

ステップ 3 再試行間隔を指定します。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。

retry-interval *seconds*

1 ー 10 秒を指定できます。デフォルトは 10 です。

例：

```
ciscoasa(config-aaa-server-host)# retry-interval 6
```

ステップ 4 デフォルトの RSA SecurID ポート（TCP/5500）と異なる場合はサーバーポートを指定します。ASA は、このポートで RSA SecurID サーバーに接続します。

server-port *port_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 5555
```

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 解凍したバージョンのノードシークレットファイルを ASA からアクセスできるサーバーに配置するか、ASA 自体にコピーします。

サーバーは、FTP、HTTP、HTTPS、SCP、SMB、TFTP のいずれかの転送プロトコルをサポートしている必要があります。

ステップ 3 ノードシークレットファイルをインポートします。

aaa sdi import-node-secret *filepath rsa_server_address password*

値は次のとおりです。

- *filepath* は、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への完全なパスです。ローカルシステムのファイルは、disk0:、disk1:、または flash: としてアドレス指定できます。リモートサーバーのファイルの場合は、ftp:// などの標準の URL 表記を使用します。
- *rsa_server_address* は、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です。
- *password* は、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です。

例：

```
ciscoasa# aaa sdi import-node-secret nodesecret.rec rsaam.example.com mysecret
nodesecret.rec imported successfully
ciscoasa#
```

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。

- **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、次のコマンドが変更されました。**aaa-server**、**aaa-server host**
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。 次のコマンドが追加されました。**aaa sdi import-node-secret**、**clear aaa sdi node-secret**、**show aaa sdi node-secrets**。

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。