AAA サーバグループ

認証、認可、およびアカウンティング（AAA）サーバー グループを使用するようにデバイスを設定すると、既存のサーバーホストをグループ化できます。既存のサーバーホストをグループ化すると、設定したサーバーホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバー グループに送信できます。この機能モジュールでは、AAA サーバー グループとデッドタイマーを設定する方法について説明します。

AAA サーバー グループに関する情報

AAA サーバグループ

AAA サーバー グループを使用するようにデバイスを設定すると、既存のサーバー ホストをグループ化できます。既存のサーバー ホストをグループ化すると、設定したサーバー ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホストの一覧と一緒に使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。

また、サーバー グループには、各エントリが一意の ID を持っていれば、同一サーバーに複数のホスト エントリを組み込むことができます。固有の識別情報は、IP アドレスと UDP ポート番号の組み合わせで構成されます。これにより、RADIUS ホストとして定義されているさまざまなポートが、固有の AAA サービスを提供できるようになります。この一意の ID により、同じ IP アドレスでサーバーの異なる UDP ポートに RADIUS の要求を送ることができるようになります。同じ RADIUS サーバー上の異なる 2 つのホスト エントリに同じサービス（たとえばアカウンティングなど）を設定した場合、2 番目に設定されたホスト エントリは、最初に設定されたホスト エントリのフェールオーバー バックアップとして動作します。最初のホスト エ

ントリがアカウンティング サービスの提供に失敗すると、ネットワーク アクセス サーバは同じデバイスに設定されている 2 番めのホスト エントリを使用してアカウンティング サービスを提供するように試行します。（試行される RADIUS ホスト エントリの順番は、設定されている順序に従います）。

AAA サーバー グループのデッドタイマー

サーバー名を指定してサーバーホストを設定したら、**deadtime** コマンドを使用して、サーバーグループごとに各サーバーを設定できます。サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバー グループに送信できます。

デッドタイムの設定は、グローバル コンフィギュレーションに限定されません。すべてのサーバー グループの各サーバー ホストには、個別のタイマーがあります。そのため、サーバーが応答せず、再送信とタイムアウトが何度も発生する場合、そのサーバーは動作していない（デッド状態）と見なされます。すべてのサーバー グループの各サーバー ホストに付属するタイマーが開始されます。基本的に、タイマーがチェックされ、サーバーに対する以降の要求は（デッド状態と見なされた場合）、（設定されていれば）代替タイマーに送信されます。ネットワーク アクセス サーバーがサーバーからの応答を受信すると、すべてのサーバー グループのそのサーバーに関するすべての設定済みタイマー（実行中の場合）が停止されます。

タイマーが期限切れになると、タイマーが付属しているサーバーは応答可能（アライブ状態）と見なされます。このサーバーは、タイマーが属するサーバー グループを使用して後で AAA 要求のために試行できる唯一のサーバーになります。

（注） 1 つのサーバーが複数のタイマーを持ち、異なるデッドタイム値がサーバー グループに設定されることがあるため、同時刻の同じサーバーでも複数の状態（デッドとアライブ）になる可能性があります。

（注） サーバーの状態を変更するには、すべてのサーバー グループですべての設定済みタイマーを起動および終了する必要があります。

新しいタイマーと deadtime 属性が追加されるため、サーバー グループのサイズはやや増えます。構造の全体的な影響は、サーバー グループの数と規模、およびその設定でサーバー グループ内でサーバーを共有する方法によって変わります。

AAA サーバー グループの設定方法

AAA サーバー グループの設定

サーバー グループ名を使用してサーバー ホストを定義するには、グローバル コンフィギュレーション モードで次のコマンドを使用します。一覧のサーバーは、グローバル コンフィギュレーション モードに存在します。

始める前に

グループの各サーバーは、**radius-server host** コマンドを使用して事前に定義する必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **radius server** *server-name*
4. **aaa group server** {**radius** | **tacacs+**} *group-name*
5. **server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*]
6. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • パスワードを入力します（要求された場合）。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 3	**radius server** *server-name* 例： `Device(config)# radius server rad1`	RADIUS サーバーの名前を指定します。
ステップ 4	**aaa group server** {**radius**	**tacacs+**} *group-name* 例： `Device(config)# aaa group server radius group1`	グループ名を使用して、AAA サーバー グループを定義します。 • グループのすべてのメンバは、タイプを同じにする必要があります。つまり、RADIUS または

	コマンドまたはアクション	目的
		TACACS+ です。このコマンドを実行すると、デバイスはサーバー グループRADIUS コンフィギュレーション モードへ移行します。
ステップ 5	**server** *ip-address* [**auth-port** *port-number*] [**acct-port** *port-number*] 例： `Device(config-sg-radius)# server 172.16.1.1 acct-port 1616`	特定の RADIUS サーバーを定義済みのサーバー グループと関連付けます。 • セキュリティ サーバーは、IP アドレスと UDP ポート番号で識別されます。 • AAA サーバー グループの RADIUS サーバーごとに、このステップを繰り返します。
ステップ 6	**end** 例： `Device(config-sg-radius)# end`	サーバー グループ RADIUS コンフィギュレーション モードを終了し、特権EXECモードに戻ります。

AAA サーバー グループのデッドタイマーの設定

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa group server radius** *group*
4. **deadtime** *minutes*
5. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**enable** 例： `Device> enable`	特権 EXEC モードを有効にします。 • プロンプトが表示されたらパスワードを入力します。
ステップ 2	**configure terminal** 例： `Device# configure terminal`	グローバル コンフィギュレーション モードを開始します。

	コマンドまたはアクション	目的
ステップ 3	**aaa group server radius** *group* 例： `Device(config)# aaa group server radius group1`	RADIUS タイプ サーバー グループを定義し、サーバー グループ RADIUS コンフィギュレーション モードを開始します。
ステップ 4	**deadtime** *minutes* 例： `Device(config-sg-radius)# deadtime 1`	デッドタイム値（分）を設定および定義します。 （注） ローカル サーバー グループのデッドタイムは、グローバル コンフィギュレーションよりも優先されます。ローカル サーバー グループ コンフィギュレーションでデッドタイム値を省略した場合は、プライマリ リストから継承されます。
ステップ 5	**end** 例： `Device(config-sg-radius)# end`	サーバーグループ RADIUS コンフィギュレーション モードを終了し、特権 EXEC モードに戻ります。

AAA サーバー グループの設定例

例：AAA サーバー グループ

次に、3 つの RADIUS サーバ メンバを持ち、各メンバがデフォルトの認証ポート（1645）とアカウンティング ポート（1646）を使用するサーバ グループ radgroup1 を作成する例を示します。

```
aaa group server radius radgroup1
 server 172.16.1.11
 server 172.17.1.21
 server 172.18.1.31
```

次に、3 つの RADIUS サーバ メンバを持ち、各メンバが IP アドレスは同じでも認証ポートとアカウンティング ポートはそれぞれ異なるサーバ グループ radgroup2 を作成する例を示します。

```
aaa group server radius radgroup2
 server 172.16.1.1 auth-port 1000 acct-port 1001
 server 172.16.1.1 auth-port 2000 acct-port 2001
 server 172.16.1.1 auth-port 3000 acct-port 3001
```

例：AAA サーバー グループを使用する複数の RADIUS サーバー エントリ

次に、2 つの RADIUS サーバー グループを認識するようにネットワーク アクセス サーバーを設定する例を示します。一方のグループである group1 には、同じ RADIUS サーバー上に同じサービス用に設定された 2 つのホスト エントリがあります。設定されている 2 番めのホスト エントリは、1 番めのエントリのフェールオーバーバックアップとして動作します各グループのデッドタイムは個々に設定されています。group 1 のデッドタイムは 1 分で、group 2 のデッドタイムは 2 分です。

（注） グローバル コマンドと **server** コマンドの両方を使用する場合、**server** コマンドがグローバル コマンドよりも優先されます。

```
! This command enables AAA.
aaa new-model
! The next command configures default RADIUS parameters.
aaa authentication ppp default group group1
! The following commands define the group1 RADIUS server group and associate servers
! with it and configures a deadtime of one minute.
aaa group server radius group1
 server 10.1.1.1 auth-port 1645 acct-port 1646
 server 10.2.2.2 auth-port 2000 acct-port 2001
 deadtime 1
! The following commands define the group2 RADIUS server group and associate servers
! with it and configures a deadtime of two minutes.
aaa group server radius group2
 server 10.2.2.2 auth-port 2000 acct-port 2001
 server 10.3.3.3 auth-port 1645 acct-port 1646
 deadtime 2
! The following set of commands configures the RADIUS attributes for each host entry
! associated with one of the defined server groups.
radius-server host 10.1.1.1 auth-port 1645 acct-port 1646
radius-server host 10.2.2.2 auth-port 2000 acct-port 2001
radius-server host 10.3.3.3 auth-port 1645 acct-port 1646
```

その他の参考資料

関連資料

関連項目	マニュアル タイトル
Cisco IOS コマンド	『*Cisco IOS Master Command List, All Releases*』
AAA コマンドと RADIUS コマンド	『*Cisco IOS Security Command Reference*』
RADIUS 属性	『*RADIUS Attributes Configuration Guide*』（Securing User Services Configuration Library の一部）

関連項目	マニュアル タイトル
AAA	『*Authentication, Authorization, and Accounting Configuration Guide*』（Securing User Services Configuration Library の一部）
L2TP、VPN、または VPDN	『*Dial Technologies Configuration Guide*』および『*VPDN Configuration Guide*』
モデムの設定と管理	『*Dial Technologies Configuration Guide*』
PPP の RADIUS ポートの識別	『*Wide-Area Networking Configuration Guide*』

RFC

RFC	タイトル
RFC 2138	『*Remote Authentication Dial In User Service (RADIUS)*』
RFC 2139	『*RADIUS Accounting*』
RFC 2865	『*RADIUS*』
RFC 2867	『*RADIUS Accounting Modifications for Tunnel Protocol Support*』
RFC 2868	『*RADIUS Attributes for Tunnel Protocol Support*』

シスコのテクニカル サポート

説明	リンク
右の URL にアクセスして、シスコのテクニカル サポートを最大限に活用してください。これらのリソースは、ソフトウェアをインストールして設定したり、シスコの製品やテクノロジーに関する技術的問題を解決したりするために使用してください。この Web サイト上のツールにアクセスする際は、Cisco.com のログイン ID およびパスワードが必要です。	http://www.cisco.com/cisco/web/support/index.html

AAA サーバー グループの機能情報

次の表に、このモジュールで説明した機能に関するリリース情報を示します。この表は、ソフトウェア リリース トレインで各機能のサポートが導入されたときのソフトウェア リリースだけを示しています。その機能は、特に断りがない限り、それ以降の一連のソフトウェア リリースでもサポートされます。

プラットフォームのサポートおよびシスコ ソフトウェアイメージのサポートに関する情報を検索するには、Cisco Feature Navigator を使用します。Cisco Feature Navigator にアクセスするには、www.cisco.com/go/cfn に移動します。Cisco.com のアカウントは必要ありません。

表 *1: AAA* サーバー グループの機能情報

機能名	リリース	機能情報
AAA Server Group		AAA サーバー グループを使用するようにデバイスを設定すると、既存のサーバー ホストをグループ化できます。これによって、設定したサーバー ホストのサブセットを選択し、それを特定のサービスに使用できます。サーバー グループは、グローバル サーバー ホストの一覧と一緒に使用されます。サーバー グループには、選択したサーバー ホストの IP アドレスが一覧表示されます。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**aaa group server radius**、**aaa group server tacacs+**、および **server**（RADIUS）。

機能名	リリース	機能情報
AAA サーバー グループの拡張機能		AAA サーバー グループの拡張機能により、サーバー グループ内のサーバーの完全な設定が可能です。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ
AAA サーバー グループ デッドタイマー		サーバー グループ内でデッドタイムを設定することで、AAA トラフィックを、異なる動作特性を持つ別のサーバーグループに送信できます。 • Catalyst 3850 シリーズ スイッチ • Cisco 5760 Wireless LAN Controller • Catalyst 3650 シリーズ スイッチ 次のコマンドが導入または変更されました。**deadtime**

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。