AAA 認可および AAA 認証のキャッシュ

AAA 認可キャッシュ機能および AAA 認証のキャッシュ機能を使用すると、設定した一連のユーザ プロファイルまたはサービス プロファイルの認可応答と認証応答をキャッシュに格納することができます。このため、認可応答および認証応答から返されるユーザ プロファイルとサービス プロファイルを複数のソースから照会できるようになり、オフロード サーバだけに依存する必要がなくなるので、パフォーマンスとネットワークの信頼性レベルが向上します。また、この機能のフェールオーバー メカニズムにより、ネットワークの RADIUS サーバまたは TACACS+ サーバが認可応答や認証応答を返せなくなっても、ネットワークのユーザや管理者は引き続きネットワークにアクセスできます。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の前提条件

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装には、次の前提条件が適用されます。

- プロファイル キャッシュ機能の実装方法を理解している必要があります。つまり、ネットワークのパフォーマンスを向上させたり、ネットワークの認証（RADIUS）サーバや認可（TACACS+）サーバが使用できなくなった場合にフェールオーバーを実行したりするためにプロファイルがどのようにキャッシュされるかを理解している必要があります。
- RADIUS サーバ グループと TACACS+ サーバ グループがすでに設定されている必要があります。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装について

認可プロファイルおよび認証プロファイルのキャッシュ機能によるネットワーク パフォーマンスの最適化

RADIUS クライアントおよび TACACS+ クライアントは Cisco ルータ上で稼働し、ユーザ認証およびネットワーク サービス アクセスに関するすべての情報を保持する中央の RADIUS サーバまたは TACACS+ サーバへ認証要求を送信します。ルータはオフロードの RADIUS サーバまたは TACACS+ サーバと通信してコールを認証した後、ポリシーまたはサービスをそのコールに適用する必要があります。認証、許可、アカウンティング（AAA）アカウンティングと異なり、AAA 認証および AAA 認可はブロッキング手順です。つまり、コールの認証中および認可中は、コールセットアップは進行しません。したがって、そのような認証要求または認可要求が、ルータから RADIUS オフロード サーバまたは TACACS+ サーバに渡されて処理される時間と、そのサーバからルータに渡されて処理される時間は、コールセットアップの処理に必要な時間に直に影響します。転送中の通信の問題、オフロードサーバの利用率、その他のさまざまな要因が、コール セットアップのパフォーマンスを大幅に低下させるのは、AAA 認証および AAA 認可の手順に原因があります。この問題がさらに顕著になるのは、複数の AAA 認証および AAA 認可が 1 つのコールまたはセッションに必要になるときです。

この問題の解決策は、そのような認証要求の影響を最小限にすることです。そのために、ルータで特定のユーザの認証応答および認可応答をキャッシュに格納して、要求をオフロードサーバに何度も送信する必要をなくします。このプロファイルキャッシュ機能により、コールセットアップ時間が大幅に短縮されます。また、プロファイルキャッシュ機能によってネットワークの信頼性レベルが上がります。これは、認証応答および認可応答から返されるユーザ プロファイルやサービスプロファイルを複数のソースから照会できるようになり、オフロードサーバだけに依存する必要がなくなるためです。

このようにパフォーマンスを最適化するためには、ユーザがルータから認証されるときにAAA キャッシュ プロファイルが最初に照会されるように認証方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能

何らかの理由で、RADIUS サーバまたは TACACS+ サーバが認証応答および認可応答を返せない場合、ネットワークのユーザおよび管理者はネットワークから締め出されることがあります。プロファイルのキャッシング機能により、認証フェーズを完了しなくてもユーザ名の承認が可能になります。たとえば、ユーザ名が user100@example.com でパスワードが secretpassword1 のユーザは、正規表現「.*@example.com」を使用してプロファイル キャッシュに格納されま

す。ユーザ名が user101@example.com で、パスワードが secretpassword2 である別のユーザもまた、同じ正規表現を使用して格納できます。「.*@example.com」プロファイルのユーザの数が何千にもなる可能性があるため、個人のパスワードを使用して各ユーザの認証を行うのは現実的ではありません。このため、認証はディセーブル化され、各ユーザは単にキャッシュに格納されている共通のアクセス応答の認証プロファイルにアクセスします。

Challenge Handshake Authentication Protocol（CHAP）、Microsoft チャレンジ ハンドシェイク認証プロトコル（MS-CHAP）、または拡張認証プロトコル（EAP）などの、クライアントと AAA オフロード サーバの間で暗号化されたパスワードを使用する高度なセキュリティ メカニズムを使用する場合に、同じ理論が当てはまります。認証プロファイルを処理するために、これらの一意で、安全なユーザ名とパスワードのプロファイルを許可するには、認証をバイパスします。

このフェールオーバー機能を利用するためには、ユーザがルータから認証されるときにキャッシュ サーバ グループが最後に照会されるように認証および認可の方式リストを設定する必要があります。詳細については、「認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト」を参照してください。

認可プロファイルおよび認証プロファイルのキャッシュ機能の方式リスト

方式リストとは、ユーザ認証のために照会される認証方式を記載したシーケンシャル リストです。サポートされているのは、ローカル（ローカルのデータベースを使用）、なし（なにも実行しない）、RADIUS サーバーグループ、または TACACS+ サーバーグループなどの方式です。通常は、複数の方式を方式リストに設定できます。ソフトウェアは、ユーザーを認証するため、リストに記載されている最初の方式が使用されます。その方式で応答に失敗した場合、ソフトウェアは、方式リストに記載されている次の認証方式を選択します。この処理は、リストのいずれかの認証方式で正常に通信できるか、方式リストで定義されているすべての方式を試行するまで続行されます。

ネットワークのパフォーマンスを最適化したり、プロファイル キャッシング機能を使用してフェールオーバー機能を有効にするには、方式リストの認証および認可の方式の順序を変更します。ネットワーク パフォーマンスを最適化するためには、キャッシュ サーバ グループが方式リストで最初に検出されるようにします。フェールオーバー機能を有効にするためには、キャッシュ サーバ グループが方式リストで最後に検出されるようにします。

認可プロファイルおよび認証プロファイルのキャッシュ機能に関するガイドライン

特定のアクセス ポイント（POP）の特定のルータで、認証および認可を要求できるユーザ名とプロファイルの数は相当な数になることがあるため、ユーザ名とプロファイルをすべてキャッシュするのは現実的ではありません。このため、ユーザ名およびプロファイルのうち、一般的に使用されるものや、一般的な認証応答や認可応答を共有するものだけをキャッシングに使用するように設定する必要があります。ドメインベースのサービスプロファイルに加え、America Online（AOL）のコールに使用される aolip や aolnet などの一般的に使用されるユーザ名や、公

衆電話交換網（PSTN）のコールを、ネットワークに接続されたストレージ デバイスに接続するのに使用される事前認証の着信番号識別サービス（DNIS）番号はいずれも、認証および認可のキャッシュ機能の効果が現れるユーザ名とプロファイルの例です。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための一般的な設定手順

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するには、次の手順を行います。

1. キャッシュ プロファイル グループを作成し、各グループのキャッシュに格納する情報についてのルールを定義します。

ユーザ名に正確に一致するエントリ、正規表現に一致するエントリ、またはすべての認証要求および認可要求をキャッシュに格納することを指定します。

1. 新しく定義したキャッシュ グループを参照するようにサーバ グループを更新します。
2. キャッシュに格納された情報を使用してネットワークのパフォーマンスを最適化したり、フェールオーバー メカニズムを有効にしたりするように認証または認可の方式リストを更新します。

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装方法

キャッシュ プロファイル グループの作成とキャッシュ処理ルールの定義

次の作業を行って、キャッシュ プロファイル グループを作成し、そのグループのキャッシュに格納する情報についてのルールを定義して、キャッシュ プロファイルのエントリの確認と管理を行います。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa cache profile** *group-name*
5. **profile** *name* [**no-auth**]
6. 手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。
7. **regexp** *matchexpression* {**any**| **only**}[**no-auth**]

8. 手順4で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。
9. **all** [**no-auth**]
10. **end**
11. **show aaa cache group** *name*
12. **clear aaa cache group** *name* {**profile** *name*| **all**}
13. **debug aaa cache group**

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： `Router> 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： `Router# 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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAAアクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa cache profile** *group-name* 例： `Router(config)# aaa cache profile networkusers@companyname`	認証および認可のキャッシュ プロファイル サーバ グループを定義し、プロファイル マップ コンフィギュレーション モードを開始します。
ステップ 5	**profile** *name* [**no-auth**] 例： `Router(config-profile-map# profile networkuser1 no-auth`	ユーザ名の一致に基づいて個々の認証および認可プロファイルのキャッシュを作成します。 • *name* 引数は、認証または認可のサービス要求によって照会されるユーザ名と正確に一致する必要があります。 • **no-auth** キーワードを使用して、このユーザーの認証をバイパスします。
ステップ 6	手順 4 のプロファイル グループに追加する各ユーザ名に対して手順 5 を繰り返します。	--
ステップ 7	**regexp** *matchexpression* {**any**| **only**}[**no-auth**] 例：	（任意）正規表現に基づいて、一致するエントリをキャッシュ プロファイル グループに作成します。

	コマンドまたはアクション	目的
	`Router(config-profile-map)# regexp .*@example.com any no-auth`	• **any** キーワードを使用すると、正規表現に一致する一意のユーザー名がすべて保存されます。 • **only** キーワードを使用すると、正規表現に一致するすべてのユーザー名に対して1つのプロファイルエントリのみがキャッシュされます。 • **no-auth** キーワードを使用して、このユーザーまたは一連のユーザーの認証をバイパスします。 • 正規表現のプロファイル グループ内のエントリの数が何千にもなる可能性があるため、そして各要求の検証を正規表現に対して行うと時間がかかる場合があるため、キャッシュプロファイル グループで正規表現を使用することは推奨されません。
ステップ 8	手順 4 で定義されたキャッシュ プロファイル グループに追加する各正規表現に対して手順 7 を繰り返します。	--
ステップ 9	**all** [**no-auth**] **例**： `Router(config-profile-map)# all no-auth`	（任意）認証要求および認可要求をすべてキャッシュに格納することを指定します。 • **all** コマンドは、特定のサービス認可要求に対して使用しますが、認証要求を処理するときは使用しないでください。
ステップ 10	**end** **例**： `Router(config-profile-map)# end`	特権 EXEC モードに戻ります。
ステップ 11	**show aaa cache group** *name* **例**： `Router# show aaa cache group networkusers@companyname`	（任意）指定したグループのすべてのキャッシュ エントリを表示します。
ステップ 12	**clear aaa cache group** *name* {**profile** *name*| **all**} **例**： `Router# clear aaa cache group networkusers@companyname profile networkuser1`	（任意）キャッシュの1つまたはすべてのエントリをクリアします。

	コマンドまたはアクション	目的
ステップ 13	**debug aaa cache group** 例： `Router# debug aaa cache group`	（任意）キャッシュに格納されているエントリのデバッグ情報を表示します。

キャッシュ プロファイル グループ情報を使用する RADIUS および TACACS サーバ グループの定義

このタスクを実行して、RADIUS および TACACS+ サーバ グループが各キャッシュ プロファイル グループに保存されている情報をどのように使用するかを定義します。

始める前に

RADIUS サーバ グループと TACACS+ サーバ グループが作成されている必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name*
5. **cache authorization profile** *name*
6. **cache authentication profile** *name*
7. **cache expiry** *hours* {**enforce failover**}
8. **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： `Router> 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： `Router# 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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。

	コマンドまたはアクション	目的
ステップ 4	**aaa group server radius** *group-name* or**aaa group server tacacs+** *group-name* 例： `Router(config)# aaa group server radius networkusers@companyname`	RADIUS サーバ グループ コンフィギュレーション モードを開始します。 • TACACS+ サーバー グループ コンフィギュレーション モードを開始するには、**aaa group server tacacs+** *group-name* コマンドを使用します。
ステップ 5	**cache authorization profile** *name* 例： `Router(config-sg-radius)# cache authorization profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認可のキャッシュ処理ルールをアクティブにします。 • このコマンドの *name* 引数は、AAA キャッシュ プロファイル グループ名です。
ステップ 6	**cache authentication profile** *name* 例： `Router(config-sq-radius)# cache authentication profile networkusers@companyname`	この RADIUS または TACACS+ サーバ グループのプロファイルのネットワーク ユーザで認証のキャッシュ処理ルールをアクティブにします。
ステップ 7	**cache expiry** *hours* {**enforce failover**} 例： `Router(config-sq-radius)# cache expiry 240 failover`	（オプション）キャッシュ プロファイルのエントリが期限切れになる（古くなる）までの時間を設定します。 • **enforce** キーワードは、期限切れになったキャッシュプロファイルのエントリを再使用しないことを指定するときに使用します。 • **failover** キーワードは、他のすべての方式でユーザーを認証および認可できなかった場合にキャッシュプロファイルの期限切れのエントリを使用することを指定するときに使用します。
ステップ 8	**end** 例： `Router(config-sg-radius)# end`	特権 EXEC モードに戻ります。

キャッシュ情報の使用方法を指定するための認可および認証の方式リストの更新

次の作業を行って、認可および認証のキャッシュ情報を使用するように認可および認証の方式リストを更新します。

始める前に

方式リストをすでに定義している必要があります。

手順の概要

1. **enable**
2. **configure terminal**
3. **aaa new-model**
4. **aaa authorization** {**network** | **exec** | **commands** *level* | **reverse-access**| **configuration**} {**default** | *list-name*} [*method1* [*method2...*]]
5. **aaa authentication ppp** {**default** | *list-name*} *method1* [*method2...*]
6. **aaa authentication login** {**default** | *list-name*} *method1* [*method2...*]
7. **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： `Router> 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： `Router# 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	**aaa new-model** 例： `Router(config)# aaa new-model`	AAA アクセス コントロール モデルをイネーブルにします。
ステップ 4	**aaa authorization** {**network**	**exec**	**commands** *level*	**reverse-access**| **configuration**} {**default**	*list-name*} [*method1* [*method2...*]] 例： `Router(config)# aaa authorization network default cache networkusers@companyname group networkusers@companyname`	AAA認可を有効にし、指定した機能にユーザがアクセスしたときに使用される認可方式を定義する方式リストを作成します。
ステップ 5	**aaa authentication ppp** {**default**	*list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication ppp default cache networkusers@companyname group networkusers@companyname`	PPP が実行されているシリアルインターフェイスで使用する 1 つまたは複数の認証方式を指定します。

	コマンドまたはアクション	目的
ステップ 6	**aaa authentication login** {**default** | *list-name*} *method1* [*method2...*] 例： `Router(config)# aaa authentication login default cache adminusers group adminusers`	ログイン時の認証を設定します。
ステップ 7	**end** 例： `Router(config)# end`	特権 EXEC モードに戻ります。

認可プロファイルおよび認証プロファイルのキャッシュ機能を実装するための設定例

ネットワークを最適化するための認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- ネットワーク上のすべての管理者名を含むキャッシュ プロファイル グループ adminusers を定義し、すべてのログイン セッションと exec セッションに使用するデフォルトのリストとして設定します。
- RADIUS サーバ グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最初に照会されるように方式の順序を変更します。

```
configure terminal

 aaa new-model

 ! Define aaa cache profile groups and the rules for what information is saved to cache.

 aaa cache profile admin_users

 profile adminuser1

 profile adminuser2

 profile adminuser3
```

```
 profile adminuser4

 profile adminuser5

 exit

 ! Define server groups that use the cache information in each profile group.

 aaa group server radius admins@companyname.com

 cache authorization profile admin_users

 cache authentication profile admin_users

 ! Update authentication and authorization method lists to specify how profile groups
and server groups are used.

 aaa authentication login default cache admins@companyname.com group admins@companyname.com

 aaa authorization exec default cache admins@companyname.com group admins@companyname.com

 end
```

フェールオーバーメカニズムとしての認可プロファイルおよび認証プロファイルのキャッシュ機能の実装例

次の設定例について説明します。

- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、管理者が引き続きネットワークにアクセスできるように、ネットワーク上のすべての管理者を含むキャッシュ プロファイル グループ admin_users を作成します。
- RADIUS サーバまたは TACACS+ サーバが万一使用できなくなった場合でも、ABC という会社のユーザがネットワークの使用を認可されるように、ネットワーク上のこれらのユーザをすべて含むキャッシュ プロファイル グループ abc_users を作成します。
- RADIUS サーバの各プロファイル グループの新しいキャッシュ処理ルールをアクティブにします。
- 新しいキャッシュ プロファイル グループを認証および認可の方式リストに追加し、このキャッシュ プロファイル グループが最後に照会されるように方式の順序を変更します。

```
configure terminal

 aaa new-model

 ! Define aaa cache profile groups and the rules for what information is saved to cache.
```

```
aaa cache profile admin_users

profile admin1

profile admin2

profile admin3

exit

aaa cache profile abcusers

profile .*@example.com only no-auth

exit

! Define server groups that use the cache information in each cache profile group.

aaa group server tacacs+ admins@companyname.com

server 10.1.1.1

server 10.20.1.1

cache authentication profile admin_users

cache authorization profile admin_users

exit

aaa group server radius abcusers@example.com

server 172.16.1.1

server 172.20.1.1

cache authentication profile abcusers

cache authorization profile abcusers

exit

! Update authentication and authorization method lists to specify how cache is used.

aaa authentication login default cache admins@companyname.com group admins@companyname.com

aaa authorization exec default cache admins@companyname.com group admins@companyname.com
```

```
aaa authentication ppp default group abcusers@example.com cache abcusers@example.com
aaa authorization network default group abcusers@example.com cache abcusers@example.com
end
```

RADIUS 認可変更に関する追加情報

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』
セキュリティ コマンド	• 『Security Command Reference: Commands A to C』 • 『Security Command Reference: Commands D to L』 • 『Security Command Reference: Commands M to R』 • 『Security Command Reference: Commands S to Z』
AAA の設定	『*Authentication, Authorization, and Accounting Configuration Guide*』

標準および RFC

標準/RFC	タイトル
RFC 2903	「*Generic AAA Architecture*」
RFC 5176	「*Dynamic Authorization Extensions to Remote Authentication Dial In User Service (RADIUS)*」

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

認可プロファイルおよび認証プロファイルのキャッシュ機能の実装の機能情報

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:* 認証プロファイルおよび認可プロファイルのキャッシュ機能の実装の機能情報

機能名	リリース	機能情報
AAA 認可および AAA 認証のキャッシュ	Cisco IOS XE Release 2.3	この機能により、ネットワークのパフォーマンスが最適化されるほか、RADIUS サーバまたは TACACS+ サーバが何らかの理由で使用できなくなった場合のフェールオーバー メカニズムが確立されます。 Cisco IOS XE Release 2.3 では、Cisco ASR 1000 シリーズ Aggregation Services Router にこの機能が実装されました。 次のコマンドが導入または変更されました。**aaa authentication login**、**aaa authentication ppp**、**aaa authorization**、**aaa cache profile**、**all (profile map configuration)**、**cache authentication profile (server group configuration)**、**cache authorization profile (server group configuration)**、**cache expiry (server group configuration)**、**clear aaa cache group**、**debug aaa cache group**、**profile (profile map configuration)**、**regexp (profile map configuration)**、**show aaa cache group**。

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。