



パフォーマンス拡張

この章では、最適な機能パフォーマンスのために適用できる機能拡張のヒントを紹介します。次の項目を取り上げます。

- 「RADIUS 順序変更 (ラウンドロビン)」 (P.3-47)
- 「RADIUS ロード バランシング」 (P.3-48)
- 「プロファイルのヒント」 (P.3-48)

RADIUS 順序変更 (ラウンドロビン)

RADIUS サーバを初期サーバとして設定し、初期 RADIUS サーバが動作していない場合にフェールオーバー サーバとして使用する RADIUS サーバのリストを設定できます。この機能は、デフォルトでディセーブルに設定されています。

次のグローバル コマンドは、この機能をイネーブルにするために使用されます。

```
radius-server retry method reorder
```

```
radius-server transactions max-tries <n>
```

RADIUS 順序変更が設定されていない場合

各 RADIUS サーバは、マーク付けされた非稼働状態になるまで使用されます。リストの先頭に最も近い動作可能なサーバが最初のトランザクション トランスミッションに設定された再送回数だけ使用されます。その後、リストの各動作可能なサーバが順に試されます (ラウンドロビン)。

RADIUS 順序変更が設定されている場合

次のプロセスで、初期 RADIUS サーバとして使用する RADIUS サーバを決定します。

- ネットワーク アクセス サーバ (NAS) が伝送を受信する最初のサーバとなる設定済みの RADIUS サーバにフラグを設定します。
- フラグ設定されたサーバにトランスミッションが送信された後は、設定された再送回数だけ、フラグ設定されたサーバにトランスミッションが再送されます。
- その後は、NAS が、フラグ設定されたサーバの次にリストされたサーバから始めて、設定されたトランザクションの最大再試行回数に到達するか、応答が返されるまで、サーバグループ内の動作可能な RADIUS サーバのリストの順にフェールオーバーします。
- ブート時に、フラグ設定されたサーバが CLI によって設定されたサーバグループ リスト内の最初の RADIUS サーバになります。

- (動作不能時間が 0 の場合でも) フラグ設定された RADIUS サーバが動作不能とマークされると、フラグ設定された RADIUS サーバの次にリストされた最初の動作可能な RADIUS サーバがフラグ設定された RADIUS サーバになります。
- フラグ設定された RADIUS サーバがリスト内の最後のサーバで、動作不能とマークされている場合、フラグ設定された RADIUS サーバがリスト内で最初に動作可能なサーバになります。
- すべてのサーバが動作不能とマークされている場合は、トランザクションが失敗して、フラグ設定された RADIUS サーバは変更されません。
- フラグ設定された RADIUS サーバが動作不能とマークされ、そのタイマーが切れると、アクションは実行されません。

RADIUS ロード バランシング

Cisco IOS ソフトウェアには、少数の未処理の要求を持つサーバに要求を送信する RADIUS ロードバランシング技術が含まれます。この機能をイネーブルにするには、(server-group コンフィギュレーションの一部である) 次のコマンドを使用します。

load-balance method least-outstanding [batch-size <n>]

例

```
nas(config)#aaa group server radius lbgroup
nas(config-sg-radius)#load-balance method least-outstanding [batch-size <n>]
```

説明：

batch-size <n> 少数の未処理の要求を持つサーバに割り当てられる要求の数 (ロードバランシングの後、少数の未処理の要求を持つサーバを確認するために再計算が実行されます)。

要求の割り当てをデバッグするには、次のコマンドを使用します。

debug aaa sg-server-selection

プロファイルのヒント

最適な機能パフォーマンスを得るには、Intelligent Services Gateway (ISG) に項目を定義し、可能な限りプロファイルを使用してそれらの項目を参照することを推奨します。

たとえば、ACL ベースのファイアウォール機能を定義するには、名前付き IP アクセス リストを ISG に設定してから、サービス プロファイルで名前付き IP アクセス リストを参照できます。

次のコマンド例では、ISG に名前付き IP アクセス リスト「personal-firewall」が設定されています。

```
ip access-list extended personal-firewall
  permit ...
  permit ...
  deny ...
```

その後、サービス プロファイルで名前付き IP アクセス リスト「personal-firewall」を参照できます。

```
Firewall          Password = "default"
                  Filter-ID = "personal-firewall.[in|out]"
```