



RADIUS サーバ障害発生時順序変更

RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバグループ内の別のサーバへのフェールオーバーを提供します。障害発生後は、すべての RADIUS トラフィックが新しいサーバに転送されます。新しいサーバからサーバグループ内の別のサーバにトラフィックが切り替えられるのは、新しいサーバでも障害が発生した場合に限られます。トラフィックが自動的に最初にサーバに戻されることはありません。

RADIUS トランザクションを複数のサーバに分散させることによって、認証要求とアカウントリング要求がより迅速に処理されます。

- [機能情報の確認 \(1 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更の前提条件 \(2 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更の制約事項 \(2 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更に関する情報 \(2 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更の設定方法 \(4 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更の設定例 \(8 ページ\)](#)
- [その他の参考資料 \(10 ページ\)](#)
- [RADIUS サーバ障害発生時順序変更の機能情報 \(11 ページ\)](#)

機能情報の確認

ご使用のソフトウェアリリースでは、このモジュールで説明されるすべての機能がサポートされているとは限りません。最新の機能情報および警告については、「[Bug Search Tool](#)」およびご使用のプラットフォームおよびソフトウェア リリースのリリース ノートを参照してください。このモジュールで説明される機能に関する情報、および各機能がサポートされるリリースの一覧については、機能情報の表を参照してください。

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。

RADIUS サーバ障害発生時順序変更の前提条件

- 障害発生時に順序変更を実行するように RADIUS サーバを設定する前に、**aaa new-model** コマンドを使用して、認証、認可、およびアカウントिंग (AAA) を有効にする必要があります。
- 認証、アカウントिंग、スタティック ルート ダウンロードなどの機能用に RADIUS を設定する必要もあります。

RADIUS サーバ障害発生時順序変更の制約事項

- サーバグループごとに新しい4バイトのメモリが消費されます。ただし、ほとんどのサーバは少数のサーバグループのみに設定されているため、追加の4バイトはそれほど性能に影響しない可能性があります。
- ソフトウェアセット内の RADIUS 機能によっては、この機能を使用できない場合があります。RADIUS 機能で RADIUS サーバ障害発生時順序変更機能を使用できない場合は、順序変更機能が設定されていないかのようにサーバが動作します。

RADIUS サーバ障害発生時順序変更に関する情報

RADIUS サーバの障害

RADIUS サーバ障害発生時順序変更機能が設定されていない状態でサーバの障害が発生した場合：

1. 新しい RADIUS トランザクションを実行する必要があります。
2. トランザクション用の RADIUS パケットが、グループ内で停止中としてマークされていない（設定されたデッドタイムに従って）最初のサーバに送信され、設定された再送回数だけ再送されます。
3. 再送のすべてがタイムアウトした（設定されたタイムアウトに従って）場合は、ルータがそのパケットをリストで次の非停止中サーバに設定された再送回数だけ送信します。
4. ステップ3は、トランザクションごとに指定された最大送信回数に達するまで繰り返されます。最大送信回数に到達する前にリストの最後に到達した場合は、ルータがリストの先頭に戻ってそこから処理を継続します。

このプロセスのどの時点でも、サーバが停止中サーバの検出基準（設定不可。使用されているソフトウェアのバージョンによって異なる）を満たした場合は、設定されたデッドタイムに合わせてサーバが停止中としてマークされます。

RADIUS サーバ障害発生時順序変更機能の動作方法

RADIUS サーバ障害発生時順序変更機能を設定した場合は、次のように、初期サーバとして使用する RADIUS サーバが決定されます。

- ネットワーク アクセス サーバ (NAS) は、トランスミッションが送信される最初のサーバである「フラグ設定された」サーバのステータスを保持します。
- 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フィックが再送されます。
- 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非停止中サーバのリストの順にトランスミッションを送信します。
- 起動時は、**radius-server host** コマンドを使用して設定されたように、フラグ設定されたサーバがサーバグループリストで最初のサーバになります。
- フラグ設定されたサーバが停止中としてマークされている場合は（デッドタイムが 0 の場合でも）、フラグ設定されたサーバの次にリストされた最初の非停止中サーバがフラグ設定されたサーバになります。
- フラグ設定されたサーバが、リスト内の最後のサーバで、停止中としてマークされている場合は、フラグ設定されたサーバがリスト内で停止中としてマークされていない最初のサーバになります。
- すべてのサーバが停止中としてマークされている場合は、トランザクションが失敗して、フラグ設定されたサーバへの変更が実施されません。
- フラグ設定されたサーバが停止中としてマークされており、デッドタイマーが切れた場合は、何も行われません。



- (注) トランスミッションのタイプ (チャレンジハンドシェイク認証プロトコル (CHAP)、Microsoft CHAP (MS-CHAP)、拡張可能認証プロトコル (EAP)) によっては、1 つのサーバを何度も往復しなければならない場合があります。これらの特別なトランザクションでは、サーバのラウンドトリップの全シーケンスは、1 つのトランスミッションと同じように処理されます。

RADIUS サーバが停止中の場合

次の 1 と 2 の基準が満たされた場合に、サーバを停止中としてマークすることができます。

1. **radius-server transaction max-tries** コマンドで指定された再送信回数を超えてサーバが応答しなかった場合。
2. 設定されたタイムアウトまでのどの要求にもサーバが応答しなかった場合。両方の基準 (これと上の基準) が満たされた場合にのみ、サーバが停止中としてマークされます。デッドタイムが 0 の場合でも、サーバを停止中としてマークすると、RADIUS サーバの再試行方式順序変更システムに重大な影響を及ぼします。

RADIUS サーバ障害発生時順序変更の設定方法

RADIUS サーバ障害発生時順序変更の設定

このタスクを実行して、サーバグループ内のあるサーバを、最初のサーバで障害が発生した場合に別のサーバにトラフィックを転送するように設定します。

手順の概要

1. `enable`
2. `configure terminal`
3. `aaa new-model`
4. `radius-server retry method reorder`
5. `radius-server retransmit {retries}`
6. `radius-server transaction max-tries { number }`
7. `radius-server host { hostname | ip-address } [key string]`
8. `radius-server host { hostname | ip-address } [key string]`

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： <pre>Router> enable</pre>	特権 EXEC モードをイネーブルにします。 <ul style="list-style-type: none"> • 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： <pre>Router# configure terminal</pre>	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： <pre>Router (config)# aaa new-model</pre>	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	radius-server retry method reorder 例： 例： <pre>Router (config)# radius-server retry method reorder</pre>	サーバグループ内の RADIUS トラフィック エントリの順序変更を指定します。

	コマンドまたはアクション	目的
ステップ 5	radius-server retransmit {retries} 例： <pre>Router (config)# radius-server retransmit 1</pre>	Cisco IOS XE ソフトウェアが RADIUS サーバホストのリストを検索する回数の最大値を指定します。 <i>retries</i> 引数は、再送信の最大試行回数です。デフォルトは 3 回に設定されています。
ステップ 6	radius-server transaction max-tries { number } 例： <pre>Router (config)# radius-server transaction max-tries 3</pre>	RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値を指定します。 <i>number</i> 引数は、トランザクション当たりのトランスミッション数の総数です。このコマンドが設定されなかった場合のデフォルトは 8 トランスミッションです。 (注) このコマンドは、特定のトランザクションに関するすべての RADIUS サーバに適用されます。
ステップ 7	radius-server host { hostname ip-address } [key string] 例： <pre>Router (config)# radius-server host 10.2.3.4 key radi23</pre>	RADIUS サーバホストを指定します。 (注) radius-server key コマンドを発行することによって、サーバ単位キーが設定されていないすべての RADIUS サーバのグローバルキーを設定することもできます。
ステップ 8	radius-server host { hostname ip-address } [key string] 例： <pre>Router (config)# radius-server host 10.5.6.7 key rad234</pre>	RADIUS サーバホストを指定します。 (注) 少なくとも 2 つのサーバを設定する必要があります。

RADIUS サーバ障害発生時順序変更のモニタリング

ルータ上でサーバ障害発生時順序変更プロセスをモニタするには、次のコマンドを使用します。

手順の概要

1. **enable**
2. **debug aaa sg-server selection**
3. **debug radius**

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 モードをイネーブルにします。 • パスワードを入力します（要求された場合）。
ステップ 2	debug aaa sg-server selection 例： Router# debug aaa sg-server selection	ルータ内の RADIUS および TACACS+ サーバグループシステムが特定のサーバを選択している理由に関する情報を表示します。
ステップ 3	debug radius 例： Router# debug radius	ルータが特定の RADIUS サーバを選択している理由に関する情報を表示します。

例

デバッグ 1

デバッグ 2

次の 2 つのデバッグ出力は、RADIUS サーバ障害発生時順序変更機能の動作を示しています。

次のサンプル出力では、RADIUS サーバ障害発生時順序変更機能が設定されています。サーバの再送は 0（したがって、次に設定されたサーバへのフェールオーバー前に、各サーバが一度だけ試行される）に設定され、トランザクション当たりのトランスミッション数は 4（3 回めのフェールオーバーでトランスミッション終了）に設定されています。サーバグループ内で 3 番めのサーバ（10.107.164.118）が、3 回めのトランスミッション（2 回めのフェールオーバー）のトランザクションを受け入れています。

```
00:38:35: %SYS-5-CONFIG-I: Configured from console by console
00:38:53: RADIUS/ENCODE(0000000F) : ask "Username: "
00:38:53: RADIUS/ENCODE (0000000F) : send packet; GET-USER
00:38:58: RADIUS/ENCODE (0000000F) : ask "Password: "
00:38:58: RADIUS/ENCODE(0000000F) : send packet; GET-PASSWORD
00:38:59: RADIUS: AAA Unsupported [152] 4
00:38:59: RADIUS: 7474 [tt]
00:38:59: RADIUS (0000000F) : Storing nasport 2 in rad-db
00:38:59: RADIUS/ENCODE(0000000F) : dropping service type, "radius-server attribute 6 on-for-login-auth" is off
00:38:59: RADIUS (0000000F) : Config NAS IP: 0.0.0.0
00:38:59: RADIUS/ENCODE (0000000F) : acct-session-id: 15
00:38:59: RADIUS (0000000F) : sending
00:38:59: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.1.1.1
00:38:59: RADIUS(0000000F) : Send Access-Request to 10.10.10.10:1645 id 21645/11, len 78
```

```
00:38:59: RADIUS:: authenticator 4481 E6 65 2D 5F 6F OA -1E F5 81 8F 4E 1478 9C
00:38:59: RADIUS: User-Name [1] 7 "username1"
00:38:59: RADIUS: User-Password [2] 18 *
00:38:59: RADIUS: NAS-Port fSl 6 2
00:~8:59: RADIUS: NAS-Port-Type [61] 6 Virtual [5]
00:38:59: RADIUS: Calling-Station-Id [31] 15 "10.19.192.23"
00:39:00: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:39:02: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/11
00:39:02: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 192.2.2.2
00:39:04: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/11
00:39:04: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 128.107.164.118
00:39:05: RADIUS: Received from id 21645/11 10.107.164.118:1645, Access-Accept, len 26
00:39:05: RADIUS: authenticator 5609 56 F9 64 4E DF 19- F3 A2 DD 73 EE 3F 9826
00:39:05: RADIUS: Service-Type [6] 6 Login [1]
```

次のサンプル出力では、RADIUSサーバ障害発生時順序変更機能が設定されています。サーバの再送は0に設定され、トランザクション当たりのトランスミッション数は8に設定されています。このトランザクションでは、サーバ10.10.10.0へのトランスミッションが8回めで失敗します。

```
00:42:30: RADIUS(00000011): Received from id 21645/13
00:43:34: RADIUS/ENCODE(00000012) : ask "Username: "
00:43:34: RADIUS/ENCODE(00000012) : send packet; GET-USER
00:43:39: RADIUS/ENCODE(00000012) : ask "Password: "
00:43:39: RADIUS/ENCODE(00000012) : send packet; GET-PASSWORD
00:43:40: RADIUS: AAA Unsupported [152] 4
00:43:40: RADIUS: 7474 [tt]
00:43:40: RADIUS(00000012) : Storing nasport 2 in rad-db
00:43:40: RADIUS/ENCODE(00000012): dropping service type, "radius-server attribute 6 on-for-login-auth" is off
00:43:40: RADIUS(00000012) : Co~fig NAS IP: 0.0.0.0
00:43:40: RADIUS/ENCODE(00000012) : acct-session-id: 18
00:43:40: RADIUS(00000012) : sending
00:43:40: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:40: RADIUS(00000012) : Send Access-Request to 10.107.164.118:1645 id 21645/14, len 78
00:43:40: RADIUS: authenticator B8 OA 51 3A AF A6 0018 -B3 2E 94 5E 07 OB 2A IF
00:43:40: RADIUS: User-Name [1] 7 "username1" 00:43:40: RADIUS: User-Password [2] 18 *
00:43:40: RADIUS: NAS-Port [5] 6 2
00:43:40: RADIUS: NAS-Port-Type [61] 6 Virtual [5] 00:43:40: RADIUS: Calling-Station-Id [31] 15 "172.19.192.23"
00:43:40: RADIUS: NAS-IP-Address [4] 6 10.0.1.130
00:43:42: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:42: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:44: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:44: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:46: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:46: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:48: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:48: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:50: RADIUS: Fail-over to (10.2.2.2:1645,1646) for id 21645/14
00:43:50: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.2.2.2
00:43:52: RADIUS: Fail-over to (10.107.164.118:1645,1646) for id 21645/14
00:43:52: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.107.164.118
00:43:54: RADIUS: Fail-over to (10.10.10.10:1645,1646) for id 21645/14
00:43:54: RADIUS/ENCODE: Best Local IP-Address 10.0.1.130 for Radius-Server 10.1.1.1
00:43:56: RADIUS: No response from (10.10.10.10:1645,1646) for id 21645/14 00:43:56: RADIUS/DECODE: parse response no app start; FAIL 00:43:56: RADIUS/DECODE: parse response; FAIL
```

RADIUS サーバ障害発生時順序変更の設定例

RADIUS サーバで障害発生時の順序変更を設定する例

次の設定例は、RADIUS サーバが障害発生時に順序変更されるように設定されます。RADIUS サーバ上で試行可能なトランザクション当たりのトランスミッション数の最大値は6です。

```
aaa new-model

radius-server retry method reorder

radius-server retransmit 0

radius-server transaction max-tries 6

radius-server host 10.2.3.4 key rad123

radius-server host 10.5.6.7 key rad123
```

RADIUS サーバが停止中の送信順序の決定

起動時に次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 0
Router(config)# radius-server transaction max-tries 6
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.5.6.7
```

両方のサーバがダウンしているが、まだ、停止中としてマークされていない場合は、最初のトランザクションで、次のようなトランスミッションが見られます。

```
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
10.2.3.4
10.5.6.7
```

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server transaction max-tries 3
Router(config)# radius-server host 10.2.3.4
Router(config)# radius-server host 10.4.5.6
```


両方の RADIUS サーバが RADIUS パケットに 응답していないが、まだ、停止中としてマークされていない (NASの起動後のため) 場合は、最初のトランザクションのトランスミッションが次のようになります。

```
10.2.3.4
10.2.3.4
10.4.5.6
```

以降のトランザクションは、別のパターンに従って転送されます。トランスミッションは、どちらか (または両方) のサーバを停止中としてマークする基準が満たされているかどうかと、前述したサーバのフラグ設定パターンによって異なります。

順序変更を次のように設定し、

```
Router(config)# aaa new-model
Router(config)# radius-server retry method reorder
Router(config)# radius-server retransmit 1
Router(config)# radius-server max-tries-per-transaction 8
Router(config)# radius-server host 10.1.1.1
Router(config)# radius-server host 10.2.2.2
Router(config)# radius-server host 10.3.3.3
Router(config)# radius-server timeout 3
```

RADIUS サーバ 10.1.1.1 が RADIUS パケットに 응답していないが、まだ、停止中としてマークされておらず、残りの 2 つの RADIUS サーバが動作中の場合は、次のように表示されます。

最初のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

サーバが停止中としてマークされる前に任意のトランスミッションに対して開始された追加のトランザクションの場合：

```
10.1.1.1
10.1.1.1
10.2.2.2
```

その後開始されたトランザクションの場合：

```
10.2.2.2
```

その後で、サーバの 10.2.2.2 と 10.3.3.3 もダウンした場合は、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされる基準を満たすまで、次のようなトランスミッションが見られます。

```
10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1
10.1.1.1
10.2.2.2
10.2.2.2
```

この後に、トランスマッションが失敗し、方式リスト内で次の方式が使用されます（存在する場合）。

サーバの 10.2.2.2 と 10.3.3.3 がダウンしたが、同時に、サーバ 10.1.1.1 が復旧した場合は、次のようになります。

10.2.2.2
10.2.2.2
10.3.3.3
10.3.3.3
10.1.1.1

その後で、サーバの 10.2.2.2 と 10.3.3.3 が停止中としてマークされると、次のようになります。

10.1.1.1

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
RADIUS	『Cisco IOS XE Security Configuration Guide: Securing User Services , Release 2』の「Configuring RADIUS」
AAA コマンドと RADIUS コマンド	『Cisco IOS Security Command Reference』
AAA の有効化	『Cisco IOS XE Security Configuration Guide: Securing User Services , Release 2』の「Authentication, Authorization, and Accounting (AAA)」
セキュリティ コマンド	『Cisco IOS セキュリティ コマンドリファレンス』

標準

標準	タイトル
この機能でサポートされる新規の規格または変更された規格はありません。また、既存の規格のサポートは変更されていません。	--

MIB

MIB	MIB のリンク
この機能によってサポートされる新しい MIB または変更された MIB はありません。またこの機能による既存 MIB のサポートに変更はありません。	<p>選択したプラットフォーム、Cisco IOS XE ソフトウェアリリース、およびフィーチャセットの MIB の場所を検索しダウンロードするには、次の URL にある Cisco MIB Locator を使用します。</p> <p>http://www.cisco.com/go/mibs</p>

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	--

シスコのテクニカル サポート

説明	リンク
<p>シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングにお役立ていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。</p> <p>お使いの製品のセキュリティ情報や技術情報を入力するために、Cisco Notification Service (Field Notice からアクセス)、Cisco Technical Services Newsletter、Really Simple Syndication (RSS) フィードなどの各種サービスに加入できます。</p> <p>シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。</p>	<p>http://www.cisco.com/en/US/support/index.html</p>

RADIUS サーバ障害発生時順序変更の機能情報

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 トレー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: RADIUS サーバ障害発生時順序変更の機能情報

機能名	リリース	機能情報
RADIUS サーバ障害発生時順序変更	Cisco IOS XE Release 2.1	<p>RADIUS サーバ障害発生時順序変更機能は、高負荷期間またはサーバで障害が発生した場合に、サーバグループ内の別のサーバへのフェールオーバーを提供します。</p> <p>この機能は、Cisco IOS XE Release 2.1 で Cisco ASR 1000 シリーズ アグリゲーション サービス ルータに導入されました。</p> <p>この機能により、次のコマンドが導入または変更されました。 debug aaa sg-server selection, radius-server retry method reorder, radius-server transaction max-tries.</p>