



# AAA の Kerberos サーバー

ここでは、AAA で使用する Kerberos サーバーの設定方法について説明します。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 Kerberos サーバーを使用できます。

- [AAA の Kerberos サーバーのガイドライン](#) (1 ページ)
- [AAA の Kerberos サーバーの設定](#) (1 ページ)
- [AAA の Kerberos サーバーのモニタリング](#) (6 ページ)
- [AAA の Kerberos サーバーの履歴](#) (7 ページ)

## AAA の Kerberos 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 Kerberos サーバーの設定

ここでは、Kerberos 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。

## Kerberos AAA サーバーグループの設定

認証に Kerberos サーバーを使用する場合は、最初に少なくとも 1 つの Kerberos 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。

## 手順

- ステップ 1** Kerberos 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 kerberos
```

例 :

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

- 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。

**ステップ 4** (任意) Kerberos キー発行局 (KDC) の検証を有効にします。

#### **validate-kdc**

例 :

```
ciscoasa(config-aaa-server-group)# validate-kdc
```

認証を実行するには、Kerberos キー発行局 (KDC) からエクスポートしたキータブファイルもインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようになる攻撃を防ぐことができます。

キータブファイルのアップロード方法については、[Kerberos キー発行局の検証の設定 \(5 ページ\)](#) を参照してください。

---

#### 例

次に、watchdogs という名前の Kerberos サーバーグループを作成し、サーバーを追加して、レルムを EXAMPLE.COM に設定する例を示します。

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
hostname(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
hostname(config-aaa-server-host)# exit
hostname(config)#
```

## Kerberos サーバーグループへの Kerberos サーバーの追加

Kerberos サーバーグループを使用する前に、少なくとも 1 つの Kerberos サーバーをグループに追加する必要があります。

#### 手順

**ステップ 1** Kerberos サーバーを Kerberos 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 サーバークラス内の **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 - 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 Kerberos ポート (TCP/88) 以外を使用する場合、サーバーポートを指定します。ASA は、このポートで Kerberos サーバーに接続します。

**server-port** *port\_number*

例：

```
ciscoasa(config-aaa-server-host)# server-port 8888
```

**ステップ 5** Kerberos レalm を設定します。

**kerberos-realm** *name*

Kerberos レalm 名では数字と大文字だけを使用し、64 文字以内にする必要があります。Microsoft Windows の **set USERDNSDOMAIN** コマンドを Kerberos レalm の Active Directory サーバー上で実行する場合は、**name** の値をこのコマンドの出力と一致させる必要があります。次の例では、EXAMPLE.COM が Kerberos レalm 名です。

```
C:\>set USERDNSDOMAIN  
USERDNSDOMAIN=EXAMPLE.COM
```

ASA では、**name** に小文字のアルファベットを使用できますが、小文字は大文字に変換されません。大文字だけを使用してください。

例：

```
ciscoasa(config-asa-server-group)# kerberos-realm EXAMPLE.COM
```

## 例

```
hostname(config)# aaa-server watchdogs protocol kerberos
hostname(config-aaa-server-group)# aaa-server watchdogs host 192.168.3.4
ciscoasa(config-aaa-server-host)# timeout 9
ciscoasa(config-aaa-server-host)# retry 7
ciscoasa(config-aaa-server-host)# kerberos-realm EXAMPLE.COM
ciscoasa(config-aaa-server-host)# exit
ciscoasa(config)#
```

## Kerberos キー発行局の検証の設定

グループ内のサーバーを認証するように Kerberos AAA サーバークラスを設定できます。認証を実行するには、Kerberos キー発行局 (KDC) からエクスポートしたキータブファイルをインポートする必要があります。KDC を検証することにより、攻撃者が KDC をスプーフィングして、ユーザークレデンシャルが攻撃者の Kerberos サーバーに対して認証されるようにする攻撃を防ぐことができます。

KDC の検証を有効にすると、チケット認可チケット (TGT) を取得してユーザーを検証した後、システムはホスト/ASA\_hostname のユーザーに代わってサービスチケットも要求します。次にシステムは、返されたサービスチケットを KDC の秘密鍵に対して検証します。これは、KDC から生成され、ASA にアップロードされたキータブファイルに保存されます。KDC 認証に失敗すると、サーバーは信頼できないと見なされ、ユーザーは認証されません。

次の手順では、KDC 認証を実行する方法について説明します。

### 始める前に

Kerberos 制約付き委任 (KCD) とともに KDC 検証を使用することはできません。サーバークラスが KCD に使用されている場合、**validate-kdc** コマンドは無視されます。

### 手順

- ステップ 1** (KDC 上。) Microsoft Active Directory で ASA のユーザーアカウントを作成します ([Start] > [Programs] > [Administrative Tools] > [Active Directory Users and Computers] に移動します)。たとえば、ASA の完全修飾ドメイン名 (FQDN) が asahost.example.com の場合は、asahost という名前のユーザーを作成します。
- ステップ 2** (KDC 上。) FQDN とユーザーアカウントを使用して、ASA のホストサービスプリンシパル名 (SPN) を作成します。

```
C:> setspn -A HOST/asahost.example.com asahost
```

ステップ3 (KDC上。) ASAのキータブファイルを作成します(わかりやすくするために改行を追加)。

```
C:\Users\Administrator> ktpass /out new.keytab +rndPass
/princ host/asahost@EXAMPLE.COM
/mapuser asahost@example.com
/ptype KRB5_NT_SRV_HST
/mapop set
```

ステップ4 (ASA上。) `aaa kerberos import-keytab` コマンドを使用して、キータブ(この例では `new.keytab`) を ASA にインポートします。

```
ciscoasa(config)# aaa kerberos import-keytab ftp://ftpsrv.example.com/new.keytab
ftp://ftpsrv.example.com/new.keytab imported successfully
```

ステップ5 (ASA上。) Kerberos AAA サーバークラス設定に `validate-kdc` コマンドを追加します。キータブファイルは、このコマンドが含まれているサーバークラスでのみ使用されます。

```
ciscoasa(config)# aaa-server svrgrp1 protocol kerberos
ciscoasa(config-aaa-server-group)# validate-kdc
```

## AAA の Kerberos サーバーのモニタリング

次のコマンドを使用して、Kerberos 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 kerberos [username user]**

すべての Kerberos チケットまたは特定のユーザー名のチケットを表示します。

- **clear aaa kerberos tickets [username user]**

すべての Kerberos チケットまたは特定のユーザー名のチケットをクリアします。

- **show aaa kerberos keytab**

Kerberos キータブファイルに関する情報を表示します。

- **clear aaa kerberos keytab**

Kerberos キータブファイルをクリアします。

## AAA の Kerberos サーバーの履歴

機能名	プラットフォームリリース	説明
Kerberos サーバー	7.0(1)	<p>AAA の Kerberos サーバーのサポート。</p> <p>次のコマンドを導入しました。</p> <p><b>aaa-server protocol、max-failed-attempts、reactivation-mode、aaa-server host、kerberos-realm、server-port、clear aaa-server statistics、clear configure aaa-server、show aaa-server、show running-config aaa-server、timeout。</b></p>
AAA の IPv6 アドレス	9.7(1)	<p>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。</p>
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)	<p>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）。</p> <p>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。</p> <p>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。<b>aaa-server、aaa-server host</b></p>
Kerberos キー発行局（KDC）認証。	9.8(4) およびそれ以降の 9.14(1) までの暫定リリース	<p>Kerberos キー配布局（KDC）からキータブファイルをインポートできます。システムは、Kerberos サーバーを使用してユーザーを認証する前にサーバーがスプーフィングされていないことを認証できます。KDC 認証を実行するには、Kerberos KDC でホスト/ASA_<i>hostname</i> サービスプリンシパル名（SPN）を設定してから、その SPN のキータブをエクスポートする必要があります。その後、キータブを ASA にアップロードし、KDC を検証するように Kerberos AAA サーバークラスを設定する必要があります。</p> <p><b>aaa kerberos import-keytab、clear aaa kerberos keytab、show aaa kerberos keytab、validate-kdc</b> の各コマンドが追加されました。</p>





## 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。