



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](#) (5 ページ)
- [AAA の Kerberos サーバーの履歴](#) (6 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 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。

ステップ 2 [AAA Server Group] 領域で、[Add] をクリックします。

[Add AAA Server Group] ダイアログボックスが表示されます。

ステップ 3 [Server Group] フィールドにグループの名前を入力します。

ステップ 4 [Protocol] ドロップダウンリストから、[Kerberos] サーバータイプを選択します。

ステップ 5 [Reactivation Mode] フィールドで、[Depletion] または [Timed] をクリックします。

[Depletion] モードの場合、障害が発生したサーバーは、グループ内のサーバーがすべて非アクティブになったときに限り、再アクティブ化されます。depletion モードでは、あるサーバーが非アクティブになった場合、そのサーバーは、グループの他のすべてのサーバーが非アクティブになるまで非アクティブのままとなります。すべてのサーバーが非アクティブになると、グループ内のすべてのサーバーが再アクティブ化されます。このアプローチでは、障害が発生したサーバーに起因する接続遅延の発生を最小限に抑えられます。

Timed モードでは、障害が発生したサーバーは 30 秒の停止時間の後で再アクティブ化されます。

ステップ 6 [Depletion] 再アクティブ化モードを選択した場合は、[Dead Time] フィールドに時間間隔を入力します。

デッド時間には、グループ内の最後のサーバーがディセーブルになってから、すべてのサーバーが再びイネーブルになるまでの時間間隔を分単位で指定します。デッドタイムは、ローカルデータベースへのフォールバックを設定した場合にのみ適用されます。認証は、デッドタイムが経過するまでローカルで試行されます。

ステップ 7 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。

このオプションで設定するのは、応答のないサーバーを非アクティブと宣言する前の AAA トランザクションの失敗回数です。

ステップ 8 (任意) Kerberos キー発行局 (KDC) の検証を有効にするには、[Validate KDC] を選択します。

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す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 \(4 ページ\)](#) を参照してください。

ステップ 9 [OK] をクリックします。

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 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択します。
- ステップ 2 サーバーを追加するサーバーグループを選択します。
- ステップ 3 [Servers in the Selected Group] 領域で、[Add] をクリックします。
サーバー グループに対応する [Add AAA Server Group] ダイアログボックスが表示されます。
- ステップ 4 [Interface Name] で、認証サーバーが存在するインターフェイス名を選択します。
- ステップ 5 グループに追加するサーバーの名前または IP アドレスを入力します。
- ステップ 6 サーバーへの接続試行のタイムアウト値を指定します。
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 retry interval) 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 サーバーグループ内の指定された maximum-failed-attempts 制限に達すると、AAA サーバーは非アクティブ化され、ASA は別の AAA サーバー (設定されている場合) への要求の送信を開始します。
- ステップ 7 再試行間隔を選択します。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。1〜10 秒の範囲で選択できます。デフォルトは 10 秒です。
- ステップ 8 サーバー ポートを指定します。サーバーポートは、ポート番号 88、または ASA によって Kerberos サーバーとの通信に使用される TCP ポートの番号です。
- ステップ 9 Kerberos レルムを設定します。
Kerberos レルム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 レルムの 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 レルム名です。

```
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。
- ステップ 10 [OK] をクリックします。

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、KDC検証オプションは無視されます。

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。) [Tools] > [File Management] の順に選択し、ファイルがワークステーションにあるかリモートサーバーにあるかに応じて、[File Transfer] メニューの該当するオプションを選択してキータブファイルをフラッシュにアップロードします。
- ステップ 5 (ASA 上。) [Configuration] > [Device Management] > [Users/AAA] > [AAA Kerberos] の順に選択し、[Browse Flash] をクリックして、アップロードしたキータブファイルを選択します。
- ステップ 6 (ASA 上。) Kerberos AAA サーバグループ設定に [Validate KDC] オプションを追加します。キータブファイルは、このオプションが設定されたサーバグループでのみ使用されます。
- [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の順に選択します。
 - Kerberos サーバグループを選択して [Edit] をクリックします。または、この時点で新しいグループを作成できます。
 - [Validate KDC] オプションを選択します。
 - [OK] をクリックします。

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。コマンドは [Tools] > [Command Line Interface] ウィンドウで入力します。

- [Monitoring] > [Properties] > [AAA Servers]

このウィンドウに AAA サーバーの統計情報が表示されます。

- **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)	AAA の Kerberos サーバーのサポート。 次の画面が導入されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]
AAA の IPv6 アドレス	9.7(1)	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。
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)	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）。 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。 これらの新しい制限を受け入れるために、AAA 画面が変更されました。
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	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 <code>ホスト/ASA_hostname</code> 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 サーバーグループを設定する必要があります。 次の画面が追加または変更されました。[Configuration] > [Device Management] > [Users/AAA] > [AAA Kerberos]、[Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] の Kerberos サーバーグループの [Add/Edit] ダイアログボックス。

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。