



AAA 用 Windows NT サーバの設定

この章では、AAA で使用される Windows NT サーバを設定する方法について説明します。具体的には、次の項目が含まれます。

- 「Windows NT サーバについての情報」 (P.37-1)
- 「Windows NT サーバのライセンス要件」 (P.37-1)
- 「注意事項と制約事項」 (P.37-2)
- 「Windows NT サーバの設定」 (P.37-2)
- 「Windows NT サーバ認証および許可のテスト」 (P.37-4)
- 「Windows NT サーバのモニタリング」 (P.37-5)
- 「Windows NT サーバの機能履歴」 (P.37-5)

Windows NT サーバについての情報

ASA では、NTLM バージョン 1 をサポートしている Microsoft Windows Server オペレーティング システム（ひとまとめにして「NT サーバ」と呼びます）がサポートされています。



(注)

NT サーバでは、ユーザ パスワードの最大長は 14 文字です。それより長いパスワードは、NTLM バージョン 1 の制限により切り捨てられます。

Windows NT サーバのライセンス要件

モデル	ライセンス要件
すべてのモデル	基本ライセンス

注意事項と制約事項

この項では、この機能のガイドラインと制限事項について説明します。

コンテキスト モードのガイドライン

シングル コンテキスト モードとマルチ コンテキスト モードでサポートされています。

ファイアウォール モードのガイドライン

ルーテッド ファイアウォール モードとトランスペアレント ファイアウォール モードでサポートされています。

IPv6 のガイドライン

IPv6 をサポートします。

その他のガイドライン

- シングル モードで最大 100 個のサーバ グループ、またはマルチ モードでコンテキストごとに 4 つのサーバ 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 4 台のサーバを含めることができます。
- ローカル データベースを使用してフォール バック サポートを設定する場合は、「[フォールバック サポート](#)」(P.33-2) と「[グループ内の複数のサーバを使用したフォールバックの仕組み](#)」(P.33-2) を参照してください。

Windows NT サーバの設定

この項では、次のトピックについて取り上げます。

- 「[Windows NT サーバ グループの設定](#)」(P.37-3)
- 「[Windows NT サーバのグループへの追加](#)」(P.37-3)

Windows NT サーバの設定のタスク フロー

-
- | | |
|--------|--|
| ステップ 1 | AAA サーバ グループを追加します。「 Windows NT サーバ グループの設定 」(P.37-3) を参照してください。 |
| ステップ 2 | サーバ グループの場合は、グループにサーバを追加します。「 Windows NT サーバのグループへの追加 」(P.37-3) を参照してください。 |
-

Windows NT サーバ グループの設定

認証、許可、またはアカウントिंगに Windows NT サーバを使用する場合は、最初に少なくとも 1 台の Windows NT サーバ グループを作成して、各グループに 1 台以上のサーバを追加します。Windows NT サーバ グループは名前で識別されます。

Windows NT サーバ グループに追加するには、次の手順を実行します。

手順の詳細

-
- 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 Groups] 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] フィールドで、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、NT ドメイン サーバ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は、グループ内のサーバ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。
Timed モードでは、障害が発生したサーバは 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。
[Dead Time] には、グループ内の最後のサーバがディセーブルになってから、すべてのサーバ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。
 - ステップ 7** [Max Failed Attempts] フィールドに、許容される試行の失敗回数を指定します。
このオプションで設定するのは、応答のないサーバを非アクティブと宣言するまでに許可される接続試行の失敗回数です。
 - ステップ 8** [OK] をクリックします。
[Add AAA Server Group] ダイアログボックスが閉じ、新しいサーバ グループが [AAA Server Groups] テーブルに追加されます。
 - ステップ 9** [AAA Server Groups] ダイアログボックスの [Apply] をクリックして、変更内容を実行コンフィギュレーションに保存します。
-

Windows NT サーバのグループへの追加

Windows NT サーバをグループに追加するには、次の手順を実行します。

手順の詳細

-
- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域で、サーバを追加するサーバ グループをクリックします。
テーブル内の該当する行が選択されます。
 - ステップ 2** [Selected Group] 領域の [Servers] (下部ペイン) で、[Add] をクリックします。

サーバ 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 3** [Interface Name] ドロップダウン リストから、認証サーバが常駐するインターフェイスの名前を選択します。
- ステップ 4** [Server Name] フィールドまたは [IP Address] フィールドに、グループに追加するサーバの名前または IP アドレスを入力します。
- ステップ 5** [Timeout] フィールドで、タイムアウト値を入力します。デフォルト値をそのまま使用することもできます。[Timeout] フィールドには、バックアップ サーバへ要求を送信した ASA が、プライマリ サーバからの応答を待機する時間を秒単位で指定します。
- ステップ 6** サーバ ポートを指定します。サーバ ポートはポート番号 139 または Windows NT サーバとの通信に ASA に使用される TCP ポート番号です。
- ステップ 7** ドメイン コントローラ名を指定します。ドメイン コントローラは、このサーバの NT プライマリ ドメイン コントローラのホスト名です (15 文字以下、例 PDC01)。ここに入力する名前は、[Authentication Server Address] フィールドに IP アドレスを入力したサーバのホスト名に一致している必要があります。一致していないと、認証は失敗します。
- ステップ 8** [OK] をクリックします。
[Add AAA Server Group] ダイアログボックスが閉じ、AAA サーバが AAA サーバ グループに追加されます。
- ステップ 9** [AAA Server Groups] ペインで [Apply] をクリックし、変更内容を実行コンフィギュレーションに保存します。

Windows NT サーバ認証および許可のテスト

ASAにおいて Windows NT サーバにアクセスし、ユーザの認証および許可が実行できるかどうかを判定するには、次の手順を実行します。

- ステップ 1** [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups] を選択し、[AAA Server Groups] 領域でサーバが存在するサーバ グループをクリックします。
テーブル内の該当する行が選択されます。
- ステップ 2** [Selected Group] テーブルの [Servers] から、テストするサーバをクリックします。
テーブル内の該当する行が選択されます。
- ステップ 3** [Test] をクリックします。
選択したサーバに対応する [Test AAA Server] ダイアログボックスが表示されます。
- ステップ 4** 実行するテストのタイプ ([Authentication] または [Authorization]) をクリックします。
- ステップ 5** [Username] フィールドにユーザ名を入力します。
- ステップ 6** 認証をテストする場合は、そのユーザ名に対応するパスワードを [Password] フィールドに入力します。
- ステップ 7** [OK] をクリックします。
認証または許可のテスト メッセージが ASA からサーバへ送信されます。テストが失敗した場合は、ASDM によりエラー メッセージが表示されます。

Windows NT サーバのモニタリング

Windows NT サーバをモニタするには、次のペインを確認します。

パス	目的
[Monitoring] > [Properties] > [AAA Servers]	設定済みの Windows NT サーバの統計情報を表示します。
[Monitoring] > [Properties] > [AAA Servers]	Windows NT サーバ実行コンフィギュレーションを表示します。

Windows NT サーバの機能履歴

表 37-1 に、各機能変更と、それが実装されたプラットフォーム リリースを示します。ASDM は、複数のプラットフォーム リリースとの下位互換性があるため、サポートが追加された特定の ASDM リリースは一覧には含まれていません。

表 37-1 Windows NT サーバの機能履歴

機能名	プラットフォーム リリース	機能情報
AAA 用 Windows NT サーバ	7.0(1)	Windows NT サーバのサポートと AAA 用に設定する方法について説明します。 次の画面が導入されました。 [Configuration] > [Device Management] > [Users/AAA] > [AAA Server Groups]

