



## ユーザ アクセスの制御

---

この章は、次の項で構成されています。

- 「ユーザの管理」 (P.15-1)
- 「ユーザ パスワードの変更」 (P.15-2)
- 「ユーザ権限の変更」 (P.15-2)
- 「ユーザ グループの管理」 (P.15-3)
- 「パスワード ポリシーの変更」 (P.15-4)
- 「AAA モードの設定」 (P.15-4)
- 「仮想ドメインの変更」 (P.15-4)
- 「アクセスの監査」 (P.15-5)
- 「監査ログの表示」 (P.15-6)
- 「TACACS+ サーバの追加」 (P.15-7)
- 「RADIUS サーバの追加」 (P.15-7)

## ユーザの管理

すべての Prime NCS (WAN) ユーザは、ユーザ名とパスワードなどの基本パラメータを持っています。admin 権限を持つユーザはアクティブ ユーザ セッションを表示できます。

アクティブ セッションを表示するには、次の手順に従います。

---

**ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[Active Sessions] をクリックします。

**ステップ 2** ユーザ名に対応する [Audit Trail] アイコンをクリックすると、次のデータが表示されます。

- [User] : ユーザ ログイン名
- [Operation] : 監査する操作のタイプ
- [Time] : 操作が監査された時刻
- [Status] : 成功または失敗
- [Reason] : ユーザ ログインが失敗した場合の失敗の理由
- [Configuration Changes] : 設定変更があると、このフィールドには [Details] リンクが設けられます。個別のユーザが行った設定変更の詳細については、[Details] リンクをクリックしてください。



(注) 監査証跡エントリは、個別のデバイス変更に関してログに記録されることがあります。たとえば、テンプレートが複数のスイッチに適用された場合、テンプレートの適用先のスイッチごとに、複数の監査証跡エントリが存在することになります。

## ユーザの追加

ユーザを追加して、事前定義済みの静的ロールを割り当てることができます。完全なアクセス以外に、区別した権限で特定のユーザグループに対して管理アクセスを付与できます。Prime NCS (WAN) はこれらのアクセス制限を使用して外部ユーザの認証をサポートし、TACACS+ サーバおよび RADIUS サーバに対してユーザを認証します。

- 
- ステップ 1 [Administration] > [Users, Roles & AAA] を選択し、[Users] をクリックします。
  - ステップ 2 [Add a User] を選択し、[Go] をクリックします。
  - ステップ 3 新しいユーザのユーザ名、パスワード、および確認パスワードを入力し、このユーザが属するグループを選択します。
  - ステップ 4 [Virtual Domains] タブをクリックして仮想ドメインをこのユーザに割り当てます。[仮想ドメインの変更](#)を参照してください。
  - ステップ 5 [Save] をクリックします。
- 

## ユーザパスワードの変更

ユーザのパスワードを変更するには、次の手順に従います。

- 
- ステップ 1 [Administration] > [Users, Roles & AAA] を選択し、[Users] をクリックします。
  - ステップ 2 パスワードを変更するユーザの名前を選択します。
  - ステップ 3 パスワードフィールドに入力し、[Save] をクリックします。
- 

## ユーザ権限の変更

Prime NCS (WAN) はタスクのリストを使用して、ユーザが Prime NCS (WAN) のいずれの部分にアクセスできるか、およびその部分でユーザが実行できる機能を制御します。Prime NCS (WAN) におけるユーザ権限の変更は、各ユーザが属するユーザグループを変更して行います。各グループのいずれのユーザに実行を認可するか、およびそのユーザがアクセスできる画面を変更するには、ユーザグループのタスクリストを使用します。

仮想ドメインがアクセスできるサイトまたはデバイスを割り当てることもできます。

ユーザグループのタスクリストを編集するには、次の手順に従います。

- ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[User Groups] をクリックします。
- ステップ 2** グループ名をクリックして、このグループに実行を許可するタスクを変更します。
- ステップ 3** [Members] タブをクリックして、このグループのユーザを表示します。

## ユーザグループの管理

Prime NCS (WAN) には、に説明されている事前定義済みのユーザグループがあります。ユーザの権限を変更できますが、追加ユーザを加えることはできません。新しいユーザを作成した場合は、そのユーザをグループに割り当てます。

表 15-1 に、Prime NCS (WAN) のデフォルト ユーザグループとその権限を示します。

表 15-1 デフォルト ユーザグループ

| グループ名             | グループのユーザの権限   |
|-------------------|---|
| System Monitoring | Prime NCS (WAN) の動作をモニタします。   |
| ConfigManagers    | Prime NCS (WAN) の動作をモニタおよび設定します。  |
| Admin             | Prime NCS (WAN) の動作をモニタおよび設定して、Prime NCS (WAN) のユーザアカウントおよびパスワードの管理を除いたすべてのシステム管理タスクを実行します。   |
| SuperUsers        | Prime NCS (WAN) の動作をモニタおよび設定して、Prime NCS (WAN) のユーザアカウントおよびパスワードの管理を含むすべてのシステム管理タスクを実行します。スーパーユーザのタスクは、変更できます。  |
| North bound API   | Prime NCS (WAN) Navigator だけで使用されます。  |
| User Assistant    | ローカル ネット ユーザ管理のみ。ユーザアシスタントではデバイスを設定またはモニタできません。   |
| Lobby Ambassador  | ユーザアカウントの設定と管理だけのゲストアクセス。   |
| Monitor lite      | 資産ロケーションのモニタリング。  |
| Root              | Prime NCS (WAN) の動作をモニタおよび設定して、任意のパスワードの変更を含むすべてのシステム管理タスクを実行します。このグループに割り当てることができるユーザは 1 つだけで、インストールの際に決定されます。このユーザをシステムから削除できません。また、このユーザに対してタスクを変更できません。 |

ユーザグループとそれに関連付けられているタスクを表示するには、次の手順に従います。

- ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[User Groups] をクリックします。
- ステップ 2** グループ名をクリックして、このグループに実行を許可するタスクを変更します。
- ステップ 3** [Members] タブをクリックして、このグループのユーザを表示します。

## 仮想ドメインアクセスの変更

仮想ドメインがアクセスできるサイトまたはデバイスを編集するには、次の手順に従います。

- 
- ステップ 1 [Administration] > [Virtual Domains] を選択します。
  - ステップ 2 サイトまたはデバイスの割り当て先ドメインを選択します。
  - ステップ 3 [Sites] タブまたは [Devices] タブをクリックし、必要な項目を [Available] リストから [Selected] リストに移動します。
  - ステップ 4 [Submit] をクリックします。
- ユーザを仮想ドメインに関連付けるには、[Administration] > [Users, Roles & AAA] を選択し、[Users] をクリックします。仮想ドメインへのユーザの割り当てを参照してください。
- 

## パスワードポリシーの変更

Prime NCS (WAN) は、最小長、繰り返し文字など、さまざまなパスワードポリシー制御をサポートしています。

パスワードポリシーを変更するには、次の手順に従います。

- 
- ステップ 1 [Administration] > [Users, Roles & AAA] を選択し、[Local Password Policy] をクリックします。
  - ステップ 2 必要なポリシーを選択し、[Save] をクリックします。
- 

## AAA モードの設定

Prime NCS (WAN) は、ローカルと TACACS+ および RADIUS をサポートしていますが、先に TACACS+ または RADIUS サーバを指定する必要があります。

TACACS+ サーバを指定して AAA モードを TACACS+ に変更するには、次の手順に従います。

- 
- ステップ 1 [Administration] > [Users, Roles & AAA] を選択し、[TACACS+] をクリックします。
  - ステップ 2 コマンドプルダウンメニューから [Add TACACS+ Server] を選択し、[Go] をクリックします。
  - ステップ 3 TACACS+ サーバパラメータを入力し、[Save] をクリックします。
  - ステップ 4 [AAA Mode] をクリックします。
  - ステップ 5 [TACACS+] を選択し、ローカル状態へのフォールバックを有効にするかどうかを指定します。
  - ステップ 6 [Save] をクリックします。
- 

## 仮想ドメインの変更

Prime NCS (WAN) の仮想ドメインは、Prime NCS (WAN) の一連のデバイスまたはマップ、あるいはその両方で構成され、これらの管理対象オブジェクトに関連する情報にユーザビューを制限します。

仮想ドメインを使用して、管理者はユーザが担当するデバイスおよびマップだけを表示できるようにすることができます。また、仮想ドメインのフィルタにより、ユーザはネットワークの割り当てられた部分だけについて、アラームを設定、表示およびレポートを生成できます。

管理者は、各ユーザに使用できる仮想ドメインを指定します。ログインの際、ユーザについてこれらのドメインのうちアクティブとなるのは 1 つだけです。ユーザは、ページ上部の [Virtual Domain] ドロップダウンリストで別の有効な仮想ドメインを選択して、現在の仮想ドメインを変更できます。仮想ドメインによって、すべてのレポート、アラーム、およびその他の機能がフィルタ処理されます。

システムに定義されている仮想ドメインが 1 つだけ（「root」）であり、かつ TACACS+/RADIUS サーバにカスタム属性フィールドの仮想ドメインがない場合、ユーザにはデフォルトで「root」の仮想ドメインが割り当てられます。仮想ドメインが複数あり、ユーザに指定された属性がない場合、ユーザのログインはブロックされます。

サイトおよびデバイスを仮想ドメインに追加するには、次の手順に従います。

- 
- ステップ 1** [Administration] > [Virtual Domains] を選択します。
  - ステップ 2** 左の [Virtual Domain Hierarchy] サイドバーメニューで、サイトまたはデバイスの追加先の仮想ドメインをクリックします。
  - ステップ 3** サイトおよびデバイスを [Available] カラムから [Selected] カラムに移動し、[Submit] をクリックします。
- 

仮想ドメインにユーザを追加するには、次の手順に従います。

- 
- ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[Users] をクリックします。
  - ステップ 2** 仮想ドメインに追加するユーザをクリックします。
  - ステップ 3** [Virtual Domains] タブをクリックします。
  - ステップ 4** ユーザの追加先の仮想ドメインを [Available Virtual Domains] カラムから [Selected Virtual Domains] カラムに移動し、[Save] をクリックします。
- 



**(注)** 各仮想ドメインには、親仮想ドメインに含まれている要素のサブセットが含まれている場合があります。ユーザが仮想ドメインに割り当てられると、そのユーザは仮想ドメインに割り当てられているデバイスを表示できます。

---

## アクセスの監査

Prime NCS (WAN) は、ユーザアクセスの監査レコードを維持します。

ユーザまたはユーザのアクティブセッションの監査証跡にアクセスするには、次の手順に従います。

- 
- ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[Active Sessions] をクリックします。
  - ステップ 2** ユーザ名に対応する [Audit Trail] アイコンをクリックすると、次のデータが表示されます。
    - [User] : ユーザ ログイン名
    - [Operation] : 監査する操作のタイプ
-

- [Time] : 操作が監査された時刻
- [Status] : 成功または失敗
- [Configuration Changes] : 設定変更があると、このフィールドには [Details] リンクが設けられません。個別のユーザが行った設定変更の詳細については、[Details] リンクをクリックしてください。



(注) 監査証跡エントリは、個別のデバイス変更に関してログに記録されることがあります。たとえば、テンプレートが複数のスイッチに適用された場合、テンプレートの適用先のスイッチごとに、複数の監査証跡エントリが存在することになります。

ユーザグループの監査証跡にアクセスするには、次の手順に従います。

**ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[User Groups] をクリックします。

**ステップ 2** ユーザ名に対応する [Audit Trail] アイコンをクリックすると、次のデータが表示されます。

- [User] : ユーザ ログイン名
- [Operation] : 監査する操作のタイプ
- [Time] : 操作が監査された時刻
- [Status] : 成功または失敗
- [Configuration Changes] : 設定変更があると、このフィールドには [Details] リンクが設けられません。個別のユーザが行った設定変更の詳細については、[Details] リンクをクリックしてください。



(注) 監査証跡エントリは、個別のデバイス変更に関してログに記録されることがあります。たとえば、テンプレートが複数のスイッチに適用された場合、テンプレートの適用先のスイッチごとに、複数の監査証跡エントリが存在することになります。

## 監査ログの表示

Prime NCS (WAN) には、次の 2 種類の監査ログがあります。

- **Application Audit ログ** : Prime NCS (WAN) の機能に関するログ イベント。たとえば、アプリケーション監査ログを表示して、特定のユーザがログインした日時と行ったアクションの内容を見ることができます。
- **Network Audit ログ** : ネットワークのデバイスに関するログ イベント。たとえば、ネットワーク監査ログを表示して、特定のテンプレートを展開したユーザとテンプレートが展開された日時を見ることができます。

**ステップ 1** [Administration] > [Audit Logs] を選択します。

**ステップ 2** [Application Audit] タブまたは [Network Audit] タブをクリックします。



(注) [Application Audit] の場合、TACACS+/RADIUS ユーザでは [User Group] カラムが空白になります。

**ステップ 3** ログに関する詳細を表示するには、詳細を表示する行をクリックして展開します。

## TACACS+ サーバの追加

TACACS+ サーバと通信できるように Prime NCS (WAN) を設定するには、次の手順に従います。

**ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[TACACS+] をクリックします。

**ステップ 2** [Add TACACS+ Server] を選択し、[Go] をクリックします。

**ステップ 3** TACACS+ サーバ情報を入力し、[Save] をクリックします。



(注) Prime NCS (WAN) が TACACS+ サーバと通信するには、このページで入力した共有秘密キーが、TACACS+ サーバに設定された共有秘密キーと一致している必要があります。

## RADIUS サーバの追加

RADIUS サーバと通信できるように Prime NCS (WAN) を設定するには、次の手順に従います。

**ステップ 1** [Administration] > [Users, Roles & AAA] を選択し、[RADIUS Servers] をクリックします。

**ステップ 2** [Add Radius Server] を選択し、[Go] をクリックします。

**ステップ 3** RADIUS サーバ情報を入力し、[Save] をクリックします。



(注) Prime NCS (WAN) が RADIUS サーバと通信するには、このページで入力する共有秘密キーが、RADIUS サーバに設定された共有秘密キーと一致している必要があります。

