

オフラインVBond/VSmartのユーザ名とパスワードのリセット

内容

[はじめに](#)

[前提条件](#)

[要件](#)

[使用するコンポーネント](#)

[問題](#)

[基本概念](#)

[Ciscotacユーザアクセス](#)

[ソリューション](#)

[ステップ1:ciscotacrwを使用して、SSHログイン経由でvBondorvSmartにアクセスします。](#)

[ステップ2：既存のユーザパスワードのリセット](#)

[ステップ3：新しいNetadminユーザを追加する（オプション）](#)

[ステップ4：ロックされたアカウントのロックを解除する（該当する場合）](#)

[ステップ5.設定の確認](#)

[関連情報](#)

はじめに

このドキュメントでは、SD-WANオフラインvBond/vSmartのユーザ名とパスワードをリセットする方法について説明します。

前提条件

要件

次の項目に関する知識があることが推奨されます。

- Ciscoソフトウェア定義型ワイドエリアネットワーク(SD-WAN)

使用するコンポーネント

このドキュメントの情報は、Cisco vManagerバージョン20.9.4に基づくものです。

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されたものです。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。本稼働中のネットワークでは、各コマンドによって起こる可能性がある影響を十分確認してください。

問題

vBondとvSmartsへのアクセスが失われました。これは、いずれかのインターフェイスへのログイン試行が過剰に失敗した後、クレデンシャルを知らないか覚えていない場合、またはアクセスがロックされている場合に発生します。同時に、vManage、vSmarts、およびvBond間の制御接続も中断されます。オフラインのvbondとvsmartは、vmanage GUIからは操作できません。

基本概念

Ciscotacユーザアクセス

Cisco Edgeソフトウェアには、Ciscoサポートチーム専用の2人のユーザ（ciscotacroおよびciscotacrw）が用意されています。これらのユーザは、クラウドとオンプレミスの両方のインストールで使用できます。これらは、同意トークンチャレンジおよびトークン応答認証で動作します。この認証では、新しいログインセッションごとに新しいトークンが必要です。ciscotacroおよびciscotacrwのユーザは、このトークンを使用して、Cisco SD-WAN Manager Webサーバ、およびCisco SD-WAN ManagerのSSH端末にログインできます。これらのユーザは、Cisco SD-WAN ManagerのSSH端末を使用して、Cisco SD-WAN Validator、Cisco SD-WAN コントローラ、およびCisco vEdgeデバイスにアクセスすることもできます。

デフォルトのCLIテンプレートには、ciscotacroおよびciscotacrwユーザ設定が含まれています。これらのユーザはデフォルトで有効になっています。ただし、必要に応じてこれらのユーザを無効にすることができます。

- ciscotacroユーザ：このユーザは、読み取り専用権限のみを持つoperatorユーザグループの一部です。このユーザは、設定のモニタだけが可能で、ネットワークの設定を変更する操作は実行できません。
- ciscotacrwユーザ：このユーザは、読み取り/書き込み権限を持つnetadminユーザグループの一部です。このユーザは、ネットワーク設定を変更できます。また、このユーザだけが同意トークンを使用してルートシェルにアクセスできます。

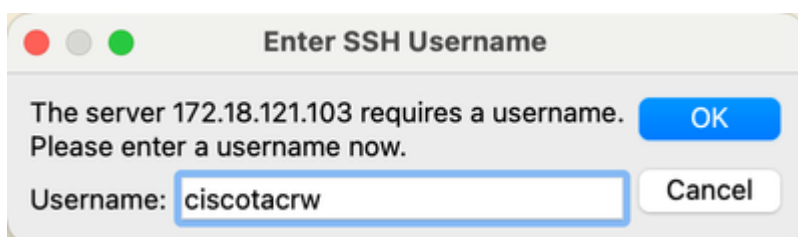


注: 「ciscotac」ユーザアカウントが導入され、バージョン20.x前後のCisco SD-WANソフトウェアリリースからデフォルトで含まれています。

ソリューション

ステップ1:ciscotacrwを使用して、SSHログイン経由でvBondまたはvSmartにアクセスします。

- ユーザ名として「ciscotacrw」と入力します。



- OKをクリックすると、それに応じてConsent Token Challengeフレーズが生成されます。



- 「Consent Token Challenge phrase」をSR case経由でTACに提供する必要があります。TACは対応する「sdwanchallenge-response token」を返します。
- 「sdwanchallenge-response token」と入力します。

ステップ2：既存のユーザパスワードのリセット

ciscotacrwアカウント（認証用のconsent-tokenを使用）を使用してオフラインvBond/vSmartにログインした後、ユーザ名とパスワードを復元またはリセットできます。

- 設定モードに入り、既存のユーザ（adminなど）のパスワードをリセットします。

```
vBond# config terminal
vBond(config)# system aaa user admin password <new password>
vBond(config)# commit
```



注：送信後、システムは自動的にプレーンテキストパスワードを暗号化します。

ステップ3：新しいNetadminユーザを追加する（オプション）

新しい管理者アカウントを作成する必要がある場合：

```
vBond(config)# system aaa user <new username> password <new password>
vBond(config)# system aaa user <new username> group netadmin
vBond(config)# commit
```

ステップ4：ロックされたアカウントのロックを解除する（該当する場合）

ログインに複数回失敗したためにアカウントがロックされた場合は、次のコマンドを使用してロックを解除できます。

```
request aaa unlock-user <username>
```

ステップ5.設定の確認

- show running-config system aaaコマンドを使用して、ユーザ設定が正しく適用されていることを確認します。
- 新しいクレデンシャルでログインし、回復が成功したことを確認します。



注:vBondはオフライン状態（vManageに関連付けられていないか、切断されていない）であるため、vManageからテンプレートを発行するのではなく、CLIを使用して直接設定を完了することをお勧めします。



警告：完了後、vManageで管理接続を再確立する必要がある場合は、認証情報がvManageの設定と一致していることを確認してください。

関連情報

- [制御接続が確立されたときにSD-WAN vSmartおよびvBondアクセスを回復する](#)
- [Ciscotacユーザアクセス](#)

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。