

Setzen Sie den Benutzernamen und das Passwort des Offline-vBond/vSmart zurück.

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Problem](#)

[Grundkonzept](#)

[CiscoTac-Benutzerzugriff](#)

[Lösung](#)

[Schritt 1: Zugriff auf vBond/vSmart über SSH-Anmeldung mit ciscotacrw](#)

[Schritt 2: Setzen Sie das vorhandene Benutzerkennwort zurück.](#)

[Schritt 3: Neuen NetAdmin-Benutzer hinzufügen \(optional\)](#)

[Schritt 4: Entsperren Sie das gesperrte Konto \(falls zutreffend\).](#)

[Schritt 5: Überprüfen der Konfiguration](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument wird beschrieben, wie Sie den Benutzernamen und das Kennwort für das SD-WAN-Offline-vBond/vSmart zurücksetzen.

Voraussetzungen

Anforderungen

Cisco empfiehlt, dass Sie über Kenntnisse in folgenden Bereichen verfügen:

- Cisco Software-defined Wide Area Network (SD-WAN).

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf Cisco vManager Version 20.9.4

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Problem

Der Zugriff auf vBonds und vSmarts wurde unterbrochen. Dies geschieht, wenn Sie Ihre Anmeldeinformationen nicht kennen oder sich nicht daran erinnern, oder wenn der Zugriff nach überzogenen und erfolglosen Versuchen, sich bei einer der Schnittstellen anzumelden, gesperrt wird. Gleichzeitig werden die Steuerungsverbindungen zwischen vManage, vSmarts und vBonds unterbrochen. Offline-Bond und vsmart können nicht über die vmanagement-GUI bedient werden.

Grundkonzept

CiscoTac-Benutzerzugriff

Die Cisco Edge-Software stellt zwei Benutzer zur Verfügung - ciscotacro und ciscotacrw - die nur vom Cisco Support-Team verwendet werden dürfen. Diese Benutzer sind sowohl für Cloud- als auch für standortbasierte Installationen verfügbar. Sie arbeiten mit einer Zustimmungs-Token-Abfrage und einer Token-Antwortauthentifizierung, bei der für jede neue Anmeldesitzung ein neues Token erforderlich ist. Benutzer von Cisco und Cisco können sich mit diesem Token beim Cisco SD-WAN Manager-Webserver sowie beim SSH-Terminal des Cisco SD-WAN Manager anmelden. Diese Benutzer können auch über das SSH-Terminal des Cisco SD-WAN Managers auf den Cisco SD-WAN-Validator, die Cisco SD-WAN-Controller und die Cisco vEdge-Geräte zugreifen.

Die Standard-CLI-Vorlagen umfassen die Benutzerkonfiguration von ciscotacro und ciscotacrw. Diese Benutzer sind standardmäßig aktiviert. Sie können diese Benutzer jedoch bei Bedarf deaktivieren.

- ciscotacro User: Dieser Benutzer gehört zur Benutzergruppe des Bedieners und hat nur Lesezugriff. Dieser Benutzer kann nur eine Konfiguration überwachen, jedoch keine Vorgänge ausführen, die die Konfiguration des Netzwerks ändern.
- ciscotacrw Benutzer: Dieser Benutzer ist Teil der netadmin Benutzergruppe mit Lese- und Schreibberechtigung. Dieser Benutzer kann eine Netzwerkkonfiguration ändern. Darüber hinaus kann nur dieser Benutzer mithilfe eines Zustimmungstokens auf die Root-Shell zugreifen.

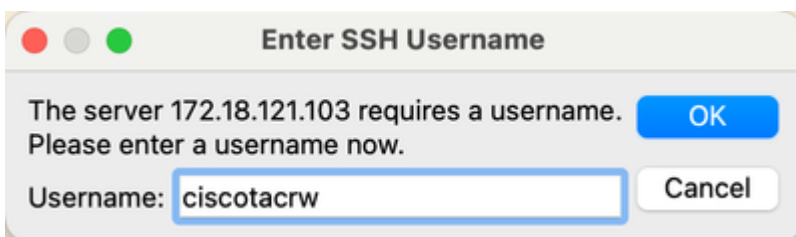


Anmerkung: Das Benutzerkonto "ciscotac" wurde eingeführt und ist standardmäßig enthalten, beginnend mit den Cisco SD-WAN-Softwareversionen um Version 20.x.

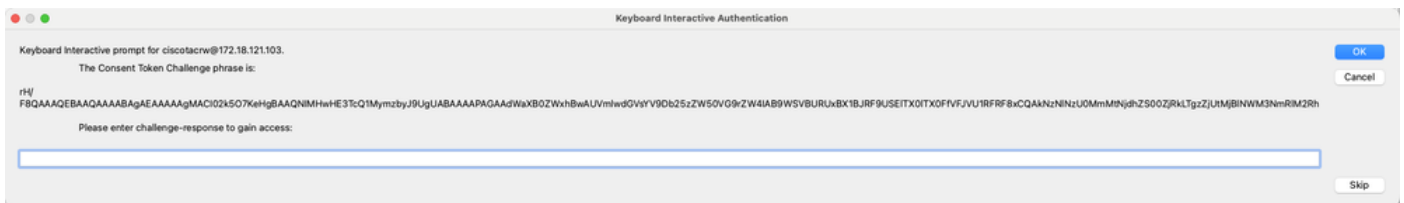
Lösung

Schritt 1: Zugriff auf vBond oder vSmart über SSH-Anmeldung mit Cisco Tacrw

- Geben Sie ciscotacrw als Benutzernamen ein.



- Klicken Sie auf OK, um den Consent Token Challenge-Satz entsprechend zu generieren.



- Sie müssen dem TAC den "Consent Token Challenge-Satz" über einen Serviceticket zur Verfügung stellen. TAC gibt dann den entsprechenden "sdwanchallenge-response-Token" zurück.
- Eingabe "sdwanchallenge-response token"

Schritt 2: Setzen Sie das vorhandene Benutzerkennwort zurück.

Nach der Anmeldung bei vBond/vSmart über das Cisco-Konto (mithilfe des Zustimmungstokens für die Authentifizierung) können Sie den Benutzernamen und das Kennwort wiederherstellen oder zurücksetzen.

- Wechseln Sie in den Konfigurationsmodus, und setzen Sie das Kennwort für den vorhandenen Benutzer (z. B. admin) zurück:

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



Anmerkung: Nach der Übermittlung verschlüsselt das System automatisch das unverschlüsselte Kennwort.

Schritt 3:Neuen NetAdmin-Benutzer hinzufügen (optional)

Wenn ein neues Administratorkonto erstellt werden muss:

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

Schritt 4: Entsperren Sie das gesperrte Konto (falls zutreffend).

Wenn Ihr Konto aufgrund mehrerer fehlgeschlagener Anmeldungen gesperrt ist, können Sie es mithilfe des folgenden Befehls entsperren:

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

Schritt 5: Überprüfen der Konfiguration

- Verwenden Sie den Befehl `show running-config system aaa`, um zu überprüfen, ob die Benutzerkonfiguration korrekt angewendet wurde.
- Versuchen Sie, sich mit den neuen Anmeldeinformationen anzumelden, um die erfolgreiche Wiederherstellung zu bestätigen.



Anmerkung: Da sich vBond im Offline-Status befindet (nicht mit vManage verknüpft oder nicht verbunden), wird empfohlen, die Konfiguration direkt über die CLI abzuschließen, anstatt die Vorlage aus vManage zu erstellen.



Warnung: Wenn Sie nach Abschluss des Vorgangs eine Managementverbindung mit vManage wiederherstellen müssen, stellen Sie sicher, dass die Anmeldeinformationen mit der Konfiguration in vManage übereinstimmen.

Zugehörige Informationen

- [Wiederherstellung von SD-WAN vSmart- und vBond-Zugriff bei Herstellung der Steuerverbindungen](#)
- [CiscoTac-Benutzerzugriff](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.