

Restablecer el nombre de usuario y la contraseña de Offline VBond/VSmart

Contenido

[Introducción](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Problema](#)

[Concepto básico](#)

[Acceso de usuario de CiscoContact](#)

[Solución](#)

[Paso 1.Utilice ciscotacrw para acceder a vBondorvSmart mediante inicio de sesión SSH](#)

[Paso 2.Restablecer la contraseña de usuario existente](#)

[Paso 3.Agregar un nuevo usuario Netadmin \(opcional\)](#)

[Paso 4.Desbloquear la cuenta bloqueada \(si corresponde\)](#)

[Paso 5.Verificar la configuración](#)

[Información Relacionada](#)

Introducción

Este documento describe cómo restablecer el nombre de usuario y la contraseña del vBond/vSmart sin conexión SD-WAN.

Prerequisites

Requirements

Cisco recomienda que tenga conocimiento sobre estos temas:

- Red de área extensa (SD-WAN) definida por software de Cisco.

Componentes Utilizados

La información de este documento se basa en Cisco vManager versión 20.9.4

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Problema

Se ha perdido el acceso a vBonds y vsmarts. Esto sucede cuando no conoce o no recuerda sus credenciales o cuando el acceso se bloquea después de intentos excesivos e infructuosos de iniciar sesión en cualquiera de las interfaces. Al mismo tiempo, se interrumpen las conexiones de control entre vManage, vsmarts y vBonds. Vbond y vsmart sin conexión no se pueden utilizar a través de la GUI de vmanage.

Concepto básico

Acceso de usuario de CiscoContact

El software Cisco Edge proporciona dos usuarios (ciscotacro y ciscotacrw) que son para uso exclusivo del equipo de soporte de Cisco. Estos usuarios están disponibles tanto para instalaciones en la nube como in situ. Funcionan en un desafío de token de consentimiento y autenticación de respuesta de token en el que se requiere un nuevo token para cada nueva sesión de inicio de sesión. Los usuarios de ciscotacro y ciscotacrw pueden utilizar este token para iniciar sesión en el servidor web Cisco SD-WAN Manager, así como en el terminal SSH en Cisco SD-WAN Manager. Estos usuarios también pueden acceder a los dispositivos Cisco SD-WAN Validator, Cisco SD-WAN Controllers y Cisco vEdge mediante el terminal SSH en Cisco SD-WAN Manager.

Las plantillas CLI predeterminadas incluyen la configuración de usuario de ciscotacro y ciscotacrw. Estos usuarios están habilitados de forma predeterminada. Sin embargo, como puede deshabilitar estos usuarios, si es necesario.

- usuario ciscotacro: este usuario forma parte del grupo de usuarios de operadores con privilegios de solo lectura solamente. Este usuario sólo puede supervisar una configuración, pero no puede realizar ninguna operación que modifique la configuración de la red.
- Usuario ciscotacrw: Este usuario forma parte del grupo de usuarios netadmin con privilegios de lectura y escritura. Este usuario puede modificar una configuración de red. Además, solo este usuario puede acceder al shell raíz mediante un token de consentimiento.

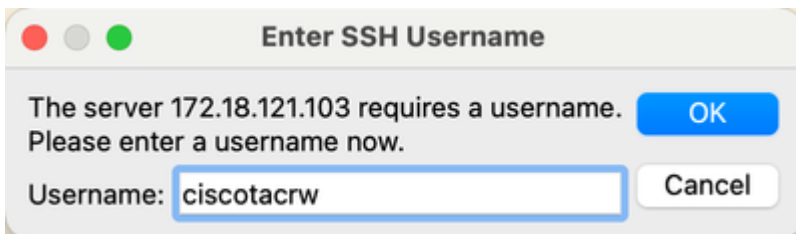


Nota: La cuenta de usuario "ciscotac" se introdujo y se incluye de forma predeterminada a partir de las versiones del software Cisco SD-WAN en torno a la versión 20.x.

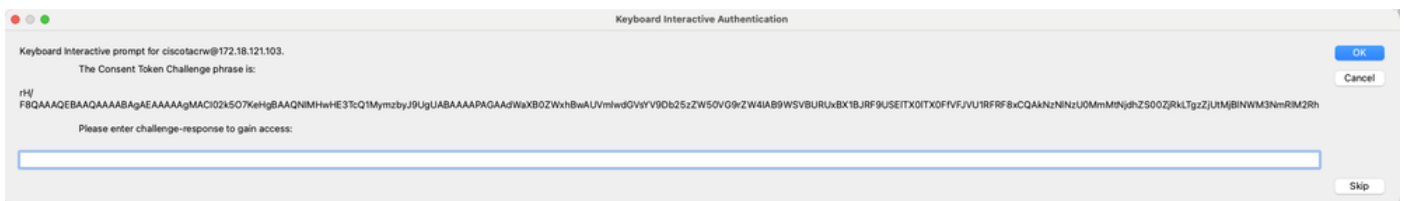
Solución

Paso 1. Utilice ciscotacrw para acceder a vBond o vSmart mediante inicio de sesión SSH

- Introduzca ciscotacrw como nombre de usuario.



- Haga clic en OK, la frase Consent Token Challenge se genera según corresponda.



- Debe proporcionar la "frase de desafío de token de consentimiento" al TAC a través del caso SR. TAC devuelve el "token sdwanchallenge-response" correspondiente.
- Introduzca "sdwanchallenge-response token"

Paso 2. Restablecer la contraseña de usuario existente

Después de iniciar sesión en vBond/vSmart sin conexión a través de la cuenta ciscotacrw (mediante el token de consentimiento para la autenticación), puede restaurar o restablecer el nombre de usuario y la contraseña.

- Introduzca el modo de configuración y restablezca la contraseña para el usuario existente (como admin):

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



Nota: Después del envío, el sistema cifra automáticamente la contraseña de texto sin formato.

Paso 3. Agregar un nuevo usuario Netadmin (opcional)

Si es necesario crear una nueva cuenta de administrador:

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

Paso 4. Desbloquear la cuenta bloqueada (si corresponde)

Si su cuenta está bloqueada debido a varios inicios de sesión fallidos, puede desbloquearla mediante el comando:

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

Paso 5. Verificar la configuración

- Utilice el comando `show running-config system aaa` para verificar si la configuración del usuario se aplica correctamente.
- Intente iniciar sesión con las nuevas credenciales para confirmar la recuperación correcta.



Nota: Como vBond está en estado sin conexión (no está asociado a vManage ni desconectado), se recomienda completar la configuración directamente mediante CLI en lugar de emitir la plantilla desde vManage.



Advertencia: Una vez finalizado, si necesita restablecer una conexión de gestión con

vManage, asegúrese de que las credenciales son coherentes con la configuración de vManage.

Información Relacionada

- [Recupere el acceso vSmart y vBond de SD-WAN cuando se establezcan las conexiones de control](#)
- [Acceso de usuario de CiscoContact](#)

Acerca de esta traducción

Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).