

# Guardia de Cisco y recuperación de contraseña del detector de la anomalía del tráfico

## Contenido

[Introducción](#)

[prerrequisitos](#)

[Requisitos](#)

[Convenciones](#)

[Procedimiento Paso a Paso](#)

[Información Relacionada](#)

## Introducción

Este documento describe el procedimiento para recuperar la contraseña del **usuario raíz** en un guardia de Cisco o un rechazo distribuido de Cisco traffic anomaly detector de la aplicación mitigante del servicio (DDoS). Esta contraseña se utiliza para controlar el **acceso a raíz a un guardia** o a un sistema detector de anomalía de tráfico de Cisco de Cisco. **La contraseña de raíz** se cifra y se puede substituir solamente por una nueva contraseña usando el procedimiento abajo.

## prerrequisitos

### Requisitos

No hay requisitos específicos para este documento.

### Convenciones

Para obtener más información sobre las convenciones del documento, consulte [Convenciones de Consejos Técnicos de Cisco](#).

## Procedimiento Paso a Paso

Complete estos pasos.

1. Asocie un teclado y un monitor al guardia de Cisco o al detector de anomalía en el tráfico de Cisco (este procedimiento no se puede realizar a través de un serial o de una conexión de red.)
2. Inicie sesión y teclee la **reinicialización**.
3. Mientras que el cuadro está accionando para arriba, mantenga la tecla Mayús pulsada. Esto le conseguirá un "inicio de Lilo: " prompt.

4. Presione la **LENGUETA** para ver las imágenes disponibles. **Note:** 3.0.8 tiene una imagen de “**Cisco**”, mientras que más viejas imágenes tienen “**Riverhead**”.
5. Teclee el **Cisco 1** para conseguir una imagen del único usuario cargada (o **Riverhead 1** en más viejos sistemas). Esto iniciará el sistema en el modo de usuario único.
6. Durante el proceso de arranque le pedirán una contraseña. Ingrese el **dud&ndud** de la contraseña corregida. Esto le dará un **shell raíz**.
7. Ahora usted puede funcionar con el **comando passwd** de cambiar la contraseña de la **raíz**. Le pedirán confirmar la contraseña que usted ha elegido, por ejemplo:

```
[root@DETECTOR root]# passwd
Changing password for user root.
New password: <new password typed in here>
Retype new password: <new password typed in here>
passwd: all authentication tokens updated successfully.
```

8. Después de que usted haya cambiado la contraseña, ejecute el **comando reboot** de recomenzar el sistema. No interrumpa el proceso de arranque de modo que el sistema ingrese a su modo de operación normal.

## [Información Relacionada](#)

- [Cisco Guard DDoS Mitigation Appliances](#)
- [Cisco Traffic Anomaly Detectors](#)
- [Soporte Técnico - Cisco Systems](#)