

Configuración de la interfaz de línea de comandos (CLI) de sólo lectura para CUCM

Contenido

[Introducción:](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Antecedentes](#)

[Cómo funciona en 11.5](#)

[Configurar](#)

[Examples:](#)

[Comando con Privilegio 0](#)

Introducción:

Este documento describe la nueva función CLI de sólo lectura introducida en la versión 11.5 de Cisco Unified Communications Manager (CUCM).

Colaborado por Manjunath Junnur, ingeniero del TAC de Cisco, Editado por Levi Thomas.

Prerequisites

Requirements

No hay requisitos específicos para este documento.

Componentes Utilizados

La información que contiene este documento se basa en estas versiones de software:

- Cisco Unified Communications Manager versión 11.5

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si tiene una red en vivo, asegúrese de entender el posible impacto de cualquier comando.

Antecedentes

A menudo, el entorno Customers requiere la capacidad de los usuarios con acceso limitado a los comandos CLI.

En esta versión, se incluyó la función de permiso de sólo lectura para CLI.

Los administradores de CUCM e IM&P pueden proporcionar a los usuarios cuentas, acceso de privilegios de lectura en la interfaz de línea de comandos (CLI), por lo que la información de configuración existente es visible pero no se puede cambiar.

Nota: Los comandos para las operaciones de escritura se niegan para los usuarios de cuentas de privilegios de sólo lectura.

Cómo funciona en 11.5

- Actualmente, en la arquitectura CLI actual, el comando **set account name** crea dos tipos de usuarios.

1. **Privilegio de nivel 0** (usuario de sólo lectura/normal)

2. **Privilegio de nivel 1** (usuario privilegiado)

Usuario de sólo lectura: Usuarios de sólo lectura, que sólo pueden acceder a comandos de sólo lectura como (show, status); no pueden acceder a set, delete commands o enable/disable settings. Si algún comando se convierte en comando de sólo lectura, en el archivo xml de configuración CLI "priv", el valor es 0 y los usuarios de sólo lectura pueden acceder a él.

Usuario privilegiado: Según el diseño, los usuarios privilegiados también pueden acceder a los comandos de sólo lectura y a los comandos de escritura. Si algún comando, en el archivo de configuración cli tiene el valor "priv" 1, estos comandos sólo pueden ser accesibles para usuarios privilegiados. Los usuarios privilegiados pueden acceder al comando con los valores priv 0 y 1

Usuario administrador: El usuario administrador tiene acceso para todos los comandos. El nivel de usuario administrador es 4. En el archivo de configuración cli Si el valor "priv" es 4 admin, el usuario accederá a esos comandos. El usuario administrador también puede acceder a los comandos priv value 4,1,0 level

Configurar

Para crear la cuenta de usuario de sólo lectura, inicie sesión en CLI y utilice el comando.

```
admin:set account name <input any name>
```

Los niveles de privilegio son:

Ordinario - Nivel 0

Avanzado - Nivel 1

Seleccione 0 para el usuario de acceso de sólo lectura.

Configurar la contraseña para el usuario

Introduzca la contraseña:*****

volver a introducir para confirmar :*****

Captura de pantalla de lo mismo:

```
admin:set account name ciscotac
```

```
Privilege Levels are:
```

```
Ordinary - Level 0
```

```
Advanced - Level 1
```

```
Please enter the privilege level :0 ←
Please enter the password :*****
re-enter to confirm :*****
Account successfully created
```

Examples:

Ejemplo 1: Inicie sesión con credenciales de usuario de sólo lectura e intente detener la replicación de la base de datos

```
admin:utils dbreplication stop all
Executed command unsuccessfully ←
No valid command entered
admin: █
```

Ejemplo 2: Consulta SQL Usi para eliminar una región .

```
[admin:run sql delete from region where region ="91b78ae6-6e6b-f9fd-cd1d-380a1b188034"
No DELETE permission for region. ←
```

Ejemplo 3: Usuarios de sólo lectura, pueden utilizar cualquier comando Show.

```
[admin:show version active ←
Active Master Version: 11.5.0.99838-4
Active Version Installed Software Options:
No Installed Software Options Found.
```

Ejemplo 4: Inicie sesión en el administrador del sistema operativo (SO) de la interfaz gráfica de usuario (GUI) con el usuario de sólo lectura y observe que no hay acceso de escritura en ninguna ficha. Si abre cualquier certificado, contiene los detalles, pero no hay opciones para eliminar o regenerar.

Certificate Details for publisher, CallManager

Status



Status: Ready

Certificate Settings

File Name	CallManager.pem
Certificate Purpose	CallManager
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
Version: V3
Serial Number: 45BA6326E241B27DCA57D66E80F61F33
SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
Issuer Name: L=Bangalore, ST=Karnataka, CN=publisher, OU=Cisco, O=Cisco,
C=IN
Validity From: Fri May 27 13:00:14 IST 2016
To: Wed May 26 13:00:13 IST 2021
Subject Name: L=Bangalore, ST=Karnataka, CN=publisher, OU=Cisco,
O=Cisco, C=IN
Key: RSA (1.2.840.113549.1.1.1)
Key value:
3082010a0282010100d634eb2a09e5ac0e91015ece7696040fa5f20baae7c4010cf0
863303e46b8d6fd73a8b5481d4cefd89ade3f5ede53dae3c89aaa7df080263d4de52a
f2dfcfec961946239d00bb7f4d13f76a777b93e57cdf5486ea2ad205b55fb0be6604a2
```

Comando con Privilegio 0

Ejemplo de comandos con privilegio 0

- show status
- show process using-most cpu
- utils dbreplicación runtimestate
- show network eth0
- lista de servicios de utils