Configurare IOS-XE per visualizzare la configurazione completa show running-config per gli utenti con bassi livelli di privilegio

Sommario

Introduzione

In questo documento viene descritto come visualizzare la configurazione in esecuzione completa per gli utenti che hanno effettuato l'accesso al router con livelli di privilegi bassi. Per comprendere il problema e le soluzioni indicate di seguito, è necessario conoscere i livelli di privilegio. I livelli di privilegio disponibili sono compresi tra 0 e 15 e consentono all'amministratore di personalizzare i comandi disponibili in base al livello di privilegio. Per impostazione predefinita, i tre livelli di privilegi su un router sono:

- **Livello 0** - Include solo i comandi di base (disable, enable, exit, help e logout)
- **Livello 1**: include tutti i comandi disponibili in modalità di esecuzione utente.
- **Livello 15**: include tutti i comandi disponibili in modalità di esecuzione privilegiata

I livelli restanti compresi tra questi livelli minimo e massimo non sono definiti finché l'amministratore non assegna loro comandi e/o utenti. Pertanto, l'amministratore può assegnare agli utenti livelli di privilegi diversi tra i livelli di privilegi minimo e massimo per separare i diversi utenti a cui hanno accesso. L'amministratore può quindi allocare singoli comandi (e varie altre opzioni) a un singolo livello di privilegio per renderli disponibili per qualsiasi utente a questo livello. Ad esempio:

```
Router(config)# nomeutente user1 privilegio 7 password P@ssw0rD1
Router(config)# privilegio exec level 7 show access-lists
```

Con questa configurazione, quando l'utente ‘user1’ è collegato al router, può eseguire il comando ‘show access-lists’ e/o qualsiasi altro comando abilitato a quel livello di privilegio. Tuttavia, lo stesso non può essere detto per abilitato il comando "show running-config", come verrà discusso di seguito con la nostra descrizione del problema.

Prerequisiti

Requisiti

Per comprendere questo documento, è necessaria una conoscenza di base dei livelli di privilegio di cisco. L'introduzione riportata sopra deve essere sufficiente a spiegare i livelli di privilegio richiesti.

Componenti usati

I componenti usati per gli esempi di configurazione in questo documento sono ASR1006.

Problema di configurazione

Quando si configurano diversi livelli di accesso al router per utenti diversi, è un'applicazione comune per un amministratore di rete tentare di assegnare a determinati utenti l'accesso solo ai comandi "show" e non fornire accesso ad alcun comando "configuration". Si tratta di un'operazione semplice per la maggior parte dei comandi show, in quanto è possibile concedere l'accesso tramite la configurazione semplice descritta di seguito.

```
Router(config)# nomeutente test_user privilege 10 password
testP@ssw0rD
Router(config)# privilegio exec livello 10 show
Router(config)# privilegio exec livello 10 show running-config
```

Con questa configurazione di esempio, la seconda riga consentirà a "test_user" di accedere a una pletora di comandi correlati a show, che normalmente non sono disponibili a questo livello di privilegio. Tuttavia, il comando show running-config viene trattato in modo diverso dalla maggior parte dei comandi show. Anche con la terza riga di codice di esempio, verrà visualizzato solo un comando "show running-config" omesso o abbreviato, nonostante il comando sia stato specificato al livello di privilegio corretto.

```
Verifica accesso utente

Username: utente_test
 Password:
N. router
 privilegio Router#show
 Il livello di privilegio corrente è 10
 N. router
 Router#show running-config
Compilazione della configurazione in corso...

Configurazione corrente: 121 byte
 !
 ! Ultima modifica alla configurazione alle 21:10:08 UTC lun 28 ago
2017
 !
 boot-start-marker
 boot-end-marker
 !
 !
 !
 fine
```

```
N. router
```

Come si può vedere, questo output non mostra alcuna configurazione e non sarebbe utile per un utente che cerca di raccogliere informazioni sulla configurazione del router. Infatti, il comando show running-config visualizza solo tutti i comandi che l'utente è in grado di modificare al livello di privilegio corrente. Questa configurazione è progettata come configurazione di protezione per impedire all'utente di accedere a comandi configurati al di sopra del livello di privilegio corrente. Questo è un problema quando si cerca di creare un utente con accesso ai comandi show, in quanto "show running-config" è un comando standard che i tecnici possono raccogliere inizialmente durante la risoluzione dei problemi.

Soluzione di configurazione e verifica

Per risolvere questo problema, è disponibile un'altra versione del tradizionale comando show run che consente di ignorare questa limitazione del comando.

```
Router(config)# show running-config view full
 Router(config)# privilegio exec livello 10 show running-config vista
full
```

L'aggiunta di "view full" al comando (e a sua volta il livello di privilegio del comando per consentire all'utente di accedere al comando), ora consente all'utente di visualizzare il comando show running-config completo senza alcun comando omesso.

```
Username: utente_test
 Password:
N. router
 privilegio Router#show
 Il livello di privilegio corrente è 10
 N. router
 Router#show running-config visualizzazione completa

Compilazione della configurazione in corso...

Configurazione corrente: 2664 byte
 !
 ! Ultima modifica alla configurazione alle 21:25:45 UTC lun 28 ago
2017
 !
 versione 15.4
 timestamp servizio debug datetime msec
 datetime msec log timestamp servizio
 no platform punt-keepalive disable-kernel-core
 !
 hostname Router
 !
 boot-start-marker
 boot system flash bootflash:pacchetti.conf
 sistema di avvio flash bootflash:asr1000rp1-
adventerprisek9.03.13.06a.S.154-3.S6a-ext.bin
 boot-end-marker
 !
```

```
 vrf definition Mgmt-intf
  !
  address-family ipv4
  exit-address-family
  !
 ipv6 famiglia di indirizzi
  exit-address-family
 !
 enable password <omesso>
 !
 no aaa new-model
 !
 nessuna ricerca nel dominio ip
 !
 modello sottoscrittore
 !
 nome-pacchetto multilink autenticato
 !
 spanning-tree extend system-id
 !
 username test_user privilege 10 password 0 testP@ssw0rD
!
 ridondanza
  modalità sso
 !
 esecuzione cdp
 !
 interfaccia Gigabit Ethernet0/2/0
  nessun indirizzo ip
  shutdown
  negoziazione automatica
 !
 interfaccia Gigabit Ethernet0/2/1
  nessun indirizzo ip
  shutdown
  negoziazione automatica
 !
 interfaccia Gigabit Ethernet0
  vrf forwarding Mgmt-intf
  indirizzo ip <omesso>
  negoziazione automatica
  cdp enable
 !
 ip forward-protocol nd
 !
 piano di controllo
 !
 !
 privilege exec level 10 show running-config view full
 alias exec show-running-config show running-config view full
 !
 riga con 0
  bit di stop 1
```

```
linea aux 0
 exec-timeout 0 1
 no exec
 output trasporto none
 bit di stop 1
vty linea 0 4
login locale
!
fine
N. router
```

Tuttavia, se si fornisce all'utente l'accesso a questa versione del comando, non si pone il problema della protezione iniziale che si stava tentando di risolvere progettando una versione omessa?

Per ovviare al problema e garantire la coerenza nella progettazione di una rete sicura, è possibile creare un alias per l'utente che eseguirà la versione completa del comando show running-config senza fornire accesso/conoscenza all'utente, come mostrato di seguito:

```
Router(config)# alias exec show-running-config show running-config
visualizzazione full
```

Nell'esempio, il nome alias è 'show-running-config' e quando l'utente è connesso al router, può immettere questo nome alias anziché il comando e ricevere l'output previsto senza conoscere il comando in esecuzione.

Conclusioni

In conclusione, questo è solo un esempio di come avere maggiore controllo quando si crea un accesso con privilegi utente a diversi livelli. Le opzioni per creare vari livelli di privilegi e accedere a diversi comandi sono numerose, e questo è un esempio di come assicurare che un utente "show-only" abbia ancora accesso alla configurazione di esecuzione completa quando non ha accesso ad alcun comando di configurazione.