Controllo degli accessi basato sui ruoli di Cisco IOS con SDM: Separazione delle autorizzazioni di configurazione tra gruppi operativi

Sommario

Introduzione

Le funzionalità di routing e sicurezza sono tradizionalmente supportate in dispositivi separati, il che offre una chiara divisione delle responsabilità di gestione tra l'infrastruttura di rete e i servizi di sicurezza. La convergenza delle funzionalità di sicurezza e routing nei router di servizi integrati Cisco non offre questa separazione chiara e multidispositivo. Alcune organizzazioni necessitano di una separazione delle funzionalità di configurazione per limitare i clienti o i gruppi di gestione dei servizi lungo i confini funzionali. CLI Views, una funzionalità software di Cisco IOS®, cerca di soddisfare questa esigenza con l'accesso CLI basato sui ruoli. Questo documento descrive la configurazione definita dal supporto SDM del controllo degli accessi basato sui ruoli di Cisco IOS e offre informazioni di base sulle funzionalità delle viste CLI dall'interfaccia della riga di comando di Cisco IOS.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Premesse

Molte organizzazioni delegano la responsabilità della manutenzione del routing e della connettività dell'infrastruttura a un gruppo di operazioni di rete e la responsabilità della manutenzione del firewall, della VPN e della funzionalità di prevenzione delle intrusioni a un gruppo di operazioni di sicurezza. Le viste CLI possono limitare la funzionalità di configurazione e monitoraggio della sicurezza al gruppo secops e, viceversa, limitare la connettività di rete, il routing e altre attività infrastrutturali al gruppo netops.

Alcuni provider di servizi desiderano offrire ai clienti funzionalità di configurazione o monitoraggio limitate, ma non consentono di configurare o visualizzare altre impostazioni dei dispositivi. Ancora una volta, le viste CLI offrono un controllo granulare sulla capacità CLI per limitare gli utenti o i gruppi di utenti a eseguire solo i comandi autorizzati.

Il software Cisco IOS ha offerto una funzionalità per limitare i comandi CLI con un server TACACS+ in modo da autorizzare o negare la funzionalità di esecuzione dei comandi CLI in base al nome utente o all'appartenenza al gruppo di utenti. Le viste CLI offrono funzionalità simili, ma il controllo dei criteri viene applicato dal dispositivo locale dopo che la vista specificata dell'utente è stata ricevuta dal server AAA. Quando si usa l'autorizzazione dei comandi AAA, ogni comando deve essere autorizzato singolarmente dal server AAA, il che produce frequenti dialoghi tra il dispositivo e il server AAA. Le viste CLI consentono il controllo dei criteri CLI per dispositivo, mentre l'autorizzazione dei comandi AAA applica lo stesso criterio di autorizzazione dei comandi a tutti i dispositivi a cui l'utente accede.

Configurazione

In questa sezione vengono presentate le informazioni necessarie per configurare le funzionalità descritte più avanti nel documento.

Nota: per ulteriori informazioni sui comandi menzionati in questa sezione, usare lo strumento di ricerca dei comandi (solo utenti registrati).

Associa utenti a una visualizzazione

Gli utenti possono essere associati a una vista CLI locale tramite un attributo restituito da AAA o nella configurazione di autenticazione locale. Per la configurazione locale, il nome utente è configurato con un'opzione di **visualizzazione** aggiuntiva, che corrisponde al nome della **visualizzazione del parser** configurato. Di seguito vengono riportati gli utenti configurati per le visualizzazioni SDM predefinite:

```
username fw-user privilege [privilege-level] view SDM_Firewall
username monitor-user privilege [privilege-level] view SDM_Monitor
username vpn-user privilege [privilege-level] view SDM_EasyVPN_Remote
username sdm-root privilege [privilege-level] view root
```

Gli utenti assegnati a una determinata visualizzazione possono passare temporaneamente a un'altra visualizzazione se dispongono della password per la visualizzazione che desiderano immettere. Per modificare la visualizzazione, usare questo comando exec:

```
enable view view-name
```

Configurazione visualizzazione parser

Le viste CLI possono essere configurate dalla CLI del router o tramite SDM. SDM fornisce il supporto statico per quattro visualizzazioni, come indicato nella sezione Supporto delle visualizzazioni CLI di SDM. Per configurare la vista CLI dall'interfaccia della riga di comando, un utente deve essere definito come utente della vista **radice** o deve appartenere alla vista con accesso alla configurazione della **vista parser**. Gli utenti che non sono associati a una visualizzazione e che tentano di configurare le visualizzazioni ricevono questo messaggio:

```
router(config#parser view test-view
No view Active! Switch to View Context
```

Le viste CLI consentono di includere o escludere gerarchie di comandi complete sia per la modalità esecutiva che per la modalità di configurazione, o solo per parti di esse. Sono disponibili tre opzioni per consentire o impedire la visualizzazione di un comando o di una gerarchia di comandi in una determinata vista:

```
router(config-view)#commands configure ?
  exclude            Exclude the command from the view
  include            Add command to the view
  include-exclusive  Include in this view but exclude from others
```

Le viste CLI troncano la configurazione in esecuzione in modo che la configurazione della vista parser non venga visualizzata. Tuttavia, la configurazione della vista parser è visibile nella configurazione di avvio.

Per ulteriori informazioni sulla definizione della vista, fare riferimento a Accesso CLI basato sui ruoli.

Verifica dell'associazione della visualizzazione parser

Gli utenti assegnati a una visualizzazione parser possono determinare a quale visualizzazione sono assegnati quando hanno effettuato il login a un router. Se il comando **show parser view** è consentito per le visualizzazioni degli utenti, questi possono utilizzare il comando **show parser view** per determinare la propria visualizzazione:

```
router#sh parser view
Current view is 'SDM_Firewall'
```

Supporto visualizzazioni CLI SDM

Il modello SDM offre tre visualizzazioni predefinite, due per la configurazione e il monitoraggio dei componenti firewall e VPN e una per il monitoraggio limitato. Anche in SDM è disponibile una vista **radice** predefinita aggiuntiva.

SDM non consente di modificare i comandi inclusi o esclusi da ciascuna vista di default, né di definire viste aggiuntive. Se dalla CLI sono definite viste aggiuntive, SDM non le offre nel pannello di configurazione **Account utente/Viste**.

Per il modello SDM, queste viste e le rispettive autorizzazioni di comando sono predefinite:

Vista SDM_Firewall

```
parser view SDM_Firewall
 secret 5 $1$w/cD$T1ryjKM8aGCnIaKSm.Cx9/
 commands interface include all ip inspect
 commands interface include all ip verify
 commands interface include all ip access-group
 commands interface include ip
 commands interface include description
 commands interface include all no ip inspect
 commands interface include all no ip verify
 commands interface include all no ip access-group
 commands interface include no ip
 commands interface include no description
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include all ip access-list
 commands configure include all interface
 commands configure include all zone-pair
 commands configure include all zone
 commands configure include all policy-map
 commands configure include all class-map
 commands configure include all parameter-map
 commands configure include all appfw
 commands configure include all ip urlfilter
 commands configure include all ip inspect
 commands configure include all ip port-map
 commands configure include ip cef
 commands configure include ip
 commands configure include all crypto
 commands configure include no end
 commands configure include all no access-list
 commands configure include all no ip access-list
 commands configure include all no interface
 commands configure include all no zone-pair
 commands configure include all no zone
```

```
 commands configure include all no policy-map
 commands configure include all no class-map
 commands configure include all no parameter-map
 commands configure include all no appfw
 commands configure include all no ip urlfilter
 commands configure include all no ip inspect
 commands configure include all no ip port-map
 commands configure include no ip cef
 commands configure include no ip
 commands configure include all no crypto
 commands configure include no
 commands exec include all vlan
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

SDM_EasyVPN_Remote View

```
parser view SDM_EasyVPN_Remote
 secret 5 $1$UnC3$ienYd0L7Q/9xfCNkBQ4Uu.
 commands interface include all crypto
 commands interface include all no crypto
 commands interface include no
 commands configure include end
 commands configure include all access-list
 commands configure include ip radius source-interface
 commands configure include ip radius
 commands configure include all ip nat
 commands configure include ip dns server
 commands configure include ip dns
 commands configure include all interface
 commands configure include all dot1x
 commands configure include all identity policy
 commands configure include identity profile
 commands configure include identity
 commands configure include all ip domain lookup
 commands configure include ip domain
 commands configure include ip
 commands configure include all crypto
 commands configure include all aaa
 commands configure include default end
 commands configure include all default access-list
 commands configure include default ip radius source-interface
 commands configure include default ip radius
 commands configure include all default ip nat
 commands configure include default ip dns server
```

```
 commands configure include default ip dns
 commands configure include all default interface
 commands configure include all default dot1x
 commands configure include all default identity policy
 commands configure include default identity profile
 commands configure include default identity
 commands configure include all default ip domain lookup
 commands configure include default ip domain
 commands configure include default ip
 commands configure include all default crypto
 commands configure include all default aaa
 commands configure include default
 commands configure include no end
 commands configure include all no access-list
 commands configure include no ip radius source-interface
 commands configure include no ip radius
 commands configure include all no ip nat
 commands configure include no ip dns server
 commands configure include no ip dns
 commands configure include all no interface
 commands configure include all no dot1x
 commands configure include all no identity policy
 commands configure include no identity profile
 commands configure include no identity
 commands configure include all no ip domain lookup
 commands configure include no ip domain
 commands configure include no ip
 commands configure include all no crypto
 commands configure include all no aaa
 commands configure include no
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include crypto ipsec client ezvpn connect
 commands exec include crypto ipsec client ezvpn xauth
 commands exec include crypto ipsec client ezvpn
 commands exec include crypto ipsec client
 commands exec include crypto ipsec
 commands exec include crypto
 commands exec include write memory
 commands exec include write
 commands exec include all ping ip
 commands exec include ping
 commands exec include configure terminal
 commands exec include configure
 commands exec include all show
 commands exec include no
 commands exec include all debug appfw
 commands exec include all debug ip inspect
 commands exec include debug ip
 commands exec include debug
 commands exec include all clear
```

Visualizzazione SDM_Monitor

```
parser view SDM_Monitor
 secret 5 $1$RDYW$OABbxSgtx1kOozLlkBeJ9/
 commands configure include end
 commands configure include all interface
 commands configure include no end
 commands configure include all no interface
 commands exec include dir all-filesystems
 commands exec include dir
 commands exec include all crypto ipsec client ezvpn
```

```
commands exec include crypto ipsec client
commands exec include crypto ipsec
commands exec include crypto
commands exec include all ping ip
commands exec include ping
commands exec include configure terminal
commands exec include configure
commands exec include all show
commands exec include all debug appfw
commands exec include all debug ip inspect
commands exec include debug ip
commands exec include debug
commands exec include all clear
```

Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

Informazioni correlate

- Accesso CLI basato sui ruoli
- Documentazione e supporto tecnico – Cisco Systems