Configurazione di TACACS+, RADIUS e Kerberos sugli switch Catalyst

Sommario

Introduzione

La famiglia di switch Cisco Catalyst (Catalyst 4000, Catalyst 5000 e Catalyst 6000 con CatOS) supporta alcune forme di autenticazione, che iniziano con il codice 2.2. Miglioramenti sono stati aggiunti con le versioni più recenti. La configurazione della porta TACACS+ TCP 49, non la porta UDP (User Datagram Protocol) XTACACS (49), RADIUS o server Kerberos per l'autenticazione, l'autorizzazione e l'accounting (AAA) è la stessa di quella dei router. Questo documento contiene esempi dei comandi minimi necessari per abilitare queste funzioni. Ulteriori opzioni sono disponibili nella documentazione dello switch per la versione in questione.

Prerequisiti

Requisiti

Nessun requisito specifico previsto per questo documento.

Componenti usati

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

Convenzioni

Per ulteriori informazioni sulle convenzioni usate, consultare il documento Cisco sulle convenzioni nei suggerimenti tecnici.

Premesse

Poiché le versioni più recenti del codice supportano opzioni aggiuntive, è necessario utilizzare il comando **show version** per determinare la versione del codice sullo switch. Dopo aver determinato la versione del codice utilizzata sullo switch, utilizzare questa tabella per determinare le opzioni disponibili sull'apparecchiatura e quelle da configurare.

Quando si aggiungono autenticazione e autorizzazione, rimanere sempre nello switch. Verificare la configurazione in un'altra finestra per evitare che venga bloccata accidentalmente.

Metodo (minimo)	**Cat versione 2.2-5.1**	**Cat versione 5.1-5.4.1**	**Cat versione da 5.4.1 a 7.5.1**	**Cat versione 7.5.1 e successive**
Autenticazione TACACS+ O	Passaggio A	Passaggio A	Passaggio A	Passaggio A
Autenticazione RADIUS O	N/D	Fase B	Fase B	Fase B
Autenticazione Kerberos OR	N/D	N/D	Passaggio K	Passaggio K
Autenticazione/autorizzazione nome utente locale	N/D	N/D	N/D	Fase C
Più (opzioni)				
Autorizzazione comando TACACS+	N/D	N/D	Passaggio D	Passaggio D
Autorizzazione TACACS+ Exec	N/D	N/D	Fase E	Fase E
Autorizzazione di esecuzione RADIUS	N/D	N/D	Passaggio F	Passaggio F
Accounting - TACACS+ o RADIUS	N/D	N/D	Fase G	Fase G
TACACS+ Abilita autorizzazione	Fase H	Fase H	Fase H	Fase H
Abilitazione	N/D	Fase I	Fase I	Fase I

autorizzazione RADIUS				
TACACS+ Abilita autorizzazione	N/D	N/D	Fase J	Fase J

Procedura di configurazione

Fase A - Autenticazione TACACS+

Nelle versioni precedenti del codice, i comandi non sono così complessi come in alcune versioni successive. Sullo switch sono disponibili opzioni aggiuntive nelle versioni più recenti.

1. Per verificare che lo switch sia collegato a una porta posteriore se il server non è attivo, usare il comando **set authentication login local enable**.
2. Usare il comando **set authentication login tacacs enable** per abilitare l'autenticazione TACACS+.
3. Usare il comando **set tacacs server #.#.#.#** per definire il server.
4. Usare il comando **set tacacs key** *your_key* per definire la chiave del server, opzione facoltativa di TACACS+, che determina la crittografia dei dati da switch a server. Se utilizzato, deve essere in accordo con il server.**Nota: il** software Cisco Catalyst OS **non** accetta il punto interrogativo (**?**) come parte di alcuna chiave o password. Il punto interrogativo viene utilizzato in modo esplicito per informazioni sulla sintassi del comando.

Fase B - Autenticazione RADIUS

Nelle versioni precedenti del codice, i comandi non sono così complessi come in alcune versioni successive. Sullo switch sono disponibili opzioni aggiuntive nelle versioni più recenti.

1. Per verificare che lo switch sia collegato a una porta posteriore se il server non è attivo, usare il comando **set authentication login local enable**.
2. Per abilitare l'autenticazione RADIUS, usare il comando **set authentication login radius enable**.
3. Definire il server. Su tutte le altre apparecchiature Cisco, le porte RADIUS predefinite sono 1645/1646 (autenticazione/accounting).Su Catalyst, la porta predefinita è 1812/1813. Se si usa Cisco Secure o un server che comunica con altre apparecchiature Cisco, usare la porta 1645/1646. Utilizzare il comando **set radius server #.#.#.# auth-port 1645 acct-port 1646 primary** per definire il server e il comando equivalente in Cisco IOS come **porte di origine 1645-1646 radius-server**.
4. Definire la chiave del server.Questa operazione è obbligatoria, in quanto determina la crittografia della password da switch a server, come mostrato nella RFC 2865 relativa all'autenticazione/autorizzazione RADIUS e nella RFC 2866 relativa all'accounting RADIUS . Se utilizzato, deve essere in accordo con il server. Eseguire il comando **set radius key** *your_key*.

Fase C - Autenticazione/autorizzazione nome utente locale

A partire dalla versione 7.5.1 di CatOS, è possibile eseguire l'autenticazione dell'utente locale. Ad

esempio, è possibile ottenere l'autenticazione/autorizzazione con l'uso di un nome utente e di una password archiviati su Catalyst, anziché con una password locale.

Sono disponibili solo due livelli di privilegi per l'autenticazione utente locale, 0 o 15. Il livello 0 è il livello di esecuzione non privilegiato. Il livello 15 è il livello di abilitazione privilegiato.

Se si aggiungono questi comandi nell'esempio, l'utente `poweruser` arriva in modalità abilitazione su Telnet o console allo switch e l'utente `non abilitazione` arriva in modalità di esecuzione su Telnet o console allo switch.

```
set localuser user poweruser password powerpass privilege 15
set localuser user nonenable password nonenable
```

Nota: se l'utente `non abilitato` conosce la password **set enable**, può continuare ad abilitare la modalità.

Dopo la configurazione, le password vengono archiviate in formato crittografato.

Èpossibile usare l'autenticazione del nome utente locale insieme all'accounting remoto TACACS+ exec, all'accounting dei comandi o all'accounting remoto RADIUS exec. Può essere usato anche in combinazione con l'autorizzazione remota TACACS+ exec o del comando, ma non ha senso usarlo in questo modo perché il nome utente deve essere archiviato sia sul server TACACS+ che localmente sullo switch.

Fase D - Autorizzazione comando TACACS+

Nell'esempio, lo switch deve essere autorizzato solo per i comandi di configurazione con TACACS+. Se il server TACACS+ non è attivo, l'autenticazione è none (nessuno). Ciò si applica sia alla porta della console che alla sessione Telnet. Immettere questo comando

set authorization comandi enable config tacacs none both

Nell'esempio, è possibile configurare il server TACACS+ in modo da consentire l'uso dei seguenti parametri:

```
command=set
arguments (permit)=port 2/12
```

Il comando **set port enable 2/12** viene inviato al server TACACS+ per una verifica.

Nota: se l'autorizzazione del comando è abilitata, a differenza del router in cui l'abilitazione non è considerata un comando, lo switch invia il comando **enable** al server quando viene tentato un'abilitazione. Verificare che anche il server sia configurato in modo da consentire il comando **enable**.

Fase E - Autorizzazione TACACS+ Exec

Nell'esempio, lo switch viene autorizzato a richiedere l'autorizzazione per una sessione di esecuzione con TACACS+. Nel caso in cui il server TACACS+ non sia attivo, l'autorizzazione è none (nessuna autorizzazione). Ciò si applica sia alla porta della console che alla sessione Telnet.

Eseguire il comando **set authorization exec enable tacacs+ none both**

Oltre alla richiesta di autenticazione, questa invia una richiesta di autorizzazione separata al server TACACS+ dallo switch. Se il profilo utente è configurato per shell/exec sul server TACACS+, l'utente può accedere allo switch.

In questo modo si impedisce agli utenti senza il servizio shell/exec configurato sul server, ad esempio gli utenti PPP, di accedere allo switch. Viene visualizzato un messaggio che indica che l'`autorizzazione della modalità di esecuzione non è riuscita`. Oltre a consentire/negare la modalità di esecuzione per gli utenti, è possibile forzare l'attivazione della modalità quando si accede con il livello di privilegio 15 assegnato sul server. Deve eseguire il codice in cui è stato risolto l'ID bug Cisco CSCdr51314 (solo utenti registrati).

Fase F - Autorizzazione di esecuzione RADIUS

Nessun comando per abilitare l'autorizzazione di esecuzione RADIUS. In alternativa, è possibile impostare Service-Type (attributo RADIUS 6) su Administrative (valore 6) nel server RADIUS per avviare l'utente in modalità abilitazione nel server RADIUS. Se il tipo di servizio è impostato su un valore diverso da 6 (amministrativo), ad esempio 1-login, 7-shell o 2-framed, l'utente arriva al prompt di esecuzione dello switch, ma non al prompt di abilitazione.

Aggiungere questi comandi nello switch per l'autenticazione e l'autorizzazione:

```
aaa authorization exec TEST group radius
 line vty 0 4
 authorization exec TEST
 login authentication TEST
```

Fase G - Accounting - TACACS+ o RADIUS

Per abilitare la contabilizzazione TACACS+ per:

1. Se viene visualizzato il prompt dello switch, usare il comando **set accounting exec enable start-stop tacacs+**.
2. Gli utenti che usano Telnet all'esterno dello switch usano il comando **set accounting connect enable start-stop tacacs+**.
3. Se si riavvia lo switch, usare il comando **set accounting system enable start-stop tacacs+**.
4. Gli utenti che eseguono comandi, usano il comando **set accounting per abilitare tutti i comandi start-stop tacacs+**.
5. Promemoria al server, ad esempio, per aggiornare i record una volta al minuto in modo da mostrare che l'utente è ancora connesso, eseguire il comando **set accounting update periodic 1**.

Per abilitare l'accounting RADIUS per:

1. Gli utenti che ricevono il prompt dello switch, eseguono il comando **set accounting exec enable start-stop radius**.
2. Gli utenti che usano Telnet fuori dallo switch, usano il comando **set accounting connect enable start-stop radius**.
3. Quando si riavvia lo switch, usare il comando **set accounting system enable start-stop radius**.
4. Promemoria al server, ad esempio, per aggiornare i record una volta al minuto in modo da

mostrare che l'utente è ancora connesso, eseguire il comando **set accounting update periodic 1**.

Record liberi TACACS+

Questo output è un esempio di come i record possono apparire sul server:

```
Fri Mar 24 13:22:41 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=5 start_time=953936729 timezone=UTC
service=shell disc-cause=2 elapsed_time=236
Fri Mar 24 13:22:50 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=15 start_time=953936975 timezone=UTC
service=shell priv-lvl=0 cmd=enable
Fri Mar 24 13:22:54 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=16 start_time=953936979 timezone=UTC
service=shell priv-lvl=15 cmd=write terminal
Fri Mar 24 13:22:59 2000 10.31.1.151 pinecone telnet85
171.68.118.100 stop task_id=17 start_time=953936984 timezone=UTC
service=shell priv-lvl=15 cmd=show version
Fri Mar 24 13:23:19 2000 10.31.1.151 pinecone telnet85
171.68.118.100 update task_id=14 start_time=953936974 timezone=UTC
service=shell
```

RADIUS su output record UNIX

Questo output è un esempio di come i record possono apparire sul server:

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Start
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Start
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Delay-Time = 0

Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Calling-Station-Id = "171.68.118.100"
Acct-Status-Type = Stop
User-Service-Type = Login-User
Acct-Session-Id = "0000002c"
Login-Service = Telnet
Login-Host = 171.68.118.100
Acct-Session-Time = 9
Acct-Delay-Time = 0
```

```
Client-Id = 10.31.1.151
NAS-Port-Type = 0
User-Name = "login"
Acct-Status-Type = Stop
Acct-Authentic = RADIUS
User-Service-Type = 7
Acct-Session-Id = "0000002b"
Received unknown attribute 49
Acct-Session-Time = 30
Acct-Delay-Time = 0
```

Fase H - Abilitazione autenticazione TACACS+

Attenersi alla seguente procedura:

1. Per verificare che il server non sia attivo, usare il comando **set authentication enable local enable** per assicurarsi che sia presente una porta di servizio.
2. Usare il comando **set authentication enable tacacs enable** per chiedere allo switch di inviare le richieste di abilitazione al server.

Fase I - Abilitazione autenticazione RADIUS

Aggiungere questi comandi per consentire allo switch di inviare il nome utente `$enab15$` al server RADIUS. Non tutti i server RADIUS supportano questo tipo di nome utente. Vedere il passo E per un'altra alternativa, ad esempio se si imposta un tipo di servizio [RADIUS attribute 6 - to Administrative], che avvia i singoli utenti in modalità abilitazione.

1. Utilizzare il comando **set authentication enable local enable** per verificare che sia presente una porta posteriore in entrata se il server non è attivo.
2. Utilizzare il comando **set authentication enable radius enable** per comunicare allo switch di inviare richieste di abilitazione al server se il server RADIUS supporta il nome utente $enab15$.

Fase J - TACACS+ Abilitazione dell'autorizzazione

L'aggiunta di questo comando determina l'invio da parte dello switch dell'istruzione enable al server quando l'utente tenta di abilitarla. Il server deve avere il comando **enable** consentito. Nell'esempio riportato di seguito viene illustrato un failover su none nel caso in cui il server non sia attivo:

set author enable tacacs+ none both

Fase K - Autenticazione Kerberos

per ulteriori informazioni su come configurare Kerberos sullo switch, consultare il documento sul controllo e il monitoraggio dell'accesso allo switch tramite autenticazione, autorizzazione e accounting.

Recupero password

per ulteriori informazioni sulle procedure di recupero della password, consultare il documento

Procedure di recupero della password.

Questa pagina è l'indice delle procedure di recupero della password per i prodotti Cisco.

Comandi ip allowed per una maggiore sicurezza

Per una maggiore sicurezza, è possibile configurare Catalyst in modo da controllare l'accesso Telnet tramite i comandi **ip allow**:

set ip allow enable telnet

set ip allow *range mask*|*host*

Ciò consente solo all'intervallo o agli host specificati di connettersi allo switch in modalità Telnet.

Debug su Catalyst

Prima di abilitare il debug su Catalyst, controllare i registri del server per individuare le cause dell'errore. In questo modo lo switch è più facile e meno invasivo. Nelle versioni precedenti, il **debug** è stato eseguito in modalità progettazione. Non è necessario accedere alla modalità di progettazione per eseguire i comandi di **debug** nelle versioni più recenti del codice:

set trace tacacs|radius|kerberos 4

Nota: il comando **set trace tacacs|radius|kerberos 0** riporta Catalyst in modalità no-tracing.

Per ulteriori informazioni sugli switch LAN multilivello, consultare la pagina di supporto dei prodotti degli switch.

Informazioni correlate

- Confronto tra TACACS+ e RADIUS
- Radius, TACACS+ e Kerberos nella documentazione di Cisco IOS
- Pagina di supporto RADIUS
- Pagina di supporto TACACS/TACACS+
- Pagina di supporto Kerberos
- RFC (Requests for Comments)
- Documentazione e supporto tecnico – Cisco Systems