Konfigurieren von TACACS+, RADIUS und Kerberos auf Cisco Catalyst Switches

Inhalt

Einleitung
Voraussetzungen
Anforderungen
Verwendete Komponenten
Konventionen
Hintergrundinformationen
Konfigurationsschritte
Schritt A: TACACS+-Authentifizierung
Schritt B: RADIUS-Authentifizierung
Schritt C: Lokale Benutzername-Authentifizierung/Autorisierung
Schritt D - TACACS+-Befehlsautorisierung
Schritt E - TACACS+ Exec-Autorisierung
Schritt F - RADIUS Exec-Autorisierung
Schritt G - Abrechnung - TACACS+ oder RADIUS
Schritt H: TACACS+-Authentifizierung aktivieren
Schritt I: RADIUS-Authentifizierung aktivieren
Schritt J - TACACS+-Autorisierung aktivieren
Schritt K - Kerberos-Authentifizierung
Kennwortwiederherstellung
ip permit-Befehle für zusätzliche Sicherheit
Debuggen auf dem Catalyst
Zugehörige Informationen

Einleitung

Die Cisco Catalyst-Switches (Catalyst 4000, Catalyst 5000 und Catalyst 6000, die CatOS ausführen) unterstützen eine bestimmte Authentifizierung, die im Code 2.2 beginnt. Verbesserungen wurden mit späteren Versionen hinzugefügt. Der TACACS+ TCP-Port 49, nicht der XTACACS User Datagram Protocol (UDP)-Port 49, der RADIUS- oder der Kerberos-Server-Benutzereinrichtung für Authentifizierung, Autorisierung und Abrechnung (AAA) ist identisch mit dem Router-Benutzer. Dieses Dokument enthält Beispiele für die zur Aktivierung dieser Funktionen erforderlichen Mindestbefehle. Weitere Optionen sind in der Switch-Dokumentation für die betreffende Version enthalten.

Voraussetzungen

Anforderungen

Es gibt keine spezifischen Anforderungen für dieses Dokument.

Verwendete Komponenten

Dieses Dokument ist nicht auf bestimmte Software- und Hardware-Versionen beschränkt.

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

Hintergrundinformationen

Da neuere Versionen des Codes zusätzliche Optionen unterstützen, müssen Sie den Befehl **show version** ausführen, um die Codeversion auf dem Switch zu ermitteln. Nachdem Sie die Version des Codes ermittelt haben, der auf dem Switch verwendet wird, können Sie anhand dieser Tabelle ermitteln, welche Optionen auf Ihrem Gerät verfügbar sind und welche Optionen Sie konfigurieren möchten.

Bleiben Sie immer im Switch, wenn Sie Authentifizierung und Autorisierung hinzufügen. Testen Sie die Konfiguration in einem anderen Fenster, um eine versehentliche Sperrung zu vermeiden.

Methode (mindestens)	**Cat Version 2.2 bis 5.1**	**Cat Version 5.1 bis 5.4.1**	**Cat Version 5.4.1 bis 7.5.1**	**Cat Version 7.5.1 oder höher**
TACACS+-Authentifizierung ODER	Schritt A	Schritt A	Schritt A	Schritt A
RADIUS-Authentifizierung ODER	–	Schritt B	Schritt B	Schritt B
Kerberos-Authentifizierung ODER	–	–	Schritt K	Schritt K
Lokale Benutzername-Authentifizierung/Autorisierung	–	–	–	Schritt C
Plus (Optionen)				
TACACS+-Befehls-Ermächtigung	–	–	Schritt D	Schritt D
TACACS+ Exec-Autorisierung	–	–	Schritt E	Schritt E
RADIUS Exec-Autorisierung	–	–	Schr	Schritt F

			itt F	
Accounting - TACACS+ oder RADIUS	–	–	Schr itt G	Schritt G
TACACS+-Autorisierung aktivieren	Sch ritt H	Sch ritt H	Schr itt H	Schritt H
RADIUS Enable-Autorisierung	–	Sch ritt I	Schr itt I	Schritt I
TACACS+-Autorisierung aktivieren	–	–	Schr itt J	Schritt J

Konfigurationsschritte

Schritt A: TACACS+-Authentifizierung

Bei früheren Codeversionen sind Befehle nicht so komplex wie bei einigen späteren Versionen. Zusätzliche Optionen in späteren Versionen können auf Ihrem Switch verfügbar sein.

1. Geben Sie den Befehl **set authentication login local enable** ein, um sicherzustellen, dass bei einem Serverausfall eine Hintertür in den Switch eingesteckt ist.
2. Geben Sie den Befehl **set authentication login tacacs enable** ein, um die TACACS+-Authentifizierung zu aktivieren.
3. Geben Sie den Befehl **set tacacs server #.#.#.#** ein, um den Server zu definieren.
4. Geben Sie den **set tacacs key *your_key*** command ein, um den Serverschlüssel zu definieren. Dieser ist optional mit TACACS+, da er die Verschlüsselung von Switch-zu-Server-Daten bewirkt. Wenn sie verwendet wird, muss sie mit dem Server übereinstimmen.**Hinweis:** Die Cisco Catalyst OS-Software akzeptiert **kein** Fragezeichen (**?**) als Teil von Schlüsseln oder Kennwörtern. Das Fragezeichen wird explizit für Hilfe in der Befehlssyntax verwendet.

Schritt B: RADIUS-Authentifizierung

Bei früheren Codeversionen sind Befehle nicht so komplex wie bei einigen späteren Versionen. Zusätzliche Optionen in späteren Versionen können auf Ihrem Switch verfügbar sein.

1. Geben Sie den Befehl **set authentication login local enable** ein, um sicherzustellen, dass bei einem Serverausfall eine Hintertür in den Switch eingesteckt ist.
2. Geben Sie den Befehl **set authentication login radius enable ein**, um die RADIUS-Authentifizierung zu aktivieren.
3. Definieren Sie den Server. Auf allen anderen Cisco Geräten sind die RADIUS-Standardports 1645/1646 (Authentifizierung/Abrechnung).Auf dem Catalyst ist der Standard-Port 1812/1813. Wenn Sie Cisco Secure oder einen Server verwenden, der mit anderen Cisco Geräten kommuniziert, verwenden Sie den 1645/1646-Port. Geben Sie den **Befehl set radius server #.#.# auth-port 1645 acct-port 1646 primary** aus, um den Server und den entsprechenden Befehl im Cisco IOS als **RADIUS-Server-Quellports 1645-1646** zu definieren.
4. Definieren Sie den Serverschlüssel.Dies ist obligatorisch, da das Switch-to-Server-Kennwort

wie in RADIUS Authentication/Authorization RFC 2865 und RADIUS Accounting RFC 2866 verschlüsselt wird. Wenn sie verwendet wird, muss sie mit dem Server übereinstimmen. Geben Sie den **set radius key *your_key*-**Befehl ein.

Schritt C: Lokale Benutzername-Authentifizierung/Autorisierung

Ab CatOS 7.5.1 ist eine lokale Benutzerauthentifizierung möglich. Beispielsweise können Sie eine Authentifizierung/Autorisierung erreichen, indem Sie einen im Catalyst gespeicherten Benutzernamen und ein Kennwort verwenden, anstatt eine Authentifizierung mit einem lokalen Kennwort durchzuführen.

Es gibt nur zwei Berechtigungsebenen für die lokale Benutzerauthentifizierung: 0 oder 15. Level 0 ist die nicht privilegierte Führungsebene. Stufe 15 ist die privilegierte Aktivierungsstufe.

Wenn Sie diese Befehle in diesem Beispiel hinzufügen, wechselt der Benutzer `poweruser` in den Aktivierungsmodus auf einem Telnet oder einer Konsole zum Switch, und der Benutzer `nicht aktiviert` kommt im exec-Modus auf einem Telnet oder einer Konsole zum Switch.

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

Hinweis: Wenn der Benutzer `nicht aktiviert` das **festgelegte enable-**Kennwort kennt, kann dieser Benutzer den Modus weiterhin aktivieren.

Nach der Konfiguration werden die Kennwörter verschlüsselt gespeichert.

Die lokale Benutzername-Authentifizierung kann in Verbindung mit der Remote-TACACS+-exec-, Command Accounting- oder Remote-RADIUS Exec-Accounting verwendet werden. Es kann auch in Verbindung mit Remote-TACACS+ Exec- oder Befehlsautorisierung verwendet werden, aber es ist nicht sinnvoll, diesen auf diese Weise zu verwenden, da der Benutzername sowohl auf dem TACACS+-Server als auch lokal auf dem Switch gespeichert werden muss.

Schritt D - TACACS+-Befehlsautorisierung

In diesem Beispiel wird dem Switch angewiesen, die Autorisierung nur für Konfigurationsbefehle mit TACACS+ zu verlangen. Wenn der TACACS+-Server ausgefallen ist, ist keine Authentifizierung erforderlich. Dies gilt sowohl für den Konsolenport als auch für die Telnet-Sitzung. Geben Sie den folgenden Befehl ein:

set authorization-Befehle aktivieren config tacacacs none keine beiden

In diesem Beispiel können Sie den TACACS+-Server so konfigurieren, dass er beim Festlegen der folgenden Parameter zugelassen wird:

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

Der Befehl **set port enable 2/12** wird zur Überprüfung an den TACACS+-Server gesendet.

Hinweis: Bei aktivierter Befehlsautorisierung sendet der Switch im Gegensatz zu dem Router, bei

dem enable nicht als Befehl angesehen wird, den **enable**-Befehl an den Server, wenn versucht wird, eine Aktivierung durchzuführen. Stellen Sie sicher, dass der Server auch so konfiguriert ist, dass der Befehl **enable** zulässig ist.

Schritt E - TACACS+ Exec-Autorisierung

In diesem Beispiel wird dem Switch angewiesen, eine Autorisierung für eine Exec-Sitzung mit TACACS+ zu erfordern. Wenn der TACACS+-Server ausgefallen ist, ist keine Autorisierung erforderlich. Dies gilt sowohl für den Konsolenport als auch für die Telnet-Sitzung. Geben Sie den Befehl **set authorized exec enable tacacs+ none beide** Befehle aus.

Zusätzlich zur Authentifizierungsanforderung wird eine separate Autorisierungsanfrage vom Switch an den TACACS+-Server gesendet. Wenn das Benutzerprofil für Shell/exec auf dem TACACS+-Server konfiguriert ist, kann dieser Benutzer auf den Switch zugreifen.

Dadurch wird verhindert, dass Benutzer ohne auf dem Server konfigurierten Shell/Exec-Service, z. B. PPP-Benutzer, sich beim Switch anmelden. Sie erhalten die Meldung, dass die `Exec-Modusautorisierung fehlgeschlagen ist`. Zusätzlich zum Zulassen/Verweigern des exec-Modus für Benutzer können Sie in den Aktivierungsmodus gezwungen werden, wenn Sie die auf dem Server zugewiesene Berechtigungsstufe 15 eingeben. Es muss Code ausführen, in dem die Cisco Bug-ID CSCdr51314 (nur registrierte Kunden) behoben ist.

Schritt F - RADIUS Exec-Autorisierung

Es gibt keinen Befehl zum Aktivieren der RADIUS Exec-Autorisierung. Die Alternative besteht darin, im RADIUS-Server den Diensttyp (RADIUS-Attribut 6) auf "Administrative" (Wert 6) festzulegen, um den Benutzer im RADIUS-Server in den Aktivierungsmodus zu starten. Wenn der Servicetyp für andere als 6 administrative Einstellungen festgelegt ist, z. B. 1-login, 7-shell oder 2-framed, erreicht der Benutzer die Eingabeaufforderung des Switch exec, jedoch nicht die Eingabeaufforderung enable.

Fügen Sie diese Befehle zur Authentifizierung und Autorisierung in den Switch hinzu:

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

Schritt G - Abrechnung - TACACS+ oder RADIUS

So aktivieren Sie TACACS+ Accounting für:

1. Wenn Sie die Switch-Eingabeaufforderung erhalten, geben Sie den Befehl **set accounting exec enable start-stop tacacs+** ein.
2. Benutzer, die Telnet außerhalb des Switches verwenden, aktivieren den Befehl **set accounting connect enable start-stop tacacs+**.
3. Wenn Sie den Switch neu starten, geben Sie den Befehl **set accounting system enable start-stop tacacs+** ein.
4. Benutzer, die Befehle ausführen, geben die **set accounting-Befehle aus, um alle Start-Stopp-Taks+**-Befehle **zu aktivieren**.
5. Erinnert z. B. an den Server, Datensätze einmal pro Minute zu aktualisieren, um anzuzeigen,

dass der Benutzer noch angemeldet ist, geben Sie den Befehl **set accounting update periodisch 1 aus**.

So aktivieren Sie RADIUS Accounting für:

1. Benutzer, die die Switch-Eingabeaufforderung erhalten, geben den Befehl **set accounting exec enable start-stop radius** ein.
2. Benutzer, die Telnet aus dem Switch entfernen, geben den Befehl **set accounting connect ein, um den Radius-**Befehl **start-stop zu aktivieren**.
3. Wenn Sie den Switch neu starten, geben Sie den Befehl **set accounting system enable start-stop radius** ein.
4. Erinnert z. B. an den Server, Datensätze einmal pro Minute zu aktualisieren, um anzuzeigen, dass der Benutzer noch angemeldet ist, geben Sie den Befehl **set accounting update periodisch 1 aus**.

TACACS+ Freeware-Datensätze

Diese Ausgabe ist ein Beispiel dafür, wie die Datensätze auf dem Server angezeigt werden können:

```
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 auf UNIX-Datensatzausgabe

Diese Ausgabe ist ein Beispiel dafür, wie die Datensätze auf dem Server angezeigt werden können:

```
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
```

Schritt H: TACACS+-Authentifizierung aktivieren

Führen Sie diese Schritte aus:

1. Geben Sie den Befehl **set authentication enable local enable** ein, um sicherzustellen, dass bei einem Serverausfall eine Hintertür vorhanden ist.
2. Geben Sie den Befehl **set authentication enable tacacs enable** ein, um den Switch anzuweisen, Aktivierungsanfragen an den Server zu senden.

Schritt I: RADIUS-Authentifizierung aktivieren

Fügen Sie diese Befehle hinzu, damit der Switch den Benutzernamen `$enab15$` an den RADIUS-Server sendet. Nicht alle RADIUS-Server unterstützen einen solchen Benutzernamen. In Schritt E finden Sie eine weitere Alternative, z. B. wenn Sie einen Diensttyp [RADIUS-Attribut 6 - to Administrative] festlegen, der einzelne Benutzer in den Aktivierungsmodus startet.

1. Geben Sie den Befehl **set authentication enable local enable** ein, um sicherzustellen, dass eine Hintertür geöffnet ist, wenn der Server ausgefallen ist.
2. Geben Sie den Befehl **set authentication enable radius enable** ein, um den Switch anzuweisen, Aktivierungsanfragen an den Server zu senden, wenn der RADIUS-Server den $enab15$-Benutzernamen unterstützt.

Schritt J - TACACS+-Autorisierung aktivieren

Wenn dieser Befehl hinzugefügt wird, sendet der Switch enable an den Server, wenn der Benutzer versucht, dies zu aktivieren. Dem Server muss der Befehl **enable** erlaubt sein. In diesem Beispiel gibt es ein Failover auf none, wenn der Server ausgefallen ist:

set author enable enable tacacacs+ Keine beiden

Schritt K - Kerberos-Authentifizierung

Unter Steuern und Überwachen des Zugriffs auf den Switch mithilfe von Authentifizierung, Autorisierung und Abrechnung finden Sie weitere Informationen zum Einrichten von Kerberos für den Switch.

Kennwortwiederherstellung

Unter Kennwortwiederherstellungsverfahren finden Sie weitere Informationen zu Kennwortwiederherstellungsverfahren.

Diese Seite ist der Index der Kennwortwiederherstellungsverfahren für Cisco Produkte.

ip permit-Befehle für zusätzliche Sicherheit

Für zusätzliche Sicherheit kann Catalyst so konfiguriert werden, dass der Telnet-Zugriff über die Befehle **ip permit** gesteuert wird:

set ipermit enable telnet

set ip permit ***range mask|host***

Dadurch wird nur der Bereich bzw. die Hosts zugelassen, die für Telnet im Switch angegeben sind.

Debuggen auf dem Catalyst

Überprüfen Sie vor dem Aktivieren des Debuggens auf dem Catalyst die Serverprotokolle aus Fehlergründen. Dies ist für den Switch einfacher und weniger störend. Bei früheren Switch-Versionen wurde das **Debuggen** im Engineering-Modus durchgeführt. Es ist nicht erforderlich, auf den Engineering-Modus zuzugreifen, um **Debugbefehle** in späteren Codeversionen auszuführen:

set trace tacacacacs|radius|kerberos 4

Hinweis: Der Befehl **set trace tacacs|radius|kerberos 0** gibt den Catalyst in den Non-Tracing-Modus zurück.

Auf der Support-Seite für Switches finden Sie weitere Informationen zu Multilayer-LAN-Switches.

Zugehörige Informationen

- TACACS+- und RADIUS-Vergleich
- RADIUS, TACACS+ und Kerberos in Cisco IOS-Dokumentation
- RADIUS-Support-Seite
- Support-Seite für TACACS/TACACS+
- Support-Seite für Kerberos

- Anforderungen für Kommentare (RFCs)
- Technischer Support und Dokumentation für Cisco Systeme