Konfigurieren der RADIUS Server-Fallback-Funktion auf Wireless LAN-Controllern

Inhalt

Einführung

In diesem Dokument wird beschrieben, wie die RADIUS-Serverfallbackfunktion mit Wireless LAN-Controllern (WLCs) konfiguriert wird.

Voraussetzungen

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- Grundkenntnisse der Konfiguration von Lightweight Access Points (LAPs) und Cisco WLCs
- Grundkenntnisse der Steuerung und Bereitstellung des Wireless Access Point Protocol (CAPWAP)
- Grundkenntnisse der Wireless-Sicherheitslösungen

Verwendete Komponenten

Die Informationen in diesem Dokument basieren auf einem Cisco 5508/5520 Controller.

Die Informationen in diesem Dokument wurden von den Geräten in einer bestimmten Laborumgebung erstellt. Alle in diesem Dokument verwendeten Geräte haben mit einer leeren

(Standard-)Konfiguration begonnen. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die potenziellen Auswirkungen eines Befehls verstehen.

Hintergrundinformationen

RADIUS-Serverfallback-Funktion

WLC-Softwareversionen vor Version 5.0 unterstützen den RADIUS-Serverfallbackmechanismus nicht. Wenn der primäre RADIUS-Server nicht mehr verfügbar ist, führt der WLC ein Failover auf den nächsten RADIUS-Server für aktive Backups durch. Der WLC verwendet weiterhin den sekundären RADIUS-Server für immer, selbst wenn der primäre Server verfügbar ist. In der Regel ist der primäre Server eine hohe Leistung und der bevorzugte Server.

In WLC 5.0 und höheren Versionen unterstützt der WLC die RADIUS-Serverfallbackfunktion. Mit dieser Funktion kann der WLC so konfiguriert werden, dass überprüft wird, ob der primäre Server verfügbar ist, und zurück zum primären RADIUS-Server, sobald dieser verfügbar ist. Dazu unterstützt der WLC zwei neue Modi, passiv und aktiv, um den Status des RADIUS-Servers zu überprüfen. Der WLC kehrt nach dem angegebenen Timeout-Wert zum am besten geeigneten Server zurück.

Fallback-Modi

Aktiver Modus

Wenn ein Server im aktiven Modus nicht auf die WLC-Authentifizierungsanforderung reagiert, markiert der WLC den Server als "Dead" (Deaktiviert) und verschiebt den Server dann in den nicht aktiven Serverpool und beginnt, regelmäßig Testnachrichten zu senden, bis der Server antwortet. Wenn der Server antwortet, verschiebt der WLC den Dead-Server in den aktiven Pool und beendet das Senden von Sonde-Nachrichten. Wenn in diesem Modus eine Authentifizierungsanfrage eingeht, wählt der WLC immer den Server mit dem niedrigsten Index (höchste Priorität) aus dem aktiven Pool der RADIUS-Server aus.

Der WLC sendet nach dem Timeout (der Standardwert ist 300 Sekunden) ein Prüfpaket, um den Serverstatus für den Fall zu bestimmen, dass der Server früher nicht reagiert.

Passiver Modus

Wenn ein Server im passiven Modus nicht auf die WLC-Authentifizierungsanforderung reagiert, verschiebt der WLC den Server in die inaktive Warteschlange und setzt einen Timer. Wenn der Timer abläuft, verschiebt der WLC den Server in die aktive Warteschlange, unabhängig vom tatsächlichen Serverstatus. Wenn eine Authentifizierungsanfrage eingeht, wählt der WLC den Server mit dem niedrigsten Index (höchste Priorität) aus der aktiven Warteschlange aus (zu der auch der nicht aktive Server gehören kann). Wenn der Server nicht reagiert, markiert der WLC ihn als inaktiv, legt den Timer fest und wechselt zum Server mit der höchsten Priorität. Dieser Prozess wird fortgesetzt, bis der WLC einen aktiven RADIUS-Server findet oder der aktive Serverpool erschöpft ist.

Der WLC geht davon aus, dass der Server nach dem Timeout aktiv ist (der Standardwert ist 300 Sekunden), falls der Server zuvor nicht reagiert. Wenn der WLC immer noch nicht reagiert, wartet er auf ein anderes Timeout und versucht es erneut, wenn eine Authentifizierungsanfrage eingeht.

Aus-Modus

Im Aus-Modus unterstützt der WLC nur Failover. Mit anderen Worten: Der Fallback ist deaktiviert. Wenn der primäre RADIUS-Server ausfällt, führt der WLC ein Failover auf den nächsten RADIUS-Server für aktive Backups durch. Der WLC verwendet weiterhin den sekundären RADIUS-Server für immer, selbst wenn der primäre Server verfügbar ist.

Konfigurieren

Konfigurieren der RADIUS Server-Fallback-Funktion mithilfe der CLI

> **Hinweis**: Verwenden Sie das Command Lookup Tool (nur registrierte Kunden), um weitere Informationen zu den in diesem Abschnitt verwendeten Befehlen zu erhalten.

Verwenden Sie diese Befehle aus der WLC-CLI, um die RADIUS-Serverfallbackfunktion im WLC zu aktivieren.

Der erste Schritt besteht darin, den Modus des RADIUS-Serverfallbacks auszuwählen. Wie bereits erwähnt, unterstützt der WLC die aktiven und passiven Fallbackmodi.

Geben Sie den folgenden Befehl ein, um den Fallbackmodus auszuwählen:

```
WLC1 > config radius fallback-test mode {active/passive/off}
```

- active - Sendet Probes an tote Server, um den Status zu testen.
- passive - Legt den Serverstatus basierend auf der letzten Transaktion fest.
- off - Deaktiviert den Serverfallbacktest (Standard).

Der nächste Schritt besteht in der Auswahl des Intervalls, das das Messintervall für den aktiven Modus oder die inaktive Zeit für die passiven Betriebsmodi angibt.

Geben Sie den folgenden Befehl ein, um das Intervall festzulegen:

```
WLC1 > config radius fallback-test mode interval {180 - 3600}
```

<180 bis 3600**>** - Geben Sie das Messintervall oder die inaktive Zeit in Sekunden ein (der Standardwert ist 300 Sekunden).

Das Intervall gibt das Messintervall im Falle eines Fallbacks im aktiven Modus oder einer inaktiven Zeit im Falle eines Fallbacks im passiven Modus an.

Für den aktiven Betriebsmodus müssen Sie einen Benutzernamen konfigurieren, der in der Anfrage verwendet wird, die an den RADIUS-Server gesendet wird.

Geben Sie den folgenden Befehl ein, um den Benutzernamen zu konfigurieren:

```
WLC1 >config radius fallback-test username {username}
```

<Benutzername> - Geben Sie einen Namen mit bis zu 16 alphanumerischen Zeichen ein (der Standardwert ist "cisco-probe").

> **Hinweis**: Sie können Ihren eigenen Benutzernamen eingeben oder den Standard beibehalten. Der Standardbenutzername ist "cisco-probe". Da dieser Benutzername zum Senden von Sonde-Nachrichten verwendet wird, müssen Sie kein Kennwort konfigurieren.

Konfigurieren der RADIUS Server-Fallback-Funktion mithilfe der GUI

Gehen Sie wie folgt vor, um den WLC mit der GUI zu konfigurieren:

1. Konfigurieren Sie den Modus des RADIUS-Serverfallbacks. Wählen Sie dazu **Security > RADIUS > Fallback** in der WLC-GUI aus. Die Seite **RADIUS > Fallback Parameters** wird angezeigt.
2. Wählen Sie aus der Dropdown-Liste **Fallbackmodus** den Fallbackmodus aus. Zu den verfügbaren Optionen gehören "active", "passive" und "off".Im Folgenden finden Sie ein Beispiel-Screenshot für die Konfiguration des aktiven Fallbackmodus, wie im Bild gezeigt.

3. Geben Sie im aktiven Betriebsmodus den Benutzernamen im Feld Benutzername ein.
4. Geben Sie den Wert für das Testintervall in Sekunden ein. ein.
5. Klicken Sie auf **Übernehmen**.

Wenn die aggressive Failover-Funktion im WLC aktiviert ist, ist der WLC zu aggressiv, um den AAA-Server als "nicht reagiert" zu markieren. Dies sollte jedoch nicht geschehen, da der AAA-Server möglicherweise nicht nur auf diesen Client reagiert, wenn Sie stummschalten. Es kann eine Antwort auf andere gültige Clients mit gültigen Zertifikaten sein. Der WLC kann den AAA-Server weiterhin als "nicht antworten" und "nicht funktionsfähig" markieren.

Um dies zu vermeiden, deaktivieren Sie die Funktion für aggressive Ausfallsicherung. Geben Sie den Befehl **config radius aggressive-Failover disable** aus der Controller-GUI ein, um dies auszuführen. Wenn diese Option deaktiviert ist, wird der Controller nur dann zum nächsten AAA-Server umgeleitet, wenn drei aufeinander folgende Clients keine Antwort vom RADIUS-Server erhalten.

> **Hinweis**: Funktionsänderung, eingeführt in Version 8.5.140, 8.8.100, 8.10.105 und höher: Wenn das aggressive RADIUS-Failover für den Controller deaktiviert ist: Das Paket wird sechsmal wiederholt, es sei denn, es kommt zu einem Abbruch von Clients. Der RADIUS-

Server (sowohl AUTH als auch ACCT) ist nach drei Timeout-Ereignissen (18 aufeinander folgende Wiederholungen) von mehreren Clients (zuvor von genau drei Clients) als nicht erreichbar gekennzeichnet. Wenn RADIUS Aggressive Failover für den Controller aktiviert ist: Das Paket wird sechsmal wiederholt, es sei denn, es kommt zu einem Abbruch von Clients. Der RADIUS-Server (sowohl AUTH als auch ACCT) ist nach einem Timeout-Ereignis (6 aufeinander folgende Wiederholungen) von mehreren Clients (zuvor von genau einem Client) als nicht erreichbar gekennzeichnet. Das bedeutet, dass 18 aufeinander folgende Wiederholungen pro RADIUS-Server (entweder AUTH oder ACCT) von mehreren Clients sein können. Daher ist nicht immer gewährleistet, dass jedes Paket sechsmal erneut versucht wird.

Überprüfen

In diesem Abschnitt überprüfen Sie, ob Ihre Konfiguration ordnungsgemäß funktioniert.

Das Output Interpreter Tool (nur registrierte Kunden) (OIT) unterstützt bestimmte **show**-Befehle. Verwenden Sie das OIT, um eine Analyse der **Ausgabe des** Befehls **show** anzuzeigen.

Geben Sie den Befehl **show radius summary** ein, um die Fallbackkonfiguration zu überprüfen. Hier ein Beispiel:

```
WLC1 >show radius summary

Vendor Id Backward Compatibility..... Disabled
Call Station Id Type.................. IP Address
Aggressive Failover................... Enabled
Keywrap............................... Disabled

Fallback Test:
Test Mode..................................... Active
Probe User Name............................... testaccount
Interval (in seconds)......................... 180

Authentication Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/Encr
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------------
1 NM 10.1.1.12 1812 Enabled 2 Disabled Disabled-none/unknown/group-0/0 none/none

Accounting Servers

Idx Type Server Address Port State Tout RFC3576 IPSec-AuthMode/Phase1/Group/Lifetime/Auth/E
--- ---- -------------- ---- ------- ---- ------- ----------------------------------------
1 N 10.1.1.12 1813 Enabled 2 N/A Disabled-none/unknown/group-0/0 none/nonen
```

Fehlerbehebung

Dieser Abschnitt enthält Informationen zur Fehlerbehebung in Ihrer Konfiguration.

Hinweis: Weitere Informationen zu Debug-Befehlen vor der Verwendung von **Debug-**Befehlen finden Sie unter Wichtige Informationen.

- **debug dot1x events enable** - Konfiguriert das Debuggen von 802.1X-Ereignissen.

- **debug aaa events enable:** Konfiguriert Debugging aller AAA-Ereignisse.

Zugehörige Informationen

- Konfigurationsbeispiel für EAP-Authentifizierung mit WLAN-Controllern (WLC)
- Lightweight AP (LAP)-Registrierung bei einem Wireless LAN Controller (WLC)
- Konfigurieren von Sicherheitslösungen
- Konfigurationsbeispiel für dynamische VLAN-Zuweisung mit RADIUS-Server und Wireless LAN-Controller
- Technischer Support und Dokumentation - Cisco Systems