Configurazione della funzionalità di fallback del server RADIUS sui controller LAN wireless

Sommario

Introduzione

In questo documento viene descritto come configurare la funzione di fallback del server RADIUS con i Wireless LAN Controller (WLC).

Prerequisiti

Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- Conoscenze base della configurazione dei Lightweight Access Point (LAP) e dei Cisco WLC
- Conoscenze base di controllo e provisioning di CAPWAP (Wireless Access Point Protocol)
- Conoscenze base delle soluzioni per la sicurezza wireless

Componenti usati

Per questo documento, è stato usato un controller Cisco 5508/5520.

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.

Premesse

Funzione di fallback del server RADIUS

Le versioni del software WLC precedenti alla 5.0 non supportano il meccanismo di fallback del server RADIUS. Quando il server RADIUS primario diventa non disponibile, il WLC eseguirà il failover sul successivo server RADIUS di backup attivo. Il WLC continuerà a utilizzare il server RADIUS secondario per sempre anche se il server primario è disponibile. In genere, il server principale è il server preferito e offre prestazioni elevate.

In WLC 5.0 e versioni successive, il WLC supporta la funzione di fallback del server RADIUS. Con questa funzione, il WLC può essere configurato in modo da controllare se il server primario è disponibile e da tornare al server RADIUS primario quando è disponibile. A tal fine, il WLC supporta due nuove modalità, passiva e attiva, per controllare lo stato del server RADIUS. Il WLC ritorna al server preferibile dopo il valore di timeout specificato.

Modalità Fallback

Modalità attiva

In modalità attiva, quando un server non risponde alla richiesta di autenticazione WLC, il WLC contrassegna il server come inattivo e quindi lo sposta nel pool di server non attivo e avvia periodicamente l'invio di messaggi di richieste finché il server non risponde. Se il server risponde, il WLC sposta il server inattivo nel pool attivo e interrompe l'invio dei messaggi di richieste. In questa modalità, quando arriva una richiesta di autenticazione, il WLC sceglie sempre il server di indice più basso (con priorità più alta) dal pool attivo di server RADIUS.

Il WLC invia un pacchetto di richiesta dopo il timeout (l'impostazione predefinita è 300 secondi) per determinare lo stato del server nel caso in cui il server non rispondesse in precedenza.

Modalità passiva

In modalità passiva, se un server non risponde alla richiesta di autenticazione WLC, il WLC sposta il server nella coda inattiva e imposta un timer. Alla scadenza del timer, il WLC sposta il server nella coda attiva indipendentemente dallo stato effettivo del server. Quando riceve una richiesta di autenticazione, il WLC sceglie il server di indice più basso (con la priorità più alta) dalla coda attiva (che potrebbe includere il server non attivo). Se il server non risponde, il WLC lo contrassegna come inattivo, imposta il timer e passa al successivo server con la priorità più alta. Questo processo continua finché il WLC non trova un server RADIUS attivo o finché il pool di server attivo non è esaurito.

Il WLC presume che il server sia attivo dopo il timeout (il valore predefinito è 300 secondi) nel caso in cui il server non rispondesse in precedenza. Se non risponde, il WLC attende un altro timeout e riprova quando arriva una richiesta di autenticazione.

Modalità Off

In modalità off, il WLC supporta solo il failover. In altre parole, il fallback è disabilitato. Quando il

server RADIUS primario diventa inattivo, il WLC eseguirà il failover sul successivo server RADIUS di backup attivo. Il WLC continua a utilizzare il server RADIUS secondario per sempre, anche se il server primario è disponibile.

Configurazione

Configurazione della funzionalità di fallback del server RADIUS con la CLI

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

Usare questi comandi dalla CLI del WLC per abilitare la funzione di fallback del server RADIUS sul WLC.

Il primo passaggio consiste nella selezione della modalità di fallback del server RADIUS. Come accennato in precedenza, il WLC supporta modalità di fallback attive e passive.

Per selezionare la modalità di fallback, immettere questo comando:

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

- active: invia richieste ai server inattivi per verificare lo stato.
- passive - Imposta lo stato del server in base all'ultima transazione.
- off - Disattiva il test di fallback del server (impostazione predefinita).

Il passaggio successivo consiste nel selezionare l'intervallo che specifica l'intervallo di sonda per la modalità attiva o il tempo di inattività per le modalità di funzionamento passive.

Per impostare l'intervallo, immettere questo comando:

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

<180-3600> - Immettere l'intervallo di sonda o il tempo di inattività in secondi (l'impostazione predefinita è 300 secondi).

L'intervallo specifica l'intervallo del probe in caso di fallback in modalità attiva o di tempo inattivo in caso di fallback in modalità passiva.

Per la modalità operativa attiva, è necessario configurare un nome utente da utilizzare nella richiesta di richiesta di richiesta inviata al server RADIUS.

Per configurare il nome utente, immettere questo comando:

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

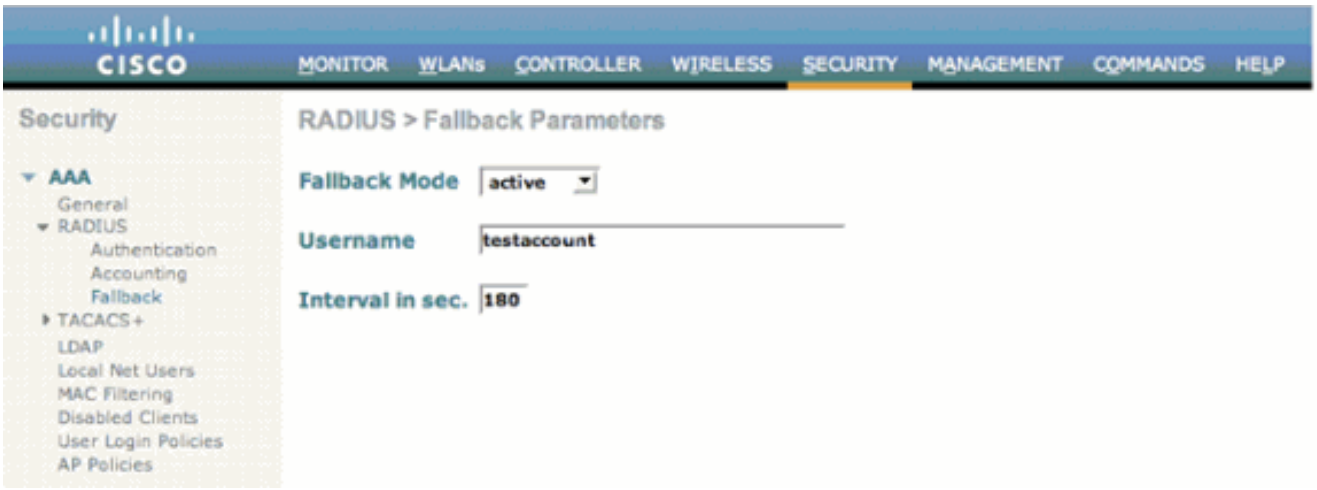
<username> - Immettere un nome composto da un massimo di 16 caratteri alfanumerici (l'impostazione predefinita è cisco-probe).

Nota: È possibile immettere il proprio nome utente o lasciare quello predefinito. Il nome utente predefinito è "cisco-probe". Poiché questo nome utente viene utilizzato per inviare i messaggi di richiesta, non è necessario configurare una password.

Configurazione della funzione di fallback del server RADIUS con la GUI

Completare questi passaggi per configurare il WLC con la GUI:

1. Configurare la modalità di fallback del server RADIUS. A tale scopo, selezionare **Sicurezza > RADIUS > Fallback** dall'interfaccia utente del WLC. Viene visualizzata la pagina **RADIUS > Parametri di fallback**.
2. Dall'elenco a discesa **Modalità fallback**, selezionare la modalità di fallback. Le opzioni disponibili includono attivo, passivo e disattivato.Di seguito è riportato un esempio di schermata per la configurazione della modalità fallback attiva, come mostrato nell'immagine.



3. Per la modalità di funzionamento attiva, immettere il nome utente nel campo username.
4. Immettere il valore dell'intervallo della sonda in Intervallo in secondi. campo.
5. Fare clic su **Apply** (Applica).

Se la funzione di failover aggressivo è abilitata nel WLC, il WLC è troppo aggressivo per contrassegnare il server AAA come "che non risponde". Tuttavia, non è consigliabile eseguire questa operazione perché è possibile che il server AAA non risponda solo a quel determinato client in caso di eliminazione invisibile all'utente. Può essere una risposta ad altri client validi con certificati validi. Il WLC può ancora contrassegnare il server AAA come "non rispondente" e "non funzionante".

Per risolvere questo problema, disattivare la funzione di failover aggressivo. Per eseguire questa operazione, immettere il comando **config radius aggressive-failover disable** dall'interfaccia utente del controller. Se questa opzione è disabilitata, il controller eseguirà il failover sul server AAA successivo solo se sono presenti tre client consecutivi che non sono in grado di ricevere una risposta dal server RADIUS.

Nota: La modifica della funzionalità è stata introdotta nelle release 8.5.140,8.8.100,8.10.105 e successive: Quando il failover aggressivo RADIUS per il controller è disabilitato: Il pacchetto viene ritentato sei volte a meno che non si verifichi un'interruzione da parte dei client. Il server RADIUS (sia AUTH che ACCT) è contrassegnato come non raggiungibile dopo tre eventi di timeout (18 tentativi consecutivi) da più client (in precedenza, esattamente

tre client). Quando è abilitato il failover aggressivo RADIUS per il controller: Il pacchetto viene ritentato sei volte a meno che non si verifichi un'interruzione da parte dei client. Il server RADIUS (sia AUTH che ACCT) è contrassegnato come non raggiungibile dopo un evento di timeout (6 tentativi consecutivi) da più client (in precedenza, da un solo client). Significa che è possibile eseguire 18 tentativi consecutivi per server RADIUS (AUTH o ACCT) da più client. Pertanto, non è sempre garantito che ciascun pacchetto venga riprovato sei volte.

Verifica

Per verificare che la configurazione funzioni correttamente, consultare questa sezione.

Lo strumento Output Interpreter (solo utenti registrati) (OIT) supporta alcuni comandi **show**. Usare l'OIT per visualizzare un'analisi dell'output del comando **show**.

Immettere il comando **show radius summary** per verificare la configurazione di fallback. Di seguito è riportato un esempio:

```
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
```

Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

Nota: consultare le informazioni importanti sui comandi di debug prima di usare i comandi di **debug.**

- **debug dot1x events enable** - Configura i debug degli eventi 802.1X.
- **debug aaa events enable**: configura il debug di tutti gli eventi AAA.

Informazioni correlate

- Esempio di configurazione dell'autenticazione EAP con i controller WLAN (WLC)
- Registrazione di un Lightweight AP (LAP) su un Wireless LAN Controller (WLC)
- Configurazione delle soluzioni di sicurezza
- Esempio di assegnazione dinamica di VLAN con il server RADIUS e il controller LAN wireless
- Documentazione e supporto tecnico – Cisco Systems