Risoluzione dei problemi di carico della CPU del controller LAN wireless

Sommario

Introduzione

Questo documento descrive come monitorare l'utilizzo della CPU sui controller LAN wireless Catalyst 9800 e fornisce diverse raccomandazioni per la configurazione.

Informazioni sull'utilizzo della CPU

Prima di approfondire la risoluzione dei problemi relativi al carico della CPU, è necessario comprendere le nozioni di base sull'utilizzo delle CPU nei controller LAN wireless Catalyst 9800 e alcuni dettagli sull'architettura software.

In generale, il documento sulle best practice di Catalyst 9800 definisce un insieme di impostazioni di configurazione appropriate che possono impedire problemi a livello di applicazione, ad esempio l'utilizzo di filtri di posizione per mDNS o la garanzia che l'esclusione dei client sia sempre abilitata. Si consiglia di applicare tali suggerimenti insieme agli argomenti esposti in questa sezione.

Nozioni di base sulle piattaforme

I controller Catalyst 9800 sono stati progettati come piattaforma flessibile, per gestire diversi carichi di rete e focalizzarsi sulla scalabilità orizzontale. Il nome di sviluppo interno era "eWLC" con la e per "elastic", per indicare che la stessa architettura software sarebbe stata in grado di essere eseguita da un sistema singolo incorporato CPU di piccole dimensioni a più appliance CPU/core su larga scala.

Ogni WLC ha avuto due "facce" distinte:

- Control Plane: gestione di tutte le interazioni di "gestione" come CLI, UI, Netconf e tutti i processi di caricamento per client e access point.
- Data plane: è responsabile dell'inoltro effettivo dei pacchetti e della decapsulazione di CAPWAP, dell'applicazione della policy AVC e di altre funzionalità.

Piano di controllo

- La maggior parte dei processi Cisco IOS-XE viene eseguita con BinOS (Linus Kernel), con una programmazione e comandi di monitoraggio specifici.
- Esiste un insieme di processi chiave, denominati WNCD (Wireless Network Control Daemon), ognuno dei quali dispone di un database in memoria locale, che gestisce la maggior parte dell'attività wireless. Ogni CPU possiede un WNCD, per distribuire il carico tra tutti i core CPU disponibili a ciascun sistema
- La distribuzione del carico tra WNCD viene eseguita durante il join AP. Quando un access point esegue un join CAPWAP al controller, un load balancer interno distribuisce l'access point utilizzando un set di regole possibili, per garantire un utilizzo corretto di tutte le risorse CPU disponibili.
- Il codice Cisco IOS® viene eseguito sul proprio processo denominato IOSd e dispone di un'utilità di pianificazione della CPU e di comandi di monitoraggio. In questo modo vengono gestite funzionalità specifiche, ad esempio CLI, SNMP, multicast e routing.

In una visualizzazione semplificata, il controller ha meccanismi di comunicazione tra il control e il data plane, "punt", invia il traffico dalla rete al control plane, e "injection", spinge i frame dal control plane alla rete.

Come parte di una possibile indagine di risoluzione dei problemi della CPU elevata, è necessario monitorare il meccanismo punt, per valutare quale traffico sta raggiungendo il control plane e potrebbe portare a un carico elevato.

Piano dati

Per il controller Catalyst 9800, viene eseguito come parte del Cisco Packet Processor (CPP), una struttura software per lo sviluppo di motori di inoltro pacchetti, utilizzata in più prodotti e tecnologie.

L'architettura consente un set di funzionalità comune, tra diverse implementazioni hardware o software, ad esempio, consentendo funzionalità simili per 9800CL rispetto a 9800-40, a diverse scale di throughput.

Bilanciamento del carico AP

Il WLC esegue il bilanciamento del carico tra le CPU durante il processo di join dell'access point CAPWAP, con l'elemento di differenziazione della chiave che è il nome tag del sito dell'access point. L'idea è che ogni access point rappresenti un carico di CPU specifico aggiunto, derivante dalla sua attività client, e l'access point stesso. Per eseguire questo bilanciamento, è possibile utilizzare diversi meccanismi:

- Se l'access point utilizza "default-tag", viene bilanciato in modo round-robin su tutte le CPU/WNCD, con ogni nuovo join dell'access point che passa al successivo WNCD. Questo è il metodo più semplice, ma ha alcune implicazioni:
    - Si tratta dello scenario subottimale, in quanto i punti di accesso nello stesso dominio di roaming RF eseguirebbero frequentemente roaming inter-WNCD, comportando ulteriori comunicazioni tra processi. Il roaming tra istanze è più lento di una piccola percentuale.
    - Per il tag del sito FlexConnect (remoto), non è disponibile alcuna distribuzione di chiavi PMK. Ciò significa che non è possibile eseguire il roaming veloce per la modalità Flex, con un impatto sulle modalità di roaming OKC/FT.

      In generale, il tag predefinito può essere utilizzato in scenari di carico inferiore (ad esempio, meno del 40% del carico dell'access point e del client della piattaforma 9800) e per l'installazione di FlexConnect solo quando il roaming veloce non è un requisito.

- Se l'access point ha un tag del sito personalizzato, la prima volta che un access point appartenente al nome del tag del sito si unisce al controller, il tag del sito viene assegnato a una specifica istanza WNCD. Tutti i successivi join aggiuntivi con lo stesso tag vengono assegnati allo stesso WNCD. Ciò garantisce il roaming tra gli access point nello stesso tag di sito, che avviene nel contesto WCND, che fornisce un flusso ottimale, con un minore utilizzo della CPU. Il roaming tra WNCD è supportato, ma non è ottimale come il roaming all'interno di WNCD.

- Decisione di bilanciamento del carico predefinita: quando un tag viene assegnato a un WNCD, il servizio di bilanciamento del carico seleziona l'istanza con il numero di tag di sito più basso in quel momento. Poiché il carico totale che tale tag di sito potrebbe avere non è noto, può causare scenari di bilanciamento non ottimali. Ciò dipende dall'ordine dei join AP, dal numero di tag di sito definiti e dall'eventuale asimmetria del conteggio AP

- Bilanciamento del carico statico: per impedire l'assegnazione di tag di sito non bilanciati a WNCD, il comando di caricamento del sito è stato introdotto nella versione 17.9.3 e successive, per consentire agli amministratori di predefinire il carico previsto di ogni tag di sito. Ciò è particolarmente utile quando si gestiscono scenari di campus o più filiali, ognuna mappata a diversi conteggi AP, per garantire che il carico sia distribuito uniformemente in WNCD.

Ad esempio, se si dispone di un access point serie 9800-40 che gestisce un ufficio principale più 5 filiali con un numero di punti di accesso diverso, la configurazione potrebbe essere simile alla

seguente:

```
wireless tag site office-main
 load 120

wireless tag site branch-1
 load 10

wireless tag site branch-2
 load 12

wireless tag site branch-3
 load 45

wireless tag site branch-4
 load 80

wireless tag site branch-5
 load 5
```

In questo scenario, non si desidera che il tag dell'ufficio principale si trovi nello stesso WNCD della filiale 3 e della filiale 4, che siano presenti in totale 6 tag del sito e che la piattaforma disponga di 5 WNCD, quindi è possibile che i tag del sito con il carico più elevato si trovino sulla stessa CPU. Utilizzando il comando load è possibile creare una topologia di bilanciamento del carico del punto di accesso prevedibile.

Il comando load è un hint di dimensione previsto. Non deve corrispondere esattamente al numero di punti di accesso, ma in genere è impostato sui punti di accesso previsti che potrebbero unirsi.

- Negli scenari in cui sono presenti edifici di grandi dimensioni gestiti da un singolo controller, è più semplice e semplice creare un numero di tag sito pari a quello dei WNCD per la piattaforma specifica (ad esempio, C9800-40 ne ha cinque, C9800-80 ne ha otto). Assegnare i punti di accesso nella stessa area o nello stesso dominio di roaming agli stessi tag di sito per ridurre al minimo la comunicazione tra WNCD.
- Bilanciamento del carico RF: consente di bilanciare i punti di accesso tra le istanze WNCD, utilizzando la relazione RF adiacente di RRM, e di creare sottogruppi in base alla vicinanza tra i punti di accesso. Questa operazione deve essere eseguita dopo che i punti di accesso sono stati attivati per un certo periodo di tempo ed è stata eliminata la necessità di configurare eventuali impostazioni di bilanciamento del carico statico. È disponibile dalla versione 17.12 e successive.

Come scoprire quanti WNCD sono presenti?

Per le piattaforme hardware, il conteggio WNCD è fisso: 9800-40 ha 5, 9800-80 ha 8. Per 9800CL (virtuale), il numero di WNCD dipende dal modello di macchina virtuale utilizzato durante la distribuzione iniziale.

Come regola generale, se si desidera conoscere il numero di WNCD in esecuzione nel sistema, è

possibile utilizzare questo comando per tutti i tipi di controller:

<#root>

```
9800-40#show processes cpu platform sorted  |  count wncd
Number of lines which match regexp =
```

5

Nel caso specifico di 9800-CL, è possibile utilizzare il comando **show platform software system all** per raccogliere i dettagli sulla piattaforma virtuale:

<#root>

9800cl-1#show platform software system all
Controller Details:
==========
VM Template: small
Throughput Profile: low
AP Scale: 1000
Client Scale: 10000

WNCD instances: 1

Monitoraggio del bilanciamento del carico AP

L'assegnazione da AP a WNCD viene applicata durante il processo di join CAPWAP dell'access point, pertanto non è prevista alcuna modifica durante le operazioni, indipendentemente dal metodo di bilanciamento, a meno che non si verifichi un evento di reimpostazione CAPWAP a livello di rete in cui tutti gli access point si disconnettono e si ricongiungono.

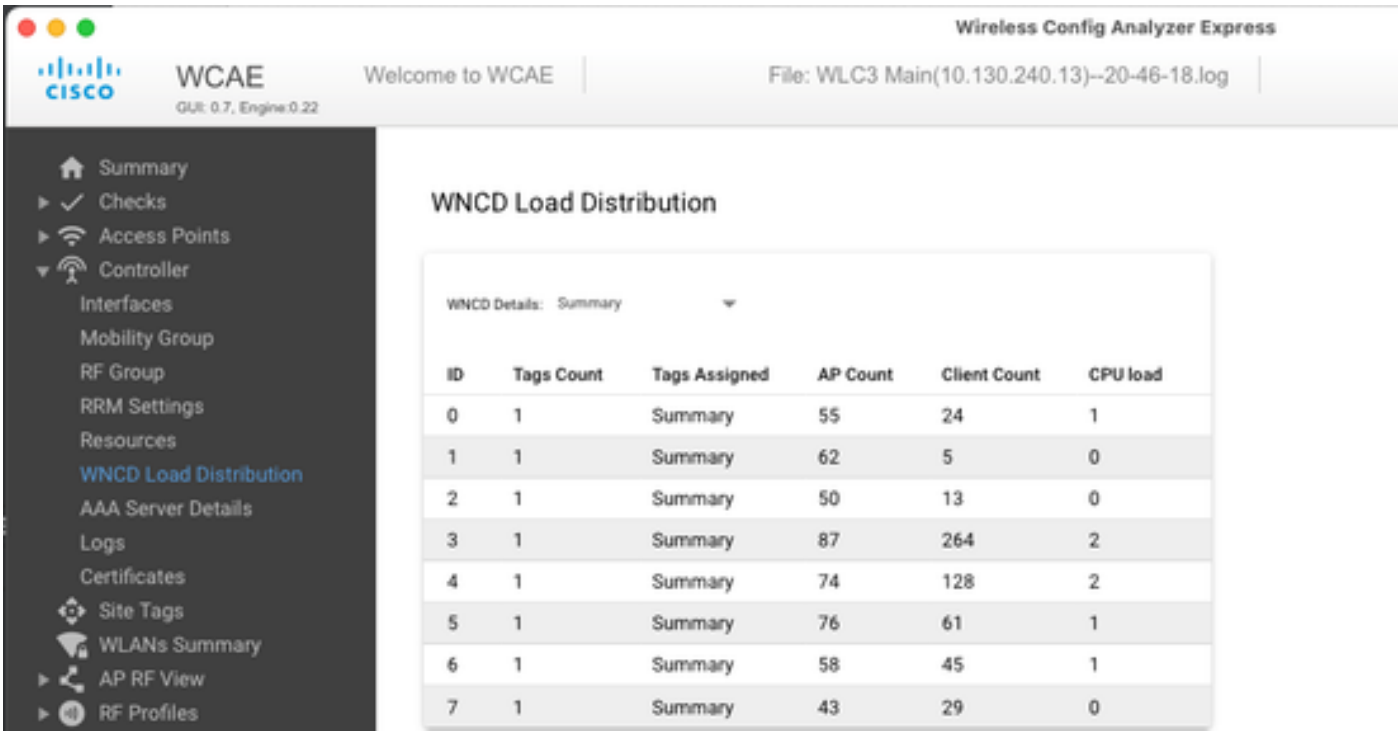
Il comandoshow wireless loadbalance tag affinity CLI può fornire un modo semplice per visualizzare lo stato corrente del bilanciamento del carico dell'access point in tutte le istanze WNCD:

98001#show wireless loadbalance tag affinity

Tag	Tag type	No of AP's Joined	Load Config	Wncd Instance
Branch-tag	SITE TAG	10	0	0
Main-tag	SITE TAG	200	0	1
default-site-tag	SITE TAG	1	NA	2

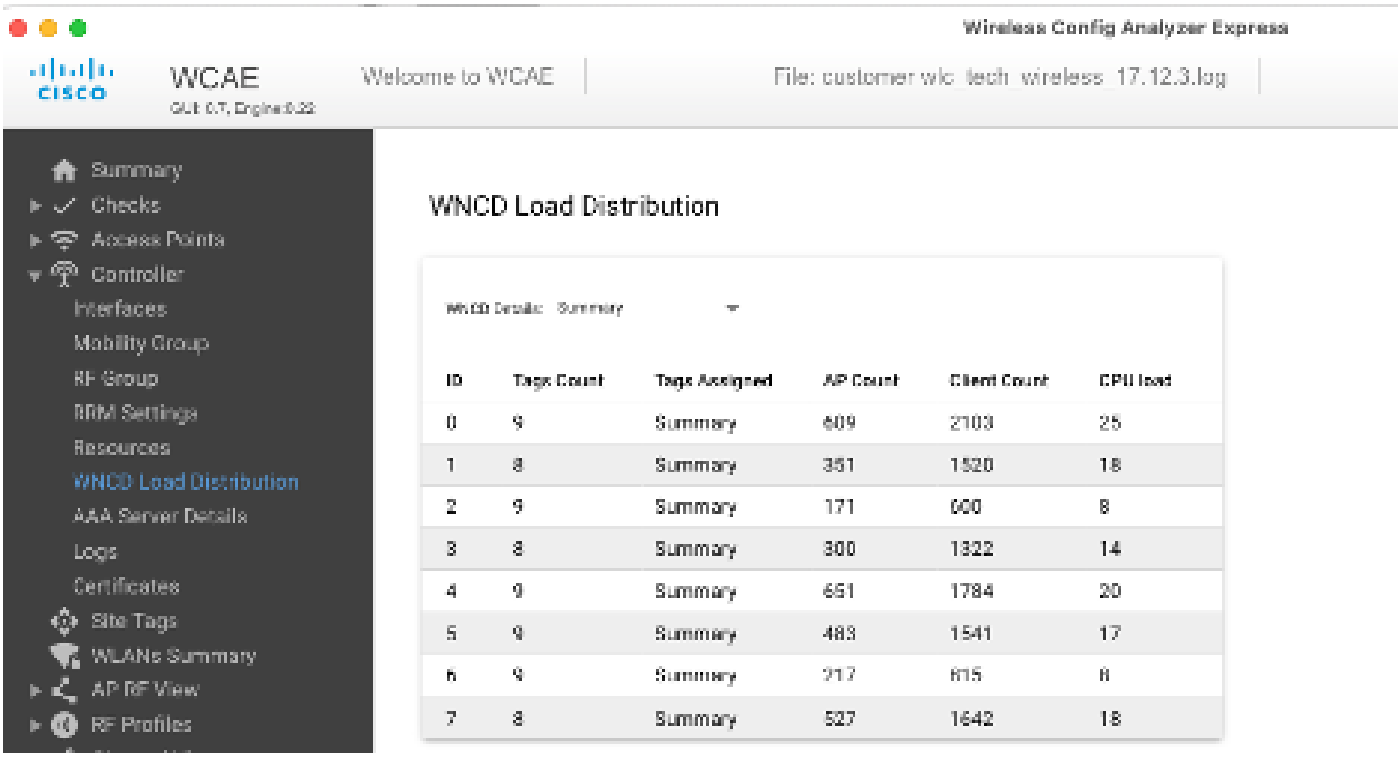
se si desidera correlare la distribuzione AP rispetto al numero di client e al carico della CPU, il modo più semplice consiste nell'utilizzare lo strumento di supporto WCAE e caricare una show tech wireless presa durante i periodi di attività. Lo strumento riepiloga il numero di client WNCD, ricavato da ciascun access point associato.

Esempio di controller correttamente bilanciato, in condizioni di basso utilizzo e numero di client:



ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
0	1	Summary	55	24	1
1	1	Summary	62	5	0
2	1	Summary	50	13	0
3	1	Summary	87	264	2
4	1	Summary	74	128	2
5	1	Summary	76	61	1
6	1	Summary	58	45	1
7	1	Summary	43	29	0

Un altro esempio, per un controller con carico maggiore, che mostra il normale utilizzo della CPU:



ID	Tags Count	Tags Assigned	AP Count	Client Count	CPU load
0	9	Summary	609	2103	25
1	8	Summary	351	1520	18
2	9	Summary	171	600	8
3	8	Summary	300	1322	14
4	9	Summary	651	1784	20
5	9	Summary	483	1541	17
6	9	Summary	217	615	8
7	8	Summary	527	1642	18

Qual è il meccanismo di bilanciamento del carico AP consigliato?

In breve, è possibile riepilogare le diverse opzioni in:

- Rete piccola, nessuna necessità di roaming veloce, meno del 40% del carico del controller: tag predefinito.
- Se è necessario il roaming veloce (OKC, FT, CCKM) o un numero elevato di client:

- Edificio singolo: creazione di un numero di tag sito pari alle CPU (dipendenti dalla piattaforma)
- Prima delle 17.12 o prima del numero di punti di accesso 500: più edifici, diramazioni o campus di grandi dimensioni: creare un tag di sito per posizione RF fisica e configurare il comando di caricamento per sito.
- 17.12 e superiore con più di 500 punti di accesso: utilizzare il bilanciamento del carico RF.

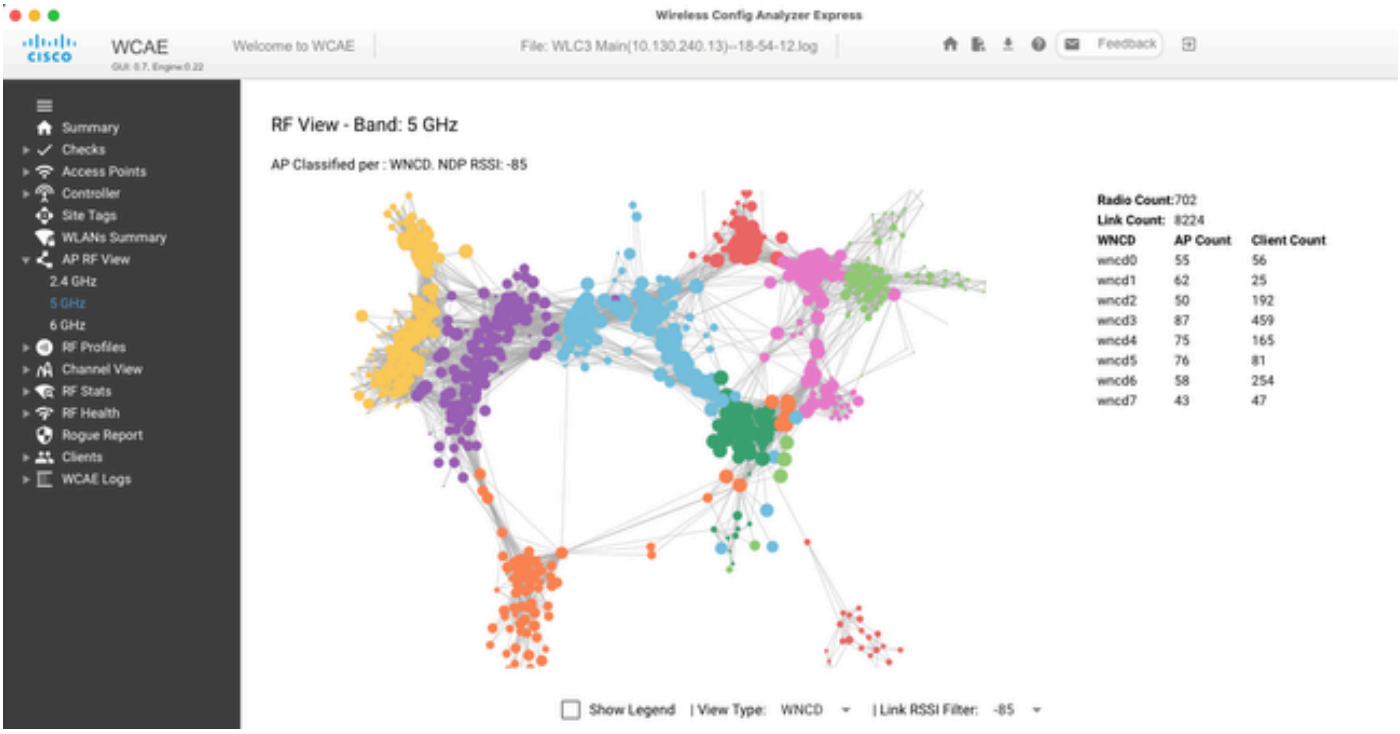
Questa soglia di 500 punti di accesso indica quando è efficace applicare il meccanismo di bilanciamento del carico, in quanto per impostazione predefinita raggruppa i punti di accesso in blocchi di 100 unità.

Visualizzazione distribuzione WNCD AP

In alcuni casi è preferibile eseguire un bilanciamento più avanzato ed è preferibile avere un controllo granulare sulla distribuzione dei punti di accesso tra le CPU, ad esempio in scenari ad alta densità in cui la metrica del carico chiave è il conteggio dei client anziché concentrarsi esclusivamente sul numero di punti di accesso presenti nel sistema.

Un buon esempio di questa situazione sono i grandi eventi: un edificio potrebbe ospitare migliaia di client, su diverse centinaia di punti di accesso, e sarebbe necessario dividere il carico su quante più CPU possibile, ma allo stesso tempo ottimizzare il roaming. Quindi, non girate attraverso WNCD a meno che non sia necessario. Si desidera evitare situazioni di tipo "sale e pepe" in cui più punti di accesso in diversi WNCD/tag di sito sono mescolati nella stessa posizione fisica.

Per ottimizzare e visualizzare la distribuzione, è possibile utilizzare lo strumento WCAE e sfruttare la funzionalità di visualizzazione RF dell'access point:



Questo ci permette di vedere la distribuzione AP/WNCD, appena impostato View Type su WNCD. In questo caso, ogni colore rappresenta un WNCD/CPU. È inoltre possibile impostare il filtro RSSI su -85 per evitare connessioni con segnale basso, anch'esse filtrate dall'algoritmo RRM nel controller.

Nell'esempio precedente, corrispondente a Cisco EMEA 24, è possibile notare che la maggior parte dei punti di accesso adiacenti sono raggruppati nello stesso WNCD, con sovrapposizione incrociata molto limitata.

I tag del sito allocati allo stesso WNCD, ottengono lo stesso colore.

Monitoraggio dell'utilizzo della CPU del Control Plane

È importante ricordare il concetto di architettura Cisco IOS-XE e tenere presente che esistono due "viste" principali dell'utilizzo della CPU. Una viene dal supporto Cisco IOS storico, e l'altra dal supporto principale, con una vista olistica della CPU su tutti i processi e core.

In generale, è possibile utilizzare il comando show processes cpu platform sorted per raccogliere informazioni dettagliate per tutti i processi in Cisco IOS-XE:

9800cl-1#show processes cpu platform sorted

CPU utilization for five seconds: 8%, one minute: 14%, five minutes: 11%
Core 0: CPU utilization for five seconds: 6%, one minute: 11%, five minutes: 5%
Core 1: CPU utilization for five seconds: 2%, one minute: 8%, five minutes: 5%
Core 2: CPU utilization for five seconds: 4%, one minute: 12%, five minutes: 12%
Core 3: CPU utilization for five seconds: 19%, one minute: 23%, five minutes: 24%

Pid	PPid	5Sec	1Min	5Min	Status	Size	Name
19953	19514	44%	44%	44%	S	190880	ucode_pkt_PPE0
28947	8857	3%	10%	4%	S	1268696	linux_iosd-imag
19503	19034	3%	3%	3%	S	247332	fman_fp_image

```
30839      2     0%     0%     0% I           0  kworker/0:0
30330  30319     0%     0%     0% S        5660  nginx
30329  30319     0%     1%     0% S       20136  nginx
30319  30224     0%     0%     0% S       12480  nginx
30263      1     0%     0%     0% S        4024  rotee
30224   8413     0%     0%     0% S        4600  pman
30106      2     0%     0%     0% I           0  kworker/u11:0
30002      2     0%     0%     0% S           0  SarIosdMond
29918  29917     0%     0%     0% S        1648  inet_gethost
```

A questo proposito, è opportuno sottolineare diversi punti chiave:

- Il processo ucode_pkt_PPE0 sta gestendo il piano dati sulle piattaforme 9800L e 9800CL, e si prevede un utilizzo elevato in ogni momento, anche superiore al 100%. Ciò fa parte dell'attuazione e non costituisce un problema.

- È importante differenziare l'utilizzo di picco rispetto a un carico sostenuto e isolare ciò che è previsto in un determinato scenario. Ad esempio, la raccolta di un output CLI molto grande, come show tech wireless può generare un picco di carico sui processi IOSd, smand e pubd, poiché viene raccolto un output di testo molto grande, con centinaia di comandi CLI eseguiti, questo non è un problema, e il carico si esaurisce dopo il completamento dell'output.

```
  Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
--------------------------------------------------------------------------------
19371   19355     62%     83%     20%  R          128120  smand
27624   27617     53%     59%     59%  S         1120656  pubd
 4192    4123     11%      5%      4%  S         1485604  linux_iosd-imag
```

- È previsto un picco di utilizzo per i core WNCD durante i periodi di attività client elevata. È possibile vedere picchi dell'80%, senza alcun impatto funzionale, e di solito non costituiscono un problema.

```
  Pid    PPid    5Sec    1Min    5Min  Status       Size  Name
--------------------------------------------------------------------------------
21094   21086     25%     25%     25%  S          978116  wncd_0
21757   21743     21%     20%     20%  R         1146384  wncd_4
22480   22465     18%     18%     18%  S         1152496  wncd_7
22015   21998     18%     17%     17%  S          840720  wncd_5
21209   21201     16%     18%     18%  S          779292  wncd_1
21528   21520     14%     15%     14%  S          926528  wncd_3
```

- È necessario analizzare un utilizzo elevato e prolungato della CPU in un processo, superiore al 90%, per più di 15 minuti.

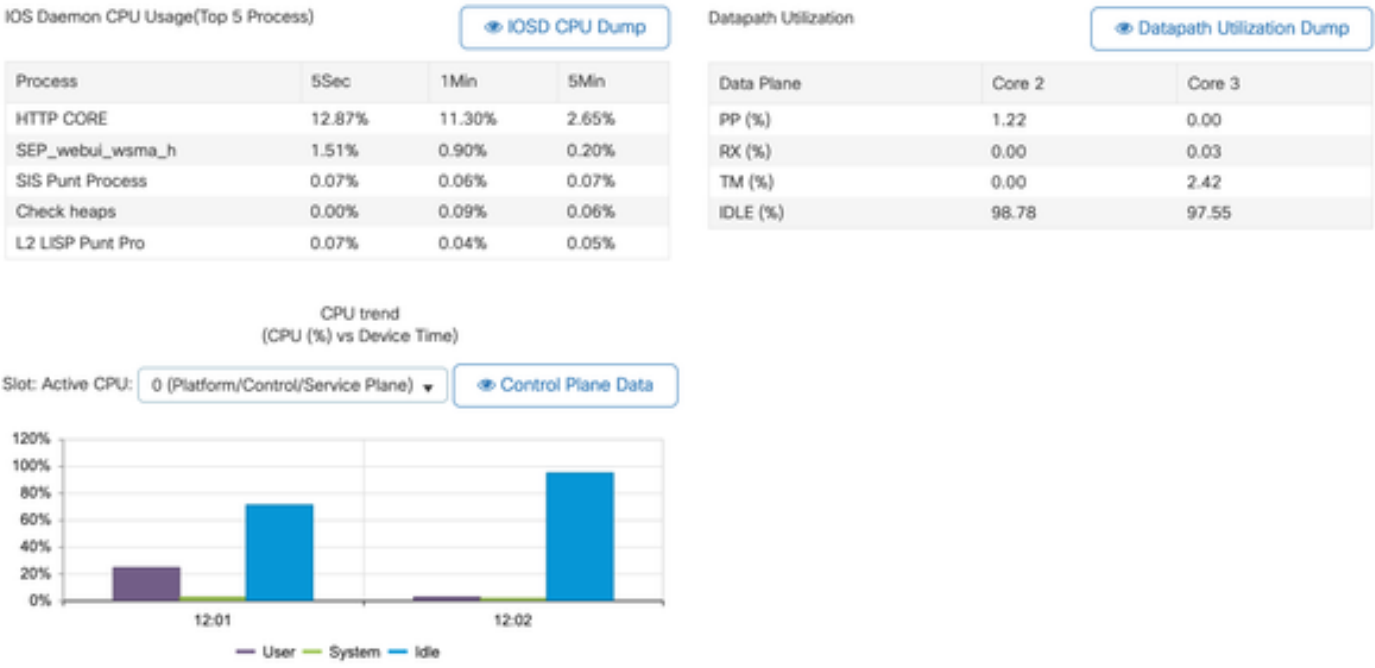
- Per monitorare l'utilizzo della CPU IOSd, usare il comando show processes cpu sorted . Questa corrisponde all'attività nella parte del processo linux_iosd-image dell'elenco Cisco IOS-XE.

9800cl-1#show processes cpu sorted

CPU utilization for five seconds: 2%/0%; one minute: 3%; five minutes: 3%

PID	Runtime(ms)	Invoked	uSecs	5Sec	1Min	5Min	TTY	Process
215	81	88	920	1.51%	0.12%	0.02%	1	SSH Process
673	164441	7262624	22	0.07%	0.00%	0.00%	0	SBC main process
137	2264141	225095413	10	0.07%	0.04%	0.05%	0	L2 LISP Punt Pro
133	534184	21515771	24	0.07%	0.04%	0.04%	0	IOSXE-RP Punt Se
474	1184139	56733445	20	0.07%	0.03%	0.00%	0	MMA DB TIMER
5	0	1	0	0.00%	0.00%	0.00%	0	CTS SGACL db cor
6	0	1	0	0.00%	0.00%	0.00%	0	Retransmission o
2	198433	726367	273	0.00%	0.00%	0.00%	0	Load Meter
7	0	1	0	0.00%	0.00%	0.00%	0	IPC ISSU Dispatc
10	3254791	586076	5553	0.00%	0.11%	0.07%	0	Check heaps
4	57	15	3800	0.00%	0.00%	0.00%	0	RF Slave Main Th
8	0	1	0	0.00%	0.00%	0.00%	0	EDDRI_MAIN

- È possibile utilizzare la GUI 9800 per una rapida visualizzazione del caricamento IOSd, dell'utilizzo per core e del carico del piano dati:



Questa opzione è disponibile nella Monitoring/System/CPU Utilization scheda.

Che cos'è ogni processo?

L'elenco esatto dei processi varia a seconda del modello di controller e della versione di Cisco IOS-XE. Questo è un elenco di alcuni dei processi chiave e non è destinato a coprire tutte le voci possibili.

Nome processo	Che cosa fa?	Valutazione
wncd_x	Gestisce la maggior parte delle operazioni wireless. A seconda del modello 9800, è possibile avere da 1 a 8 varianti	Si possono verificare picchi di utilizzo elevato durante le ore di lavoro. Segnala se l'utilizzo è bloccato al 95% o più per diversi minuti
linux_iosd-image	Processo IOS	Previsto un utilizzo elevato se si raccolgono output CLI di grandi dimensioni (show tech) Operazioni SNMP di grandi dimensioni o troppo frequenti possono causare un utilizzo elevato della CPU
ginex	server Web	Questo processo può mostrare picchi e deve essere segnalato solo con un carico elevato sostenuto
ucode_pkt_PPE0	Piano dati in 9800CL/9800L	Utilizzare il comando **show platform hardware chassis active qfp datapath utilization** per monitorare questo componente
ezman	Chipset manager per interfacce	Un alto livello di CPU indica un problema hardware o un possibile problema software del kernel. Deve essere segnalato
DB	Gestione database	In questo caso, è necessario indicare un CPU elevata
odm_X	Operation Data Manager gestisce il database consolidato tra i processi	Prevista elevata CPU nei sistemi con carico
disgustoso	Gestisce la funzionalità Rogue	In questo caso, è necessario indicare un CPU elevata

smand	Gestione shell. Si occupa dell'analisi della CLI e dell'interazione tra diversi processi	Prevista CPU elevata durante la gestione di output CLI di grandi dimensioni. È necessario indicare un elevato utilizzo della CPU in assenza di carico
emd	Gestione shell. Si occupa dell'analisi della CLI e dell'interazione tra diversi processi	Prevista CPU elevata durante la gestione di output CLI di grandi dimensioni. È necessario indicare un elevato utilizzo della CPU in assenza di carico
pubd	Parte della gestione della telemetria	CPU elevata prevista per sottoscrizioni di telemetria di grandi dimensioni. È necessario indicare un elevato utilizzo della CPU in assenza di carico

Meccanismi di protezione della CPU elevati

I controller LAN wireless Catalyst 9800 dispongono di meccanismi di protezione estesi per l'attività dei client wireless o di rete, per impedire l'utilizzo di una CPU elevata a causa di scenari accidentali o intenzionali. Sono disponibili diverse funzionalità chiave progettate per consentire di contenere i dispositivi che presentano problemi:

Esclusione client

Questa opzione è attivata per impostazione predefinita e fa parte dei criteri di protezione wireless e può essere attivata o disattivata per profilo criteri. In questo modo è possibile rilevare diversi problemi di comportamento, rimuovere il client dalla rete e impostarlo in un "elenco di esclusione temporaneo". Mentre il client si trova in questo stato escluso, gli access point non comunicano con loro, impedendo ulteriori azioni.

Trascorso il timer di esclusione (60 secondi per impostazione predefinita), il client può eseguire nuovamente l'associazione.

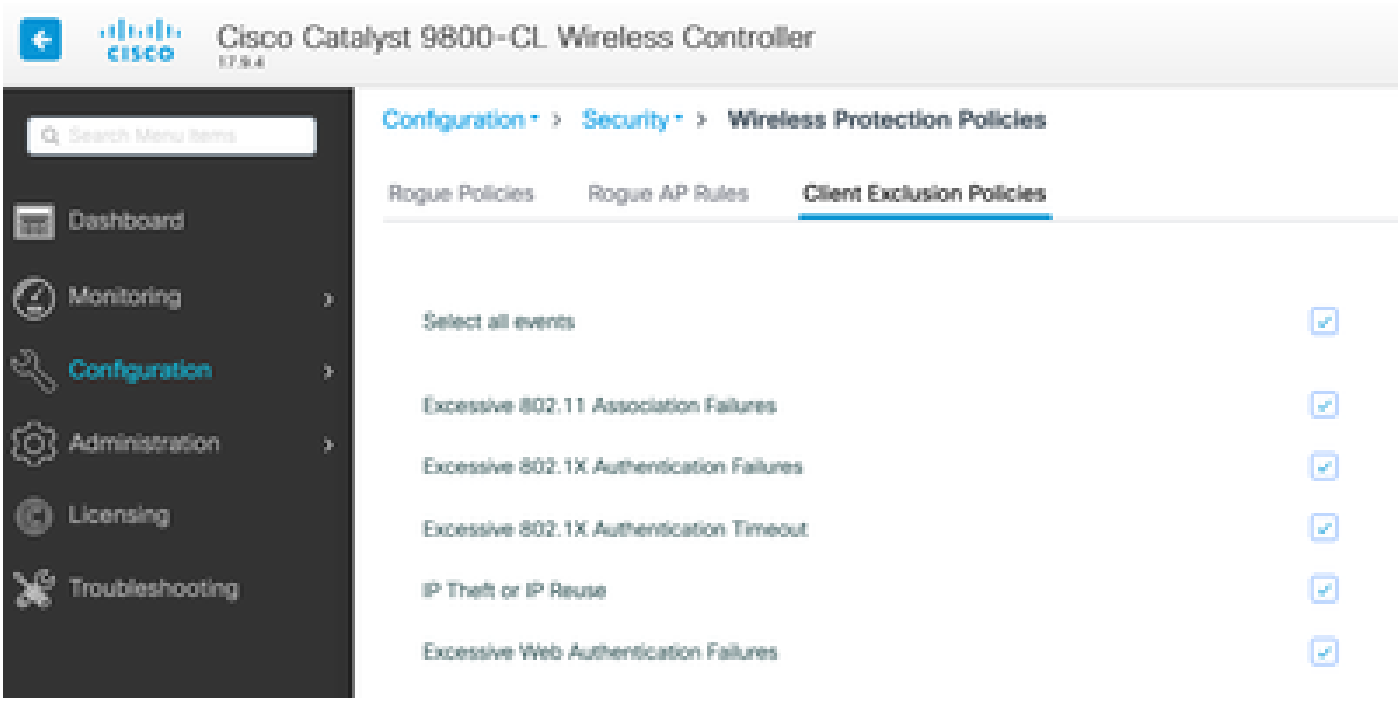
Sono disponibili diversi trigger per l'esclusione dei client:

- Ripetuti errori di associazione
- 3 o più errori di autenticazione webauth, PSK o 802.1x
- Timeout di autenticazione ripetuti (nessuna risposta dal client)
- Tentativo di riutilizzare un indirizzo IP già registrato in un altro client
- Generazione di un flusso ARP

L'esclusione dei client protegge il controller, il punto di accesso e l'infrastruttura AAA (Radius) da diversi tipi di attività elevate che potrebbero portare a un utilizzo elevato della CPU. In generale, non è consigliabile disattivare i metodi di esclusione, a meno che non siano necessari per un esercizio di risoluzione dei problemi o per un requisito di compatibilità.

Le impostazioni predefinite funzionano per quasi tutti i casi, e solo in alcuni scenari eccezionali, è necessario per aumentare il tempo di esclusione o disabilitare alcuni trigger specifici. Ad esempio, alcuni client legacy o specializzati (IOT/medici) potrebbero avere la necessità di disattivare il trigger di errore dell'associazione, a causa di difetti del client che non possono essere facilmente corretti

È possibile personalizzare i trigger nell'interfaccia utente: Configurazione/Protezione wireless/Criteri di esclusione client:



Il trigger di esclusione ARP è stato progettato per essere abilitato in modo permanente a livello globale, ma può essere personalizzato in ogni profilo dei criteri. Per controllare lo stato, usare il comando sh wireless profile policy all search for this specific output:

```
ARP Activity Limit
  Exclusion                : ENABLED
  PPS                      : 100
  Burst Interval           : 5
```

Control Plane Protection dal traffico dati

Si tratta di un meccanismo avanzato nel Data Plane per garantire che il traffico inviato al Control Plane non superi una serie predefinita di soglie. La funzione si chiama "Punt Policers" (Policer punt) e in quasi tutti gli scenari, non è necessario toccarli, e anche in questo caso, l'operazione deve essere eseguita solo durante la collaborazione con il supporto Cisco.

Il vantaggio di questa protezione è che fornisce una visione molto dettagliata di ciò che accade nella rete e se c'è una specifica attività che sta avendo una frequenza aumentata, o pacchetti inaspettatamente alti al secondo.

Questo problema viene riscontrato solo dalla CLI, in quanto normalmente fanno parte di funzionalità avanzate che raramente è necessario

modificare.

Per una visualizzazione di tutte le regole di punt:

9800-l#show platform software punt-policer

Per Punt-Cause Policer Configuration and Packet Counters

Punt		Config Rate(pps)		Conform Packets		Dropped Packets		Config Burst(pkts)		Config Alert	
Cause	Description	Normal	High	Normal	High	Normal	High	Normal	High	Normal	High
2	IPv4 Options	874	655	0	0	0	0	874	655	Off	Off
3	Layer2 control and legacy	8738	2185	33	0	0	0	8738	2185	Off	Off
4	PPP Control	437	1000	0	0	0	0	437	1000	Off	Off
5	CLNS IS-IS Control	8738	2185	0	0	0	0	8738	2185	Off	Off
6	HDLC keepalives	437	1000	0	0	0	0	437	1000	Off	Off
7	ARP request or response	437	1000	0	330176	0	0	437	1000	Off	Off
8	Reverse ARP request or repso	437	1000	0	24	0	0	437	1000	Off	Off
9	Frame-relay LMI Control	437	1000	0	0	0	0	437	1000	Off	Off
10	Incomplete adjacency	437	1000	0	0	0	0	437	1000	Off	Off
11	For-us data	40000	5000	442919246	203771	0	0	40000	5000	Off	Off
12	Mcast Directly Connected Sou	437	1000	0	0	0	0	437	1000	Off	Off

Potrebbe trattarsi di un elenco di grandi dimensioni, con più di 160 voci, a seconda della versione del software.

Nell'output della tabella, controllare la colonna dei pacchetti ignorati insieme a tutte le voci che hanno un valore diverso da zero nel conteggio massimo dei pacchetti.

Per semplificare la raccolta dei dati, è possibile utilizzare il comando show platform software punt-policer drop-only , per filtrare solo le voci del policer con rilasci.

Questa funzione può essere utile per identificare se ci sono tempeste ARP o allagamenti sonda 802.11 (usano la coda "802.11 Pacchetti a sinistra". LFTS è l'acronimo di Linux Forwarding Transport Service.

Controllo dell'ingresso delle chiamate wireless

In tutte le release di manutenzione recenti, il controller dispone di un monitor di attività che consente di reagire in modo dinamico a un'elevata CPU e di garantire che i tunnel AP CAPWAP rimangano attivi, a fronte di una pressione insostenibile.

La funzionalità controlla il carico WNCD e inizia a limitare l'attività del nuovo client, per garantire che rimangano risorse sufficienti per gestire le connessioni esistenti e proteggere la stabilità di CAPWAP.

Questa opzione è abilitata per impostazione predefinita e non dispone di opzioni di configurazione.

Sono definiti tre livelli di protezione, L1 con carico dell'80%, L2 con carico dell'85% e L3 con carico dell'89%, ognuno dei quali attiva una perdita di protocollo in ingresso diversa come meccanismo di protezione. La protezione viene rimossa automaticamente non appena il carico diminuisce.

In una rete integra, gli eventi di caricamento L2 o L3 non dovrebbero essere visualizzati e, se si verificano di frequente, è necessario esaminarli.

Per il monitoraggio, usare il comando wireless stats cac come mostrato nell'immagine.

```
9800-l#  show wireless stats cac

WIRESLESS CAC STATISTICS
---------------------------------------------
L1 CPU Threshold: 80        L2 CPU Threshold: 85        L3 CPU Threshold: 89
Total Number of CAC throttle due to IP Learn:  0
Total Number of CAC throttle due to AAA:       0
Total Number of CAC throttle due to Mobility Discovery:  0
Total Number of CAC throttle due to IPC:       0
CPU Throttle Stats
    L1-Assoc-Drop:    0         L2-Assoc-Drop:    0         L3-Assoc-Drop: 0
    L1-Reassoc-Drop:  0         L2-Reassoc-Drop:  0         L3-Reassoc-Drop: 0
    L1-Probe-Drop:    12231     L2-Probe-Drop:    11608     L3-Probe-Drop: 93240
    L1-RFID-Drop:     0         L2-RFID-Drop:     0         L3-RFID-Drop: 0
    L1-MDNS-Drop:     0         L2-MDNS-Drop:     0         L3-MDNS-Drop: 0
```

Protezione mDNS

mDNS come protocollo consente un approccio "zero-touch" per l'individuazione dei servizi tra i dispositivi, ma allo stesso tempo può essere molto attivo e, se non è configurato correttamente, può comportare un carico di unità significativo.

mDNS, senza alcun filtro, può facilmente aumentare l'utilizzo della CPU WNCD, a causa di diversi fattori:

- criteri mDNS con apprendimento illimitato, il controller otterrà tutti i servizi offerti da tutti i dispositivi. Questo può portare a elenchi di servizi molto grandi, con centinaia di voci.
- Criteri impostati senza filtro: il controller eseguirà il push di tali elenchi di servizi di grandi dimensioni a ogni client che richiede chi fornisce un determinato servizio.
- Alcuni servizi specifici di mDNS vengono forniti da "tutti" i client wireless, con conseguente aumento del numero di servizi e dell'attività, con variazioni in base alla versione del sistema operativo.

È possibile controllare le dimensioni dell'elenco mDNS per servizio con questo comando:

```
9800-l#  show mdns-sd service statistics
Service Name                                  Service Count
------------------------------------------------------------------------------
_ipp._tcp.local                               84
_ipps._tcp.local                              52
_raop._tcp.local                              950
_airplay._tcp.local                           988
_printer._tcp.local                           13
_googlerpc._tcp.local                         12
_googlecast._tcp.local                        70
_googlezone._tcp.local                        37
_home-sharing._tcp.local                      7
```

Questo può fornire un'idea di quanto grande può ottenere qualsiasi query, non denota un problema di per sé, solo un modo per monitorare ciò che viene tracciato.

Di seguito sono riportati alcuni importanti suggerimenti per la configurazione di mDNS:

- Impostare il trasporto mDNS su un singolo protocollo:

```
9800-1(config)# mdns-sd gateway
9800-1(config-mdns-sd)# transport ipv4
```

Per impostazione predefinita, viene utilizzato il trasporto IPv4. Per ottenere prestazioni ottimali, è consigliabile utilizzare IPv6 o IPv4, ma non entrambi:

- Impostare sempre un filtro di percorso nei criteri del servizio mDNS per evitare query/risposte non associate. In generale, si consiglia di utilizzare "site-tag", ma altre opzioni potrebbero funzionare, a seconda delle esigenze.

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).