Risoluzione dei problemi di gestione e postura delle sessioni ISE

Sommario

Introduzione

Questo documento descrive il problema comune relativo ai servizi di postura di Identity Service Engine (ISE): **"Il modulo di postura AnyConnect ISE è conforme..."**

Premesse

Questo documento descrive il problema comune relativo ai servizi di postura di Identity Service Engine (ISE) - **Il modulo di postura AnyConnect ISE è conforme quando lo stato della sessione è in sospeso.**

Anche se i sintomi sono sempre gli stessi, potrebbero esserci più cause principali di questo problema.

Spesso, la risoluzione di un problema di questo tipo richiede molto tempo, con un conseguente impatto grave.

Questo documento spiega:

- Manifestazione del problema dal punto di vista dell'utente finale e dell'amministratore ISE.
- Scenari problematici comuni.
- La teoria alla base di ISE, AnyConnect e le operazioni di rete che causano il problema.
- Algoritmi di identificazione rapida dei problemi.
- Soluzioni classiche a scenari problematici comuni.
- Condivisione dello stato della postura sulla directory della sessione Radius.

Per una migliore spiegazione dei concetti descritti più avanti, fare riferimento a:

Confronto tra gli stili di postura ISE per le applicazioni pre e post 2.2

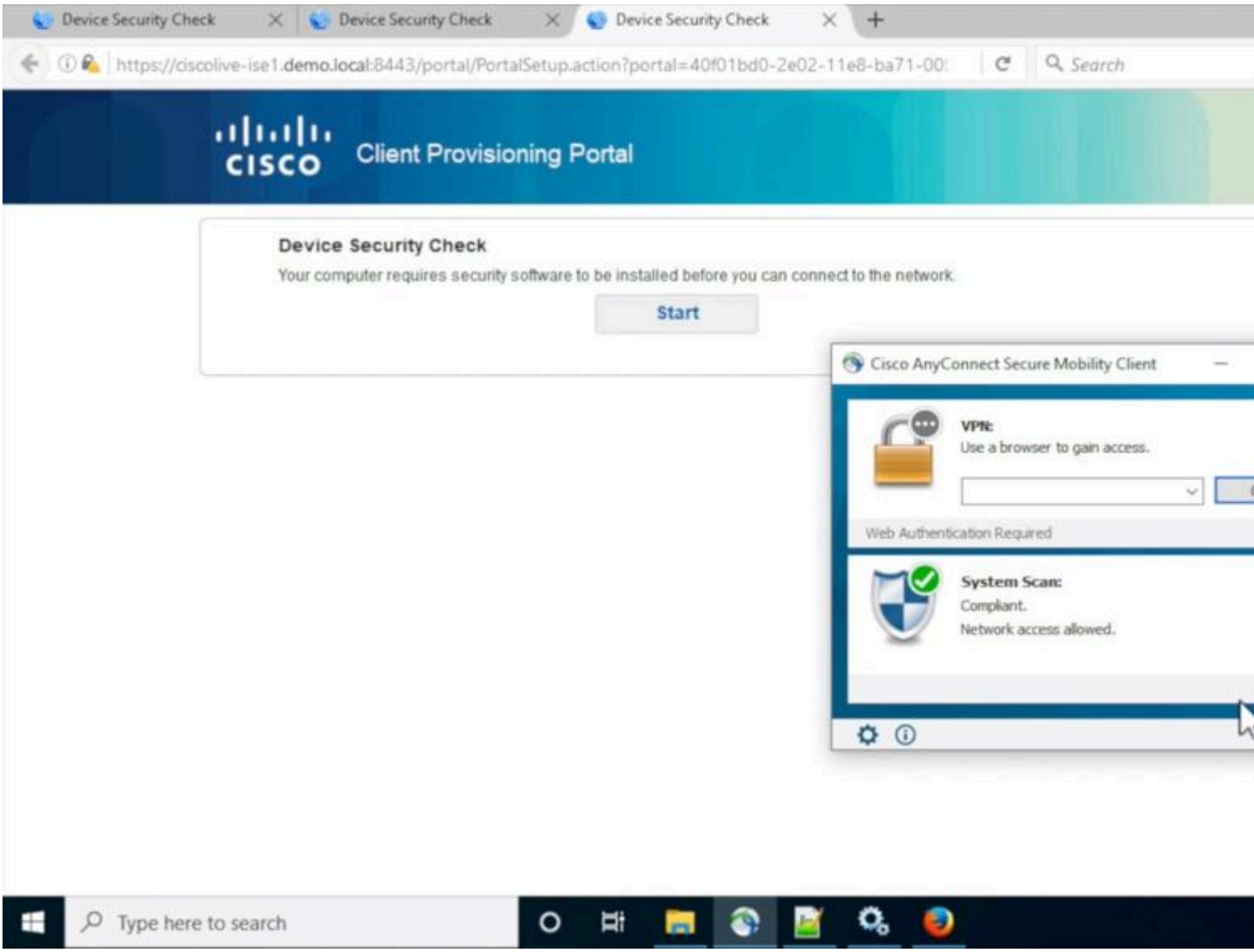
ISE, sotto la lente di ingrandimento. Come risolvere i problemi relativi ad ISE - BRKSEC-3229

Problema

Esperienza utente finale

Questo problema si verifica in genere in assenza di accesso alla rete o di reindirizzamenti costanti al portale di provisioning dei client ISE nel browser, mentre, allo stesso tempo, il modulo di postura AnyConnect ISE mostra lo stato della postura come **Conforme.**

Esperienza tipica dell'utente finale:

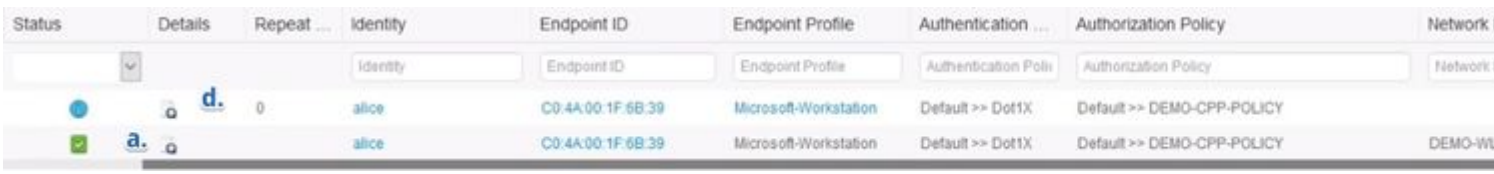


Esperienza di amministrazione ISE

Normalmente, nella fase iniziale di valutazione del problema, l'amministratore ISE esegue un'indagine dei log Radius Live per verificare che ci sia un'autenticazione effettiva per accedere all'ISE.

Il primo sintomo rilevato in questa fase indica una mancata corrispondenza in uno stato di postura tra l'endpoint e ISE, come nei log attivi o nei report di autenticazione Radius l'ultima autenticazione riuscita per l'endpoint mostra lo stato di postura **in sospeso**.

Tipica esperienza di amministrazione ISE:



- Ultima autenticazione riuscita per Alice.
- Lo stato di postura della sessione è **In sospeso.**
- Ultimo evento sessione per Alice.
- L'evento della sessione mostra lo stato della postura come **Conforme.**

Nota: c. e d. non sono sempre presenti nei log attivi quando descritto nei manifesti del problema. L'evento di sessione con stato di postura **Conforme** è più comune negli scenari causati da sessioni obsolete o fantasma descritte più avanti in questo documento.

Scenari problematici comuni

Questo problema si manifesta in genere in due scenari problematici e ognuno di essi ha più cause principali. Gli scenari:

- Il modulo di postura AnyConnect ISE è stato informato in modo errato dal PSN (Policy Service Node) durante il processo di postura che ha causato la visualizzazione di uno stato di postura errato. In questo caso, in genere viene utilizzata una sessione obsoleta o fantasma nella cache della sessione PSN.
- AnyConnect ISE mostra lo stato della postura dal ciclo di rilevamento precedente perché l'autenticazione corrente non ha attivato un processo di rilevamento. Il modulo di postura ISE in AnyConnect ha un numero limitato di eventi che attivano il processo di rilevamento e probabilmente si verificano quando, durante l'autenticazione o la riautenticazione, non è stato rilevato nessuno di questi eventi.

Problema di sessione non aggiornata/fantasma

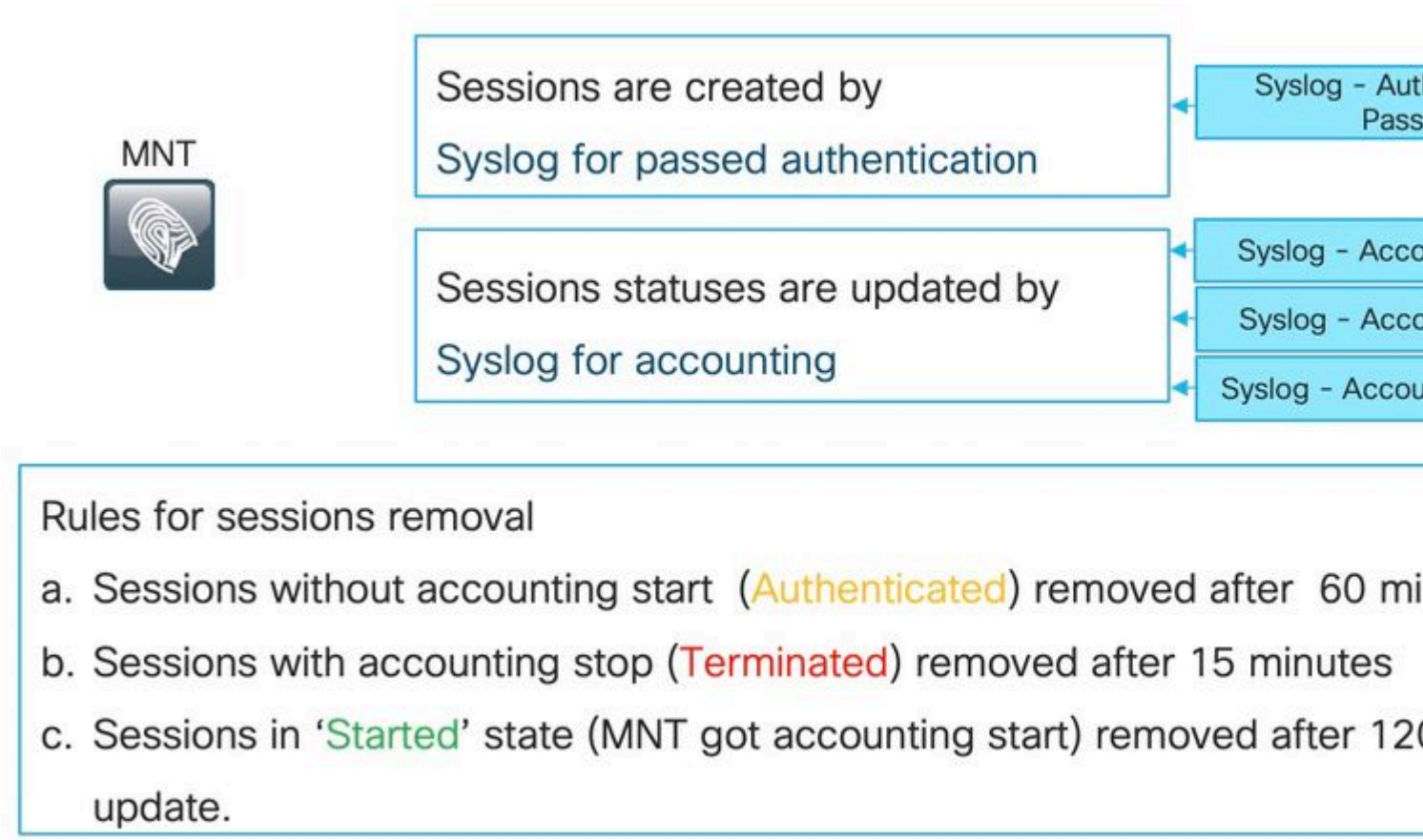
Per comprendere meglio il problema, esaminare la logica di gestione delle sessioni ISE e il processo di rilevamento di AnyConnect richiesto.

Logica di gestione delle sessioni ISE

Nell'implementazione ISE, ci sono due persone responsabili del processo di gestione della sessione: PSN e MNT (Monitoring Node).

Per risolvere e identificare correttamente questo problema, è fondamentale comprendere la teoria della gestione delle sessioni su entrambe le persone.

Gestione di MNT e sessioni



Come spiegato in questa immagine, il nodo MNT crea stagioni basate sui messaggi Syslog di autenticazione passati provenienti dai PSN.

Lo stato della sessione successiva può essere aggiornato dal syslog per l'accounting.

La rimozione della sessione su MNT si verifica in 3 scenari:

- Le sessioni senza accounting sono state rimosse circa 60 minuti dopo la creazione. È presente un job cron eseguito ogni 5 minuti per verificare gli stati delle sessioni e pulirle.
- La sessione terminata è stata rimossa circa 15 minuti dopo che l'interruzione dell'accounting è stata elaborata dallo stesso processo cron.
- Lo stesso cron su ogni esecuzione rimuove anche le sessioni che sono state in stato 'Avviato' per più di 5 giorni (120 ore). Uno stato avviato indica che il nodo MNT ha elaborato sia l'autenticazione che l'accounting per avviare Syslog per la sessione.

Esempi di messaggi Syslog da PSN. Questi messaggi vengono registrati in port-server.log quando il componente runtime-aaa è abilitato in DEBUG. Le parti in grassetto possono essere utilizzate per creare espressioni regolari di ricerca.

Autenticazione superata:

<#root>

AcsLogs

,

2020-04-07 10:07:29,202

,DEBUG,0x7fa0ada91700,cntx=0000629480,sesn=skuchere-ise26-1/375283310/10872,CPMSessionID=0A3E946C000000

5200 NOTICE Passed-Authentication: Authentication succeeded

, ConfigVersionId=87, Device IP Address=10.62.148.108, DestinationIPAddress=192.168.43.26, DestinationPo

bob@example.com

, NAS-IP-Address=10.62.148.108, NAS-Port=50105, Service-Type=Framed, Framed-IP-Address=192.168.255.205,

0A3E946C00000073559C0123

\;42SessionID=skuchere-ise26-1/375283310/10872\;, Calling-Station-ID=

00-50-56-B6-0B-C6

, NAS-Port-Type=Ethernet, NAS-Port-Id=GigabitEthernet1/0/5, EAP-Key-Name=, cisco-av-pair=service-type=Fr

Inizio accounting:

<#root>

AcsLogs

,

2020-04-07 10:07:30,202

,DEBUG,0x7fa0ad68d700,cntx=0000561096,sesn=skuchere-ise26-1/375283310/10211,CPMSessionID=0A3E946C000000

3000 NOTICE Radius-Accounting: RADIUS Accounting start request

, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=7, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.108

0A3E946C00000073559C0123

:skuchere-ise26-1/375283310/10210, Called-Station-ID=00-E1-6D-D1-4F-05, Calling-Station-ID=

00-50-56-B6-0B-C6

, Acct-Status-Type=Start, Acct-Delay-Time=0, Acct-Session-Id=00000041, Acct-Authentic=Remote, Event-Time

Aggiornamento contabile provvisorio:

<#root>

AcsLogs,2020-04-07 22:57:48,642,

DEBUG,0x7fa0adb92700,cntx=0000629843,sesn=skuchere-ise26-1/375283310/10877,CPMSessionID=0A3E946C0000007

3002 NOTICE Radius-Accounting: RADIUS Accounting watchdog update

, ConfigVersionId=87, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=8, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.108

00-50-56-B6-0B-C6

, Acct-Status-Type=Interim-Update, Acct-Delay-Time=0, Acct-Input-Octets=2293926, Acct-Output-Octets=0, A

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/10877, SelectedAccessService=Defau

Arresto accounting:

<#root>

AcsLogs,2020-04-08 11:43:22,356

,DEBUG,0x7fa0ad68d700,cntx=0000696242,sesn=skuchere-ise26-1/375283310/11515,CPMSessionID=0A3E946C000000

3001 NOTICE Radius-Accounting: RADIUS Accounting stop request

, ConfigVersionId=88, Device IP Address=10.62.148.108, UserName=

bob@example.com

, RequestLatency=12, NetworkDeviceName=3850-1-BB, User-Name=bob@example.com, NAS-IP-Address=10.62.148.10

00-50-56-B6-0B-C6

, Acct-Status-Type=Stop, Acct-Delay-Time=0, Acct-Input-Octets=4147916, Acct-Output-Octets=0, Acct-Sessio

0A3E946C00000073559C0123

, cisco-av-pair=method=dot1x, AcsSessionID=skuchere-ise26-1/375283310/11515, SelectedAccessService=Defau

Gestione di PSN e sessioni

Che cos'è la cache della sessione PSN?

Database in memoria in cui vengono archiviate tutte le sessioni attive di un PSN specifico. La cache di sessione è sempre locale rispetto al nodo e non esiste alcun meccanismo in ISE in grado di eseguire la replica dello stato di sessione FULL da un nodo all'altro.

Per ogni ID sessione attivo, PSN memorizza tutti gli attributi raccolti durante la fase di autenticazione/autorizzazione, ad esempio gruppi di utenti interni/esterni, attributi del dispositivo di accesso alla rete, attributi del certificato e così via. Tali attributi vengono utilizzati dal PSN per selezionare diversi tipi di criteri, ad esempio autenticazione, autorizzazione, provisioning client e postura.

La cache della sessione viene completamente rimossa quando i servizi nel nodo o nel nodo stesso vengono riavviati.

La logica di elaborazione della sessione corrente crea una nuova voce nella cache della sessione in due scenari. I dettagli successivi delle sessioni esistenti possono essere aggiornati dai messaggi di accounting provenienti da NAD:

- La sessione è stata autenticata correttamente nel PSN.
- PSN ha ottenuto un aggiornamento temporaneo di accounting per la sessione che non esiste nella cache della sessione.

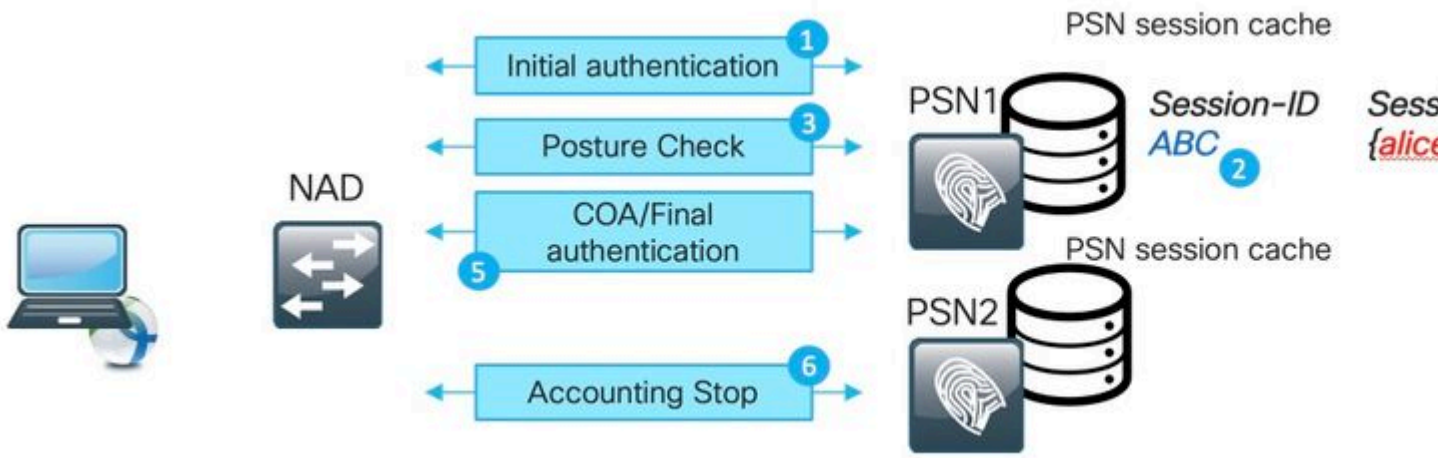
Per quanto riguarda la rimozione delle sessioni, PSN implementa la logica seguente:

- Voce della cache della sessione rimossa immediatamente dopo l'elaborazione del messaggio di arresto dell'accounting.
- Il PSN inizia a rimuovere le sessioni utilizzate meno di recente quando un nodo raggiunge **il limite** delle sessioni attive.

Sessione non aggiornata su PSN

Nella distribuzione ISE, l'arresto dell'accounting per una sessione esistente è stato elaborato dal PSN che non ha eseguito l'autenticazione effettiva:

Esempio di sessione non aggiornata:



1. L'autenticazione viene eseguita correttamente sul PSN per la sessione ABC.

2. PSN crea una voce nella cache della sessione.

3. La valutazione della postura avviene.

4. Sessione contrassegnata come **conforme**.

5. La modifica dell'autorizzazione (COA) attivata dalla modifica dello stato della postura comporta la riautenticazione dell'endpoint per applicare il livello di accesso successivo.

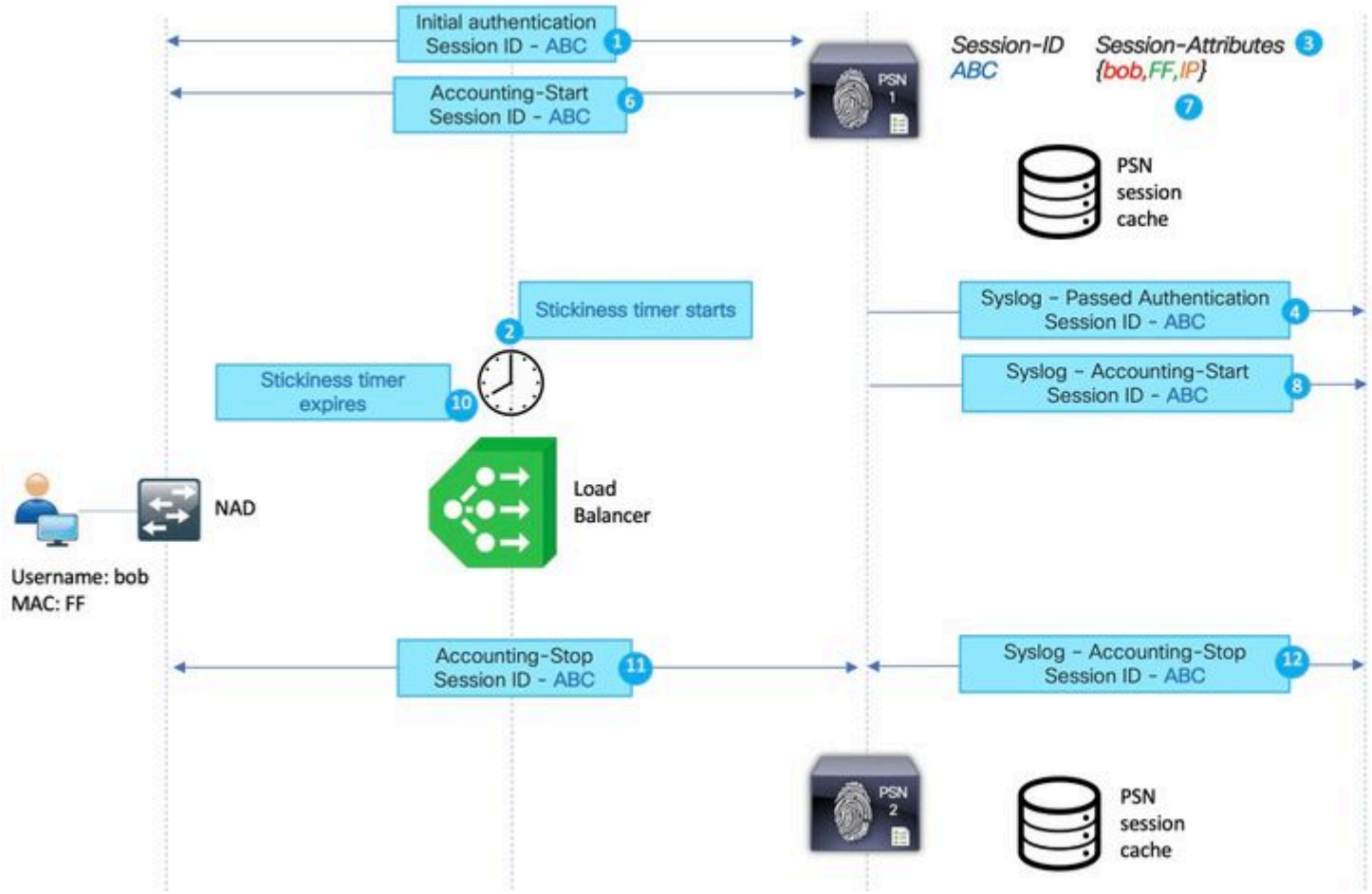
6. L'interruzione dell'accounting per la sessione ABC passa a PSN2.

Dopo la sessione del passaggio 6, l'ABC rimane bloccato nello stato non aggiornato su PSN1 poiché non verrebbe elaborato un messaggio di interruzione dell'accounting su questo PSN per rimuoverlo. La sessione viene rimossa per un periodo di tempo prolungato se nella distribuzione non viene eseguito un numero elevato di tentativi di autenticazione.

La sessione non aggiornata viene visualizzata nella cache della sessione PSN nei seguenti scenari:

- L'arresto dell'accounting è arrivato al PSN errato a causa della scadenza del timer di persistenza nel servizio di bilanciamento del carico.
- La configurazione errata in NAD non è la stessa PSN configurata per l'autenticazione e l'accounting.
- Problemi di connettività temporanei nel percorso di rete che causano il failover di NAD al PSN successivo.

Esempio di sessione non aggiornata nell'ambiente di bilanciamento del carico:



1. Autenticazione iniziale per la sessione ABC eseguita da PSN 1.

2. Questa autenticazione avvia un timer di persistenza sul load balancer.

3. Il PSN 1 crea una voce per la sessione ABC nella cache locale.

4. Messaggio syslog per l'autenticazione passata trasferita al nodo MNT.

5. Voce per la sessione ABC creata nella directory di sessione MNT con lo stato **Autenticato**.

6. Messaggio di avvio della contabilità per la sessione ABC termina su PSN 1.

7. Voce della cache della sessione per la sessione ABC aggiornata con informazioni da Accounting-Start.

8. Messaggio Syslog per Accounting-Start trasferito al nodo MNT.

9. Stato della sessione aggiornato su **Avviato**.

10. Il timer di persistenza scade sul load balancer.

11. Accounting-Stop per la sessione ABC inoltrata dal servizio di bilanciamento del carico a PSN 2.

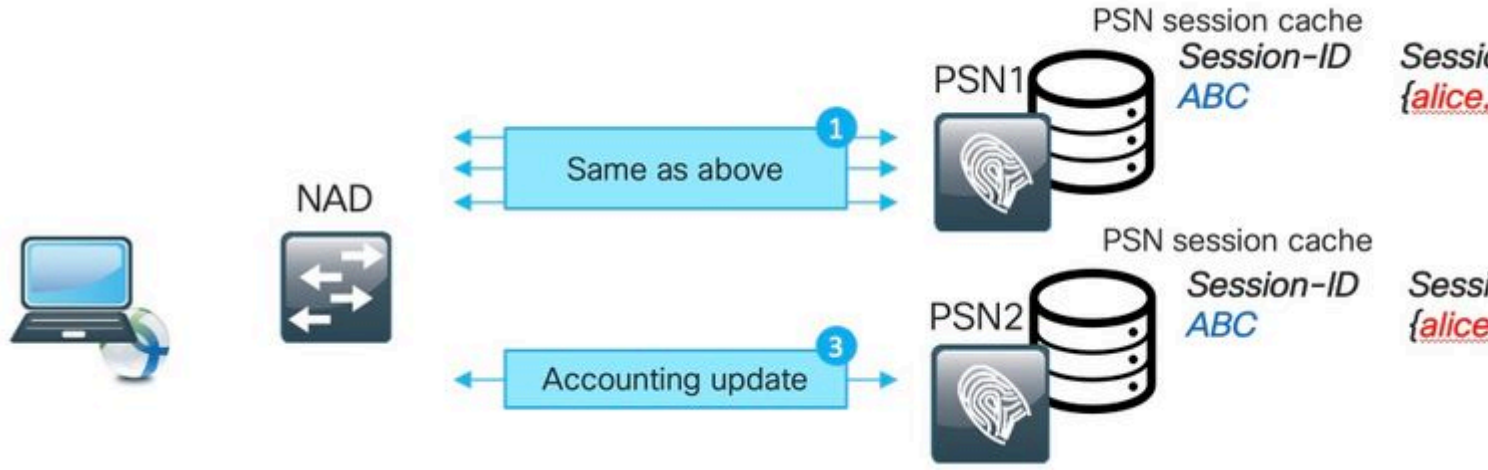
12. Messaggio syslog per Accounting-Stop inoltrato da PSN 2 a MNT.

13. Sessione ABC contrassegnata come terminata il MNT.

Sessione fantasma nel PSN

La sessione fantasma è uno scenario in cui l'aggiornamento intermedio di accounting arriva al PSN che non ha eseguito l'autenticazione per questa sessione specifica. In questo scenario viene creata una nuova voce nella cache della sessione PSN e se il PSN non riceve un messaggio di interruzione dell'accounting per questa sessione, la voce non verrà rimossa a meno che il PSN non raggiunga il limite di sessioni attive.

Esempio della sessione fantasma:



1. La stessa procedura descritta nell'esempio di sessione non aggiornata viene eseguita su PSN1 per la sessione ABC.

2. Lo stato della sessione ABC è **Conforme** nella cache di sessione PSN1.

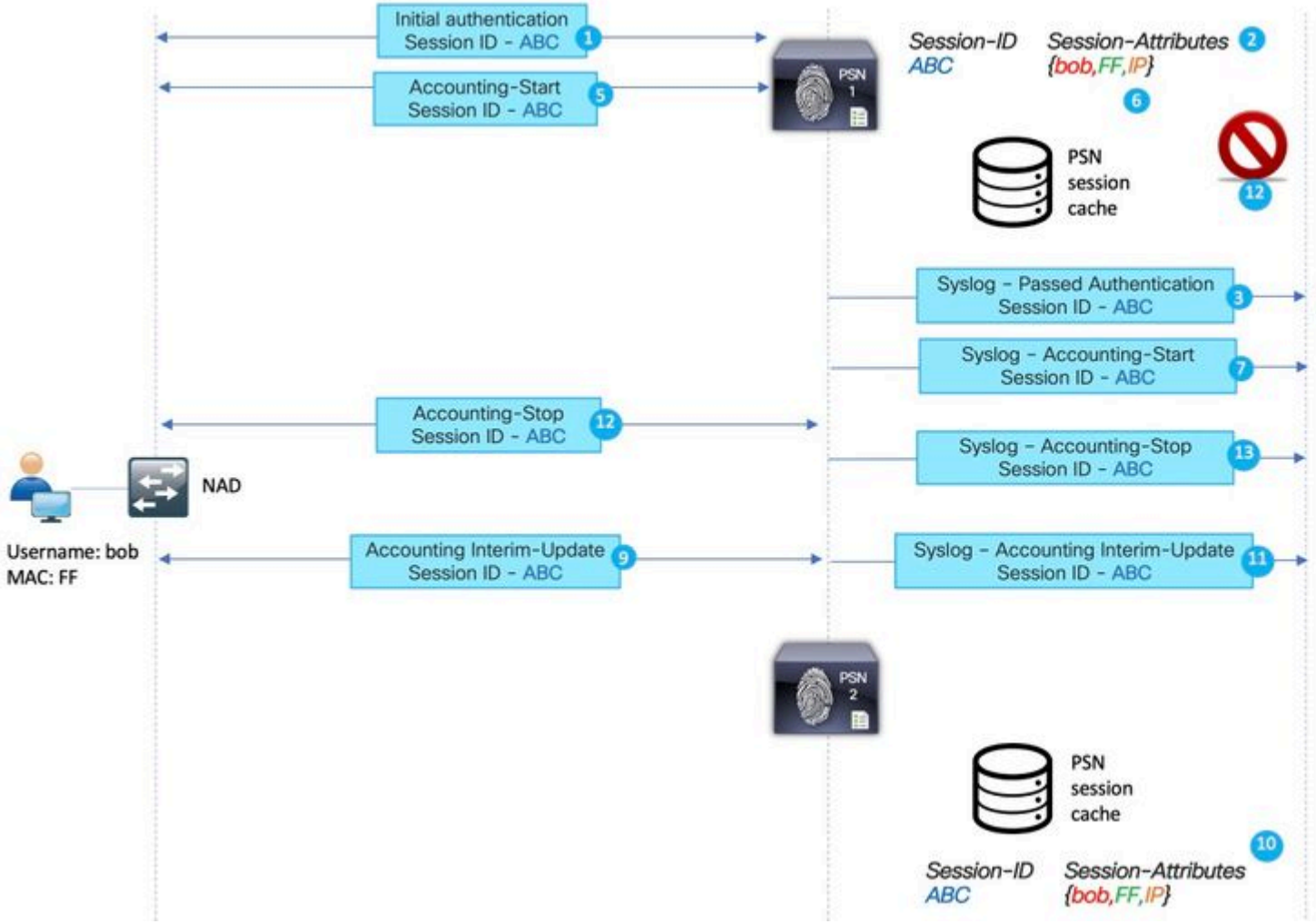
3. Aggiornamento temporaneo della contabilità per la sessione ABC ha riscontrato PSN2.

4. Voce di sessione ABC creata su PSN2. Poiché la voce della sessione è stata creata dal messaggio di accounting, dispone di un numero limitato di attributi. Ad esempio, lo stato della postura non è disponibile per la sessione ABC. Mancano anche elementi quali i gruppi di utenti e altri attributi specifici delle autorizzazioni.

La sessione fantasma viene visualizzata nella cache della sessione PSN nei seguenti scenari:

- Interruzione a breve termine del transito di rete.
- Errore di funzionamento del dispositivo di accesso alla rete.
- Configurazione errata o errata nel servizio di bilanciamento del carico.

Esempio di sessione fantasma per lo scenario con problemi temporanei nel percorso di rete verso PSN1:



1. Autenticazione iniziale per la sessione ABC eseguita da PSN.

2. PSN1 crea una voce per la sessione ABC nella cache locale.

3. Messaggio syslog per autenticazione passata trasferita al nodo MNT.

4. Voce per la sessione ABC creata nel database TimesTen con lo stato **Authenticated**.

5. Il messaggio di avvio della contabilità per la sessione ABC termina su PSN 1.

6. Voce della cache della sessione per la sessione ABC aggiornata con informazioni da Accounting-Start.

7. Messaggio Syslog per Accounting-Start trasferito al nodo MNT.

8. Stato della sessione aggiornato su **Avviato**.

9. Aggiornamento della contabilità provvisoria per la sessione ABC inoltrato a PSN2.

10. PSN2 crea una voce per la sessione ABC nella cache locale.

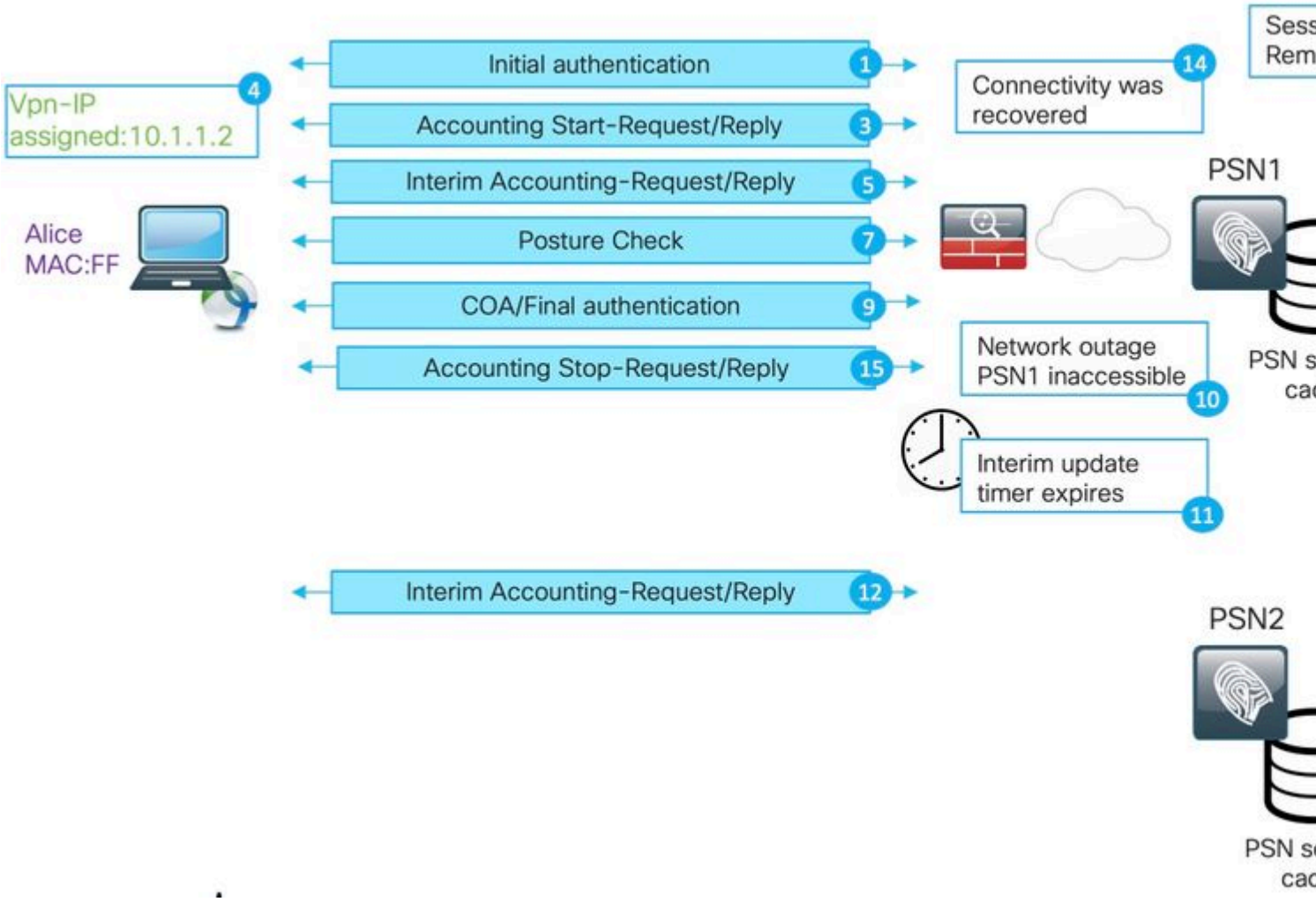
11. Accounting-Stop per la sessione ABC inoltrato a PSN1.

12. Voce per la sessione ABC rimossa dalla cache delle sessioni su PSN1.

13. Messaggio syslog per Accounting-Stop inoltrato da PSN 1 a MNT.

14. Sessione ABC contrassegnata come terminata il MNT.

Scenario della sessione fantasma creato per la connessione VPN di lunga durata:



1. Autenticazione iniziale su PSN1.

2. Sessione ABC creata nella cache della sessione.

3. L'accounting avvia il messaggio elaborato dal PSN.

4. Il nuovo indirizzo IP assegnato alla scheda di rete VPN (Virtual Private Network).

5. L'aggiornamento dell'accounting provvisorio con informazioni sull'indirizzo IP viene eseguito sul PSN.

6. Informazioni sull'indirizzo IP aggiunte alla cache della sessione.

7. La valutazione della postura viene eseguita con PSN1.

8. Stato postura aggiornato nella sessione.

9. Il push COA eseguito da ISE attiva l'assegnazione di un nuovo livello di accesso.

10. Interruzione sul percorso di rete che rende PSN1 inaccessibile.

11. Dopo la scadenza dell'intervallo di aggiornamento intermedio, ASA/FTD rileva che PSN1 non è accessibile.

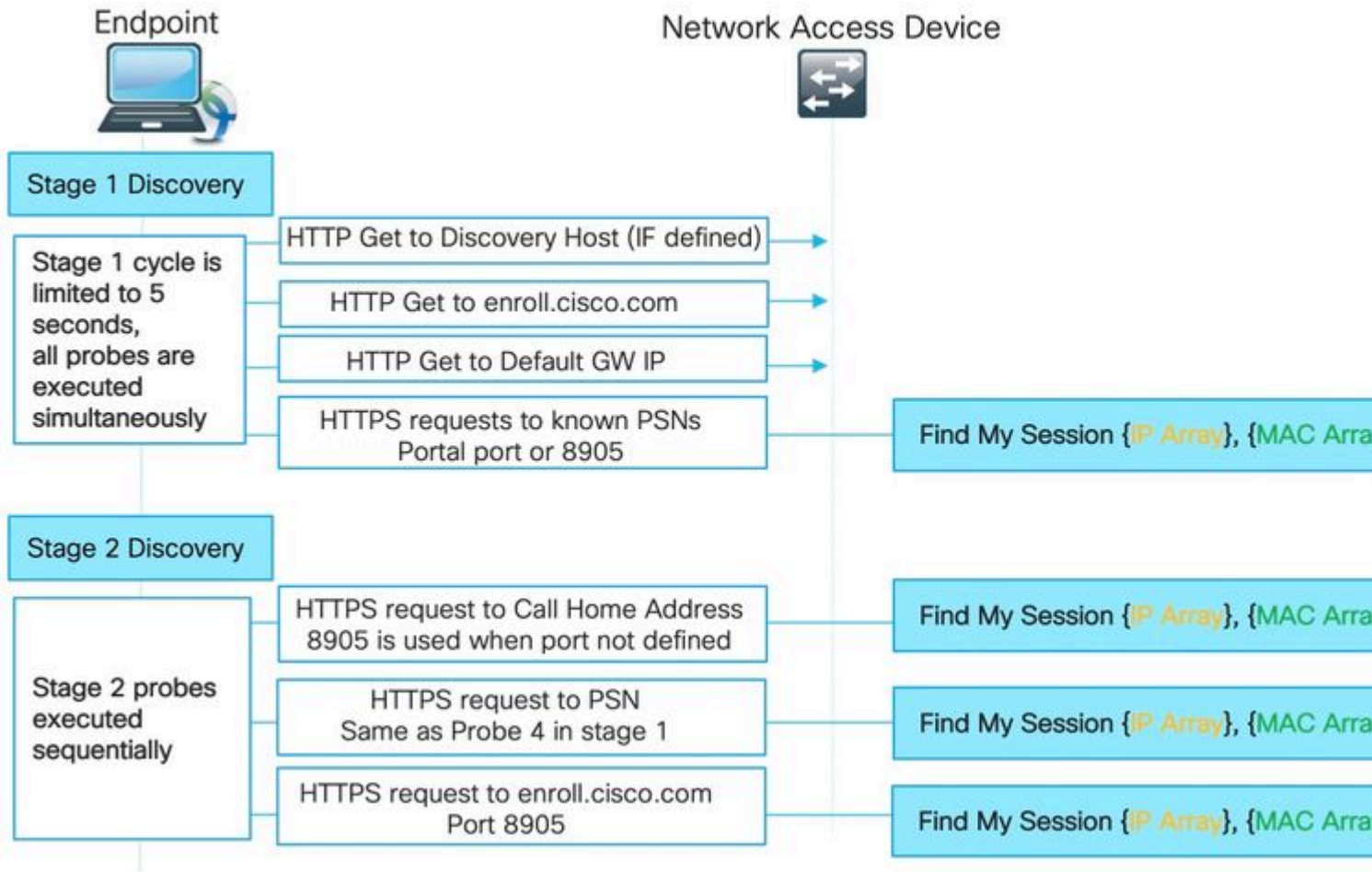
12. L'aggiornamento della contabilità provvisoria viene eseguito in PSN2.

13. Sessione fantasma creata nella cache della sessione PSN2.

Se in seguito PSN1 diventa accessibile (14), tutti i messaggi di accounting successivi vengono inoltrati (15,16) e la sessione ABC rimane nella cache della sessione PSN2 per un periodo di tempo non definito.

In che modo una sessione obsoleta e una sessione fantasma interrompono il processo di postura?

Per comprendere come la sessione non aggiornata e la sessione fantasma interrompano la postura, è possibile rivedere il processo di rilevamento del modulo di postura AnyConnect ISE:



Individuazione fase 1:

In questa fase, il modulo di postura ISE esegue 4 problemi simultanei per individuare il PSN che ha eseguito un'autenticazione per l'endpoint.

In primo luogo, 3 probe sulla cifra sono basate sul reindirizzamento (IP GW predefinito). Discovery host IP (se definito) e enroll.cisco.com IP): queste sonde puntano sempre l'agente al PSN corretto, in quanto l'URL di reindirizzamento viene preso dal NAD stesso.

La sonda numero 4 viene inviata a tutti i server primari presenti nel file **ConnectionData.xml**. Questo file creato dopo il primo tentativo di postura riuscito e il contenuto del file successivo possono essere aggiornati nel caso in cui il client esegua la migrazione tra i PSN. Sui sistemi Windows, il percorso del file è - **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.**

Poiché tutte le sonde della fase 1 vengono eseguite contemporaneamente, il risultato della sonda 4 viene utilizzato solo se tutte le altre 3 sonde hanno avuto esito negativo o se il modulo di postura ISE non è stato in grado di stabilire una comunicazione corretta con il PSN restituito nell'URL di reindirizzamento entro 5 secondi.

Quando il probe 4 atterra sul PSN, contiene un elenco di indirizzi IP e MAC attivi rilevati sull'endpoint. Il servizio PSN utilizza questi dati per trovare una sessione per l'endpoint nella cache locale. Se il PSN dispone di una sessione non aggiornata o fittizia per l'endpoint, lo stato della postura visualizzato sul lato client potrebbe essere errato.

Quando un agente riceve più risposte per la sonda 4 (**ConnectionData.xml** può contenere più di un PSN primario) viene sempre utilizzata la risposta più rapida.

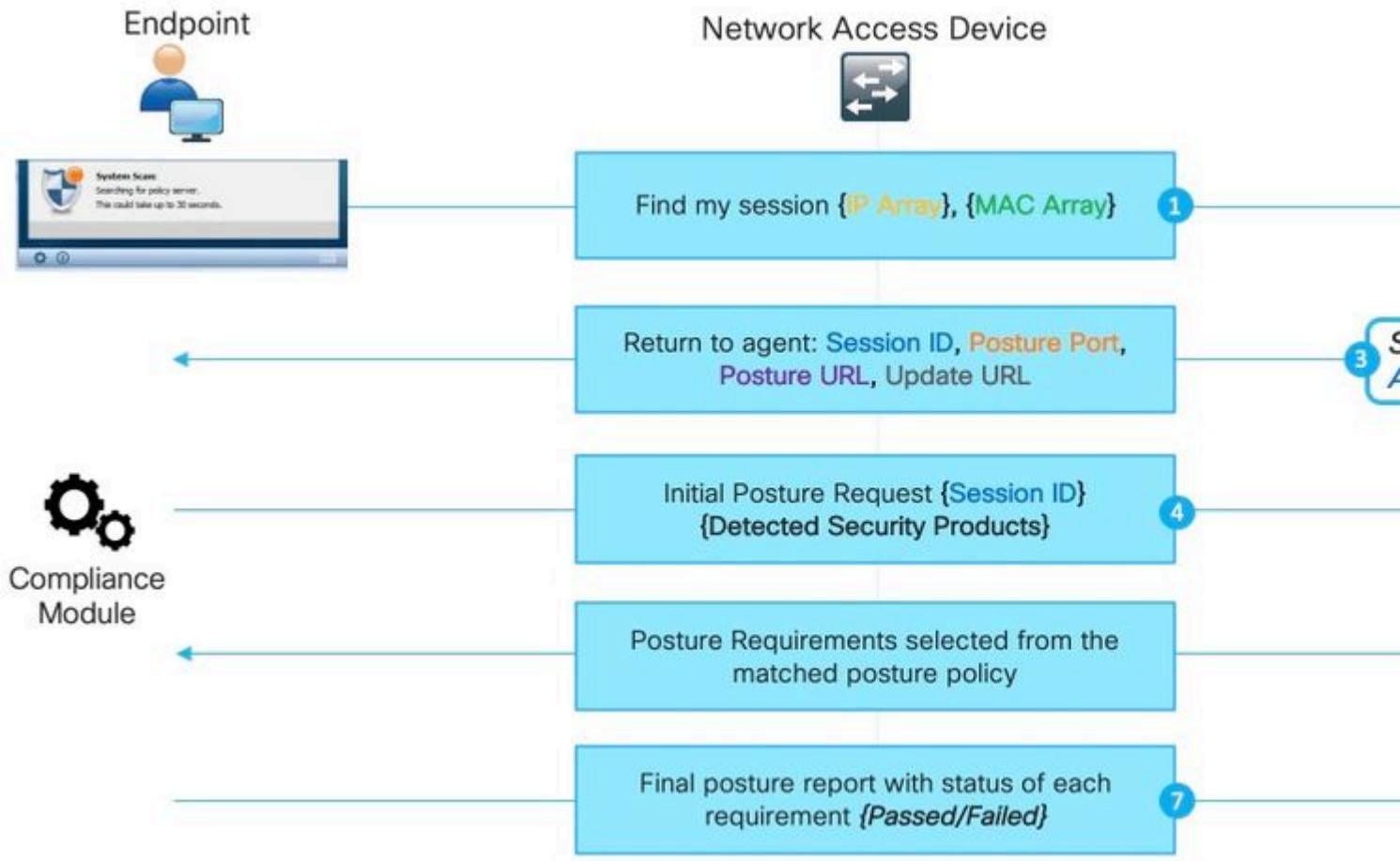
Individuazione fase 2:

Tutte le richieste di individuazione della fase 2 sono senza reindirizzamento, il che significa che ogni sonda attiva una ricerca di sessione sul PSN di destinazione. Se il PSN non è in grado di individuare la sessione nella cache della sessione locale, deve eseguire una ricerca MNT (solo basata sull'indirizzo MAC) per trovare un proprietario della sessione e restituire il nome del proprietario all'agente.

Poiché tutti i probe attivano la ricerca di sessioni, la fase 2 del rilevamento può essere ulteriormente influenzata da problemi derivanti da sessioni obsolete o fantasma.

Se il PSN raggiunge la fase 2, la sonda di rilevamento presente nella cache della sessione crea una voce non aggiornata o fittizia per lo stesso endpoint. Il risultato è uno stato di postura errato restituito all'utente finale.

Nell'esempio viene mostrato come si verifica la postura quando il PSN mantiene una sessione obsoleta o una sessione fantasma:



Nota: è importante ricordare che questo problema può manifestarsi solo quando tutte le richieste di rilevamento basate sul reindirizzamento hanno esito negativo o quando viene implementata la postura di non reindirizzamento.

---

1. Una qualsiasi delle sonde **Find my session** emesse dal modulo ISE posture.

2. PSN esegue la ricerca di sessioni nella cache delle sessioni. Se la sessione deve essere individuata, si verifica un problema di sessione non aggiornata o fittizia.

3. PSN esegue la selezione dei criteri di provisioning client. In caso contrario, con una sessione fantasma priva di attributi di autenticazione/autorizzazione e tutti i criteri configurati dal cliente sono molto specifici (i criteri vengono creati per gruppi di Active Directory specifici, ad esempio), PSN non è in grado di assegnare un criterio di provisioning client corretto. Questa condizione può essere rilevata nel messaggio di errore: "Ignorando AnyConnect, la rete è configurata per l'utilizzo di Cisco NAC Agent".

- Nel caso in cui i criteri di provisioning client siano generici (gli attributi disponibili nella sessione fantasma sono sufficienti per corrispondere ai criteri della configurazione AnyConnect), il PSN risponde con i dettagli necessari per la continuazione del processo di valutazione.
- Anche in questa fase, quando è possibile gestire sessioni obsolete, PSN risponde immediatamente con lo stato di postura **Conforme** e tutte le fasi successive non vengono eseguite. Il PSN non invia il certificato di autenticità perché ritiene che la sessione sia già conforme. Nei log Radius Live non è visualizzato alcun evento di sessione con stato **Conforme**.

4. Per lo scenario di sessione fantasma, il modulo di postura ISE continua con la richiesta di postura iniziale.

Questa richiesta contiene informazioni su tutti i prodotti di sicurezza e di gestione delle patch rilevati sull'endpoint.

5. Il PSN utilizza le informazioni degli attributi di richiesta e di sessione per soddisfare i criteri di postura appropriati. Poiché a questo punto la sessione fantasma non dispone di attributi, non esistono criteri per la corrispondenza. In questo caso, il PSN risponde all'endpoint che è conforme, poiché si tratta di un comportamento ISE predefinito in caso di mancata corrispondenza dei criteri di postura.

> **Nota**: quando esistono criteri generici che è possibile selezionare dagli attributi della sessione fantasma, si continua con il passo 6.

---

6. PSN restituisce all'agente i criteri di postura selezionati.

> **Nota**: se non è possibile selezionare alcun criterio, il PSN restituisce lo stato Conforme.

---

7. L'agente restituisce gli stati per ogni criterio/requisito come superato o non riuscito.

8. La valutazione dei report viene effettuata su ISE e lo stato della sessione cambia in **Conforme.**

> **Nota**: in caso di problemi di postura causati dalla sessione fantasma, l'amministratore ISE potrebbe notare alcuni COA di postura non riusciti, in questo caso le richieste COA vengono eseguite dai PSN errati e per ID di sessione errati.

Il processo di individuazione non viene avviato in un nuovo tentativo di autenticazione

Modulo di postura ISE progettato per monitorare una quantità limitata di eventi sull'endpoint e avviare un processo di rilevamento. Elenco di eventi che attivano l'individuazione:

- Installazione iniziale del modulo di postura ISE.
- Accesso utente.
- Eventi di alimentazione.
- Modifica stato interfaccia.
- Il sistema operativo viene ripreso dopo la sospensione.
- Modifica del gateway predefinito (DG).
- Errore di rivalutazione della postura (PRA), vedere l'ID bug Cisco CSCvo6957

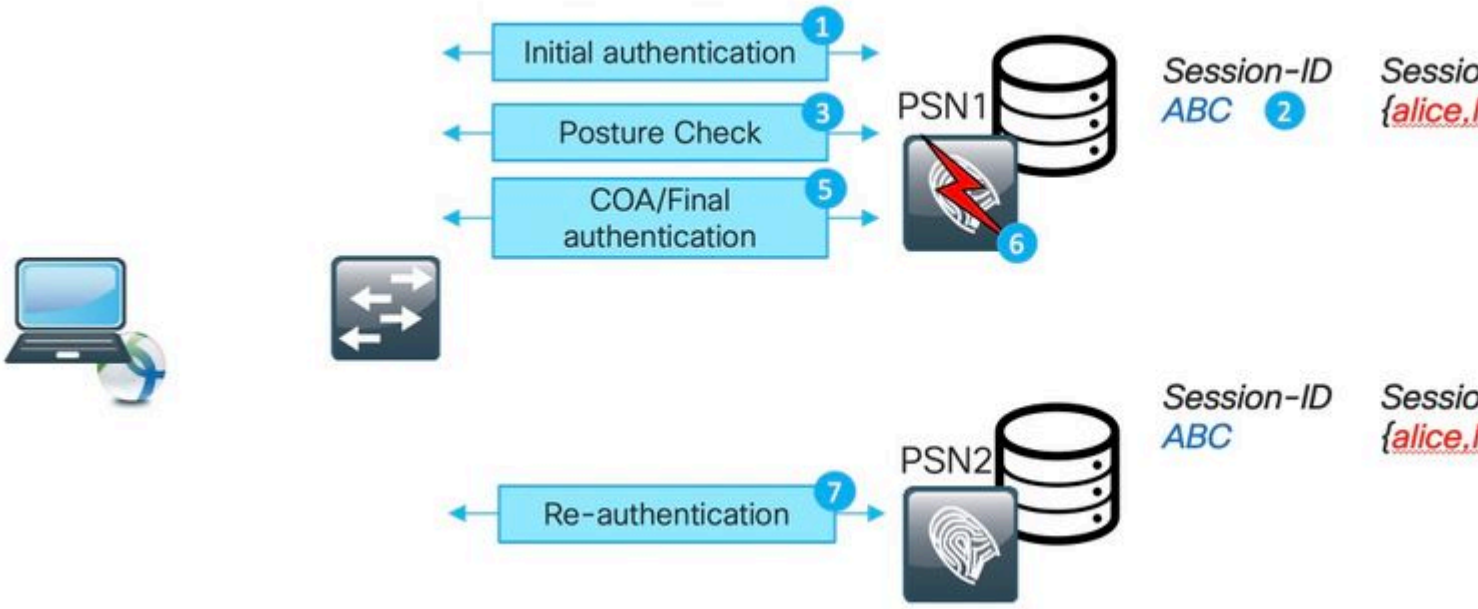
Il modulo di postura ISE non rileva nuove autenticazioni dot1x, sblocco del PC, modifica dell'indirizzo IP.

Il modulo di postura ISE non è in grado di rilevare un nuovo tentativo di autenticazione o riautenticazione in questi scenari:

- La riautenticazione ha raggiunto un numero PSN diverso (a causa di decisioni di bilanciamento del carico o di problemi con il numero PSN originale).
- NAD genera un nuovo ID sessione alla riautenticazione.

Riautenticazione su PSN diverso

Esempio di riautenticazione su PSN diverso causata dall'interruzione del PSN originale. Lo scenario con il bilanciamento del carico è molto simile. Nel caso di LB, la riautenticazione viene indirizzata al diverso PSN come risultato della scadenza del timer di persistenza.



1. Autenticazione iniziale su PSN1.

2. Sessione ABC creata nella cache della sessione PSN1.

3. Valutazione della postura eseguita con PSN1.

4. Lo stato della postura ABS della sessione viene impostato su **Conforme.**

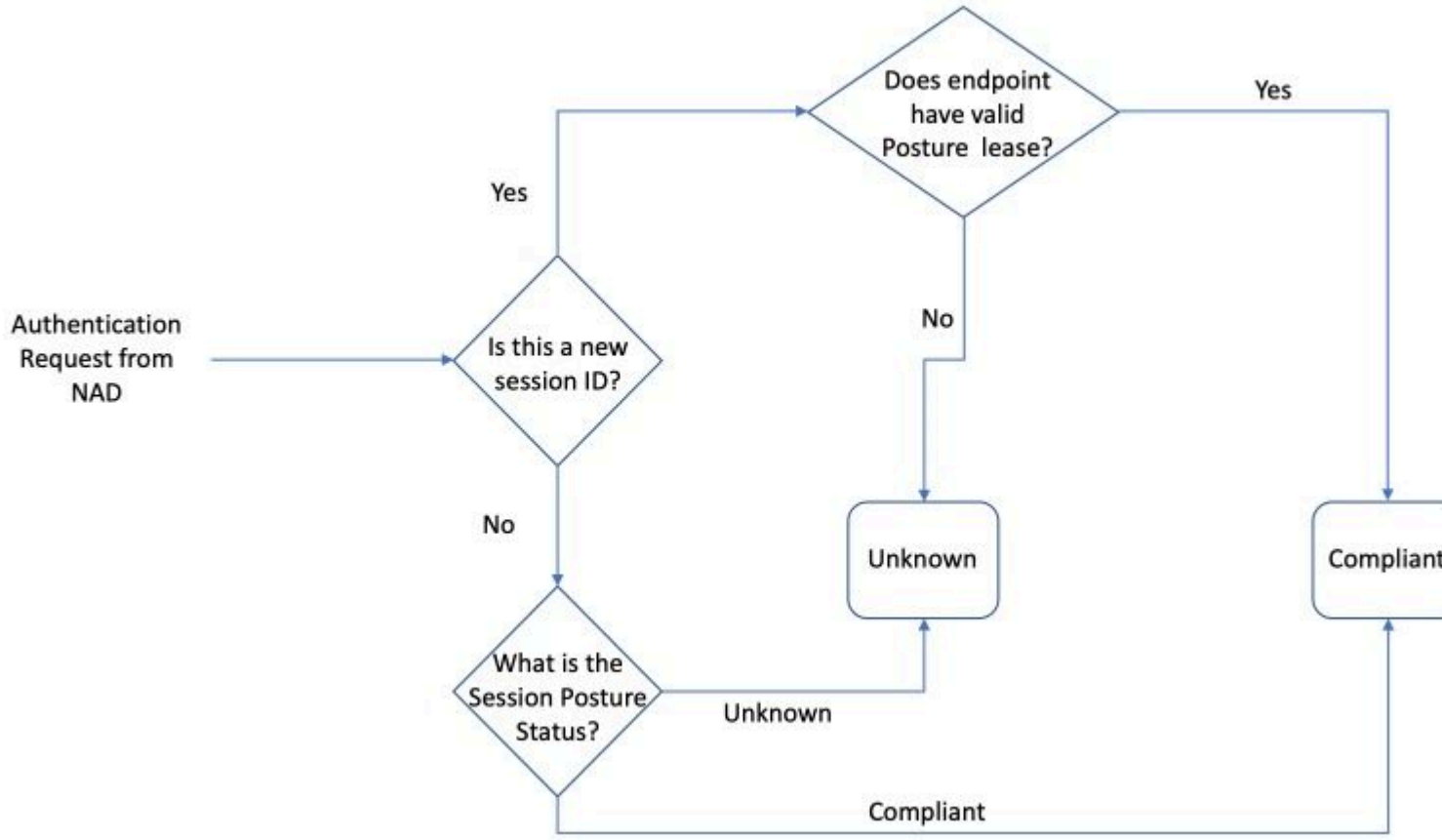
5. Il COA attivato dalla modifica dello stato della postura determina la riautenticazione dell'endpoint per applicare il livello di accesso successivo.

6. PSN1 non è più disponibile.

7. La riautenticazione per la sessione ABC ha riscontrato PSN2.

8. Poiché si tratta di una nuova sessione per la postura PSN2, lo stato della sessione diventa **In sospeso.**

Stato di postura iniziale assegnato dal PSN alla sessione:



Nota: la macchina a stati descrive solo una selezione iniziale dello stato della postura. Ogni sessione inizialmente contrassegnata come Sconosciuta può diventare successivamente conforme o Non conforme in base alla valutazione del report ricevuta dal modulo di postura ISE.

E genera un nuovo ID sessione alla riautenticazione

Questo può accadere nei due scenari più comuni:

- La riautenticazione non è configurata correttamente sul lato ISE. La soluzione a questo problema è illustrata più avanti in questo documento.
- Comportamento errato da parte di AND: in genere AND mantiene lo stesso ID di sessione durante il tentativo di riautenticazione. Nel caso in cui NAD abbia modificato un ID di sessione durante la riautenticazione, si tratta di un comportamento potenzialmente problematico che deve essere esaminato sul NAD stesso.

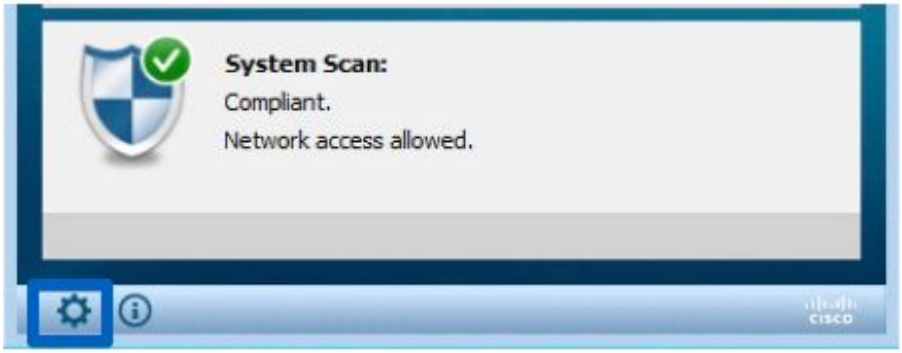
Il nuovo ID di sessione può essere generato in altri scenari con casi d'angolo. In alcuni casi, ad esempio, il roaming wireless può essere la causa di questo problema. La cosa principale qui è che ISE PSN mette sempre una nuova sessione nello stato postura **in sospeso** a meno che il lease della postura non sia configurato. Il lease della postura è descritto più avanti in questo documento.

Metodo rapido per identificare quando il problema è stato causato dalla sessione non aggiornata/fantasma

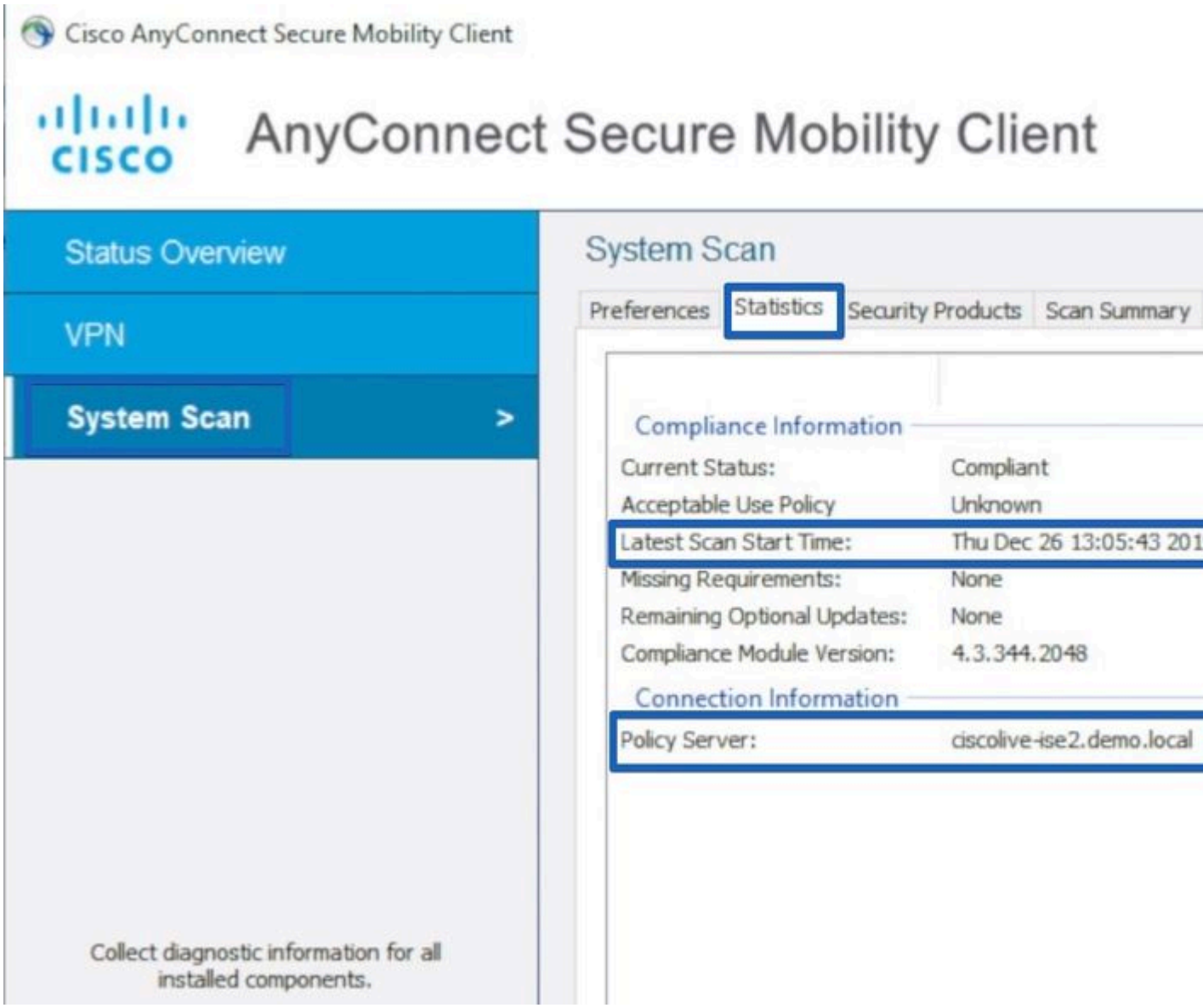
Per stabilire se AnyConnect mostra conformità mentre è in stato di reindirizzamento e è causato da una sessione non aggiornata/fittizia, dobbiamo ottenere l'accesso all'endpoint mentre è in stato di problema.

1. Dettagli analisi sistema:

1. Premere sull'icona gear nell'interfaccia utente di AnyConnect



2. Nella nuova finestra passare alla scheda Scansione sistema e alla scheda secondaria Statistiche



Prestare attenzione a due elementi:

- Ora di inizio ultima analisi: l'indicatore orario qui deve essere vicino all'ora in cui è stato rilevato il problema.

- Policy Server: questo campo indica il nome del policy server che ha eseguito una valutazione della postura per l'endpoint. Il nome di dominio completo (FQDN) deve essere confrontato con il nome di dominio completo (FQDN) dell'URL di reindirizzamento (per la postura di base di reindirizzamento) o con il nome del nome PSN ricavato dall'ultimo tentativo di autenticazione (per la postura di reindirizzamento senza reindirizzamento).

2. Confronta FQDN server dei criteri da Statistiche analisi sistema con il nome del nodo che ha eseguito l'autenticazione per l'endpoint:

Nell'esempio specificato non esiste corrispondenza tra il nome indicato come PSN con il nome ciscolive-ise2 in cui viene mantenuta una sessione non aggiornata o fittizia per l'endpoint.

La demo mostra la registrazione dei passi necessari per l'identificazione del problema:

Risoluzione avanzata dei problemi di sessioni obsolete/fantasma

L'esempio precedente è quello di distinguere il problema di una sessione obsoleta o fantasma dal problema del processo di rilevamento che non è stato avviato. Allo stesso tempo, dobbiamo identificare la sessione effettiva che ha innescato il problema per capire meglio come esattamente diventi un problema di sessione obsoleta o fantasma.

Mentre in alcuni scenari non è possibile evitare sessioni obsolete e fantasma. È necessario garantire che nell'ambiente non vengano create sessioni obsolete/fantasma a causa di alcune delle best practice non implementate.

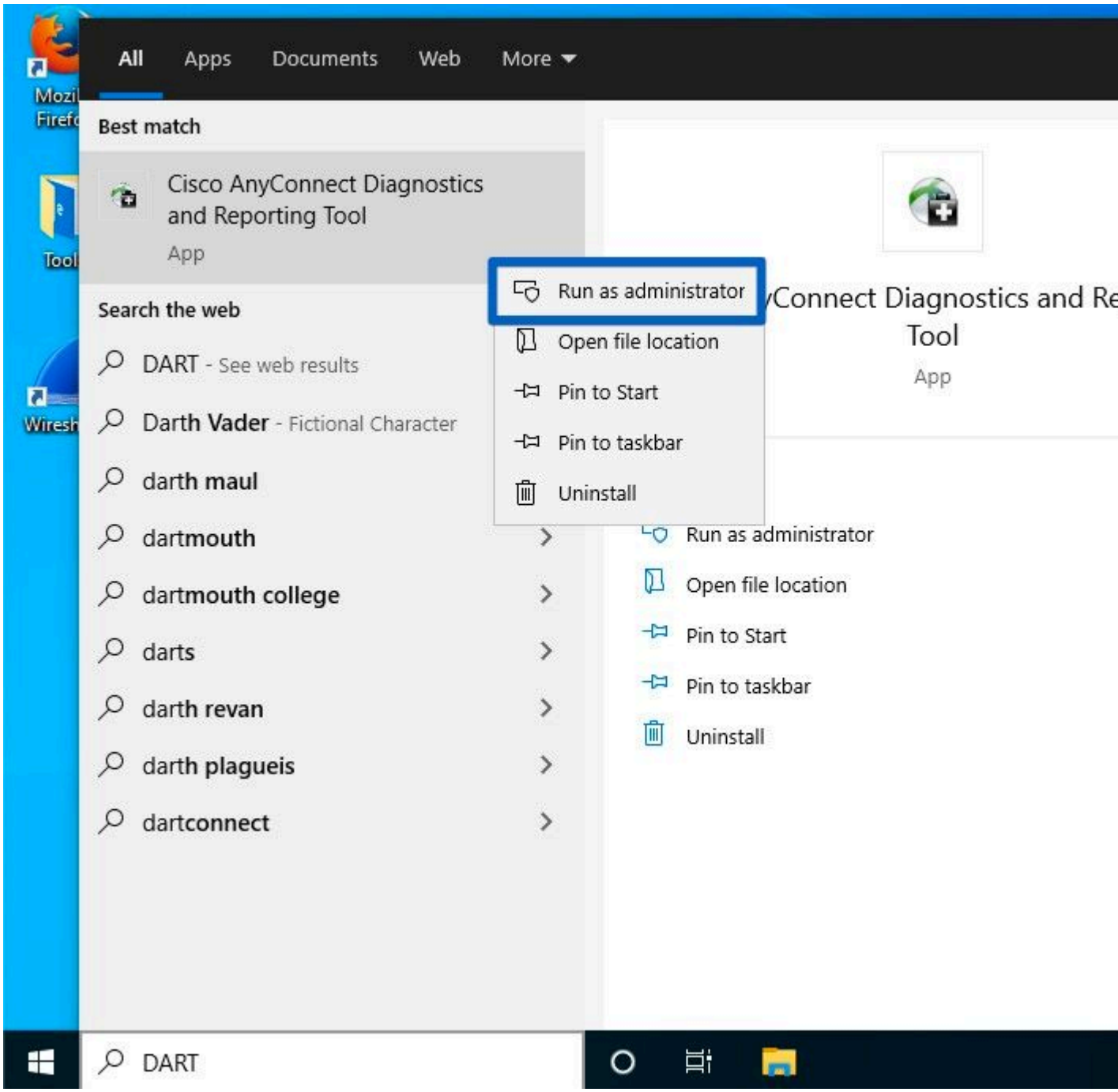
DART Bundle Collection

Analizza un bundle DART acquisito dall'endpoint che riproduce il problema.

- Conservare solo i registri importanti nel DART. Si consiglia di cancellare i registri prima di riprodurre il problema.

Per ottenere questo risultato, l'utility del bundle DART deve essere avviata come amministratore ed eseguire la pulizia del log.

1. In Windows passare a Start e iniziare a digitare DART, fare clic con il pulsante destro del mouse e scegliere - **Esegui come amministratore**



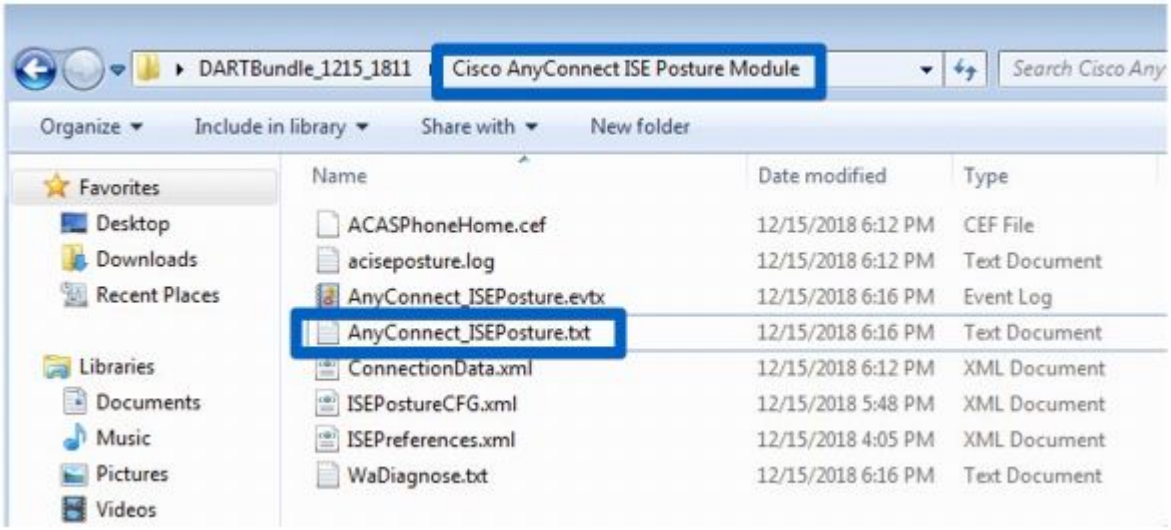
2. Nella prima schermata della procedura guidata fare clic su Avanti

3. Nella schermata successiva della procedura guidata, premere Cancella tutti i registri

4. Dopo che il problema è stato riprodotto, DART può essere raccolto da qui; premere **Avanti**.

Analisi bundle DART

Dopo aver raccolto il bundle DART, occorre annullarne l'archiviazione e concentrarsi sul file **AnyConnect_ISEPosture.txt** che si trova nella cartella **Cisco AnyConnect ISE Posture Module**. Questo file contiene tutti gli eventi correlati all'individuazione.



1. Avviare la risoluzione dei problemi e identificare tutti i momenti di riavvio del processo di individuazione. Le parole chiave da cercare sono il **riavvio del rilevamento** o il rilevamento HTTP. Passare alla riga con il riavvio del rilevamento che si è verificato nel momento in cui si è verificato il problema:

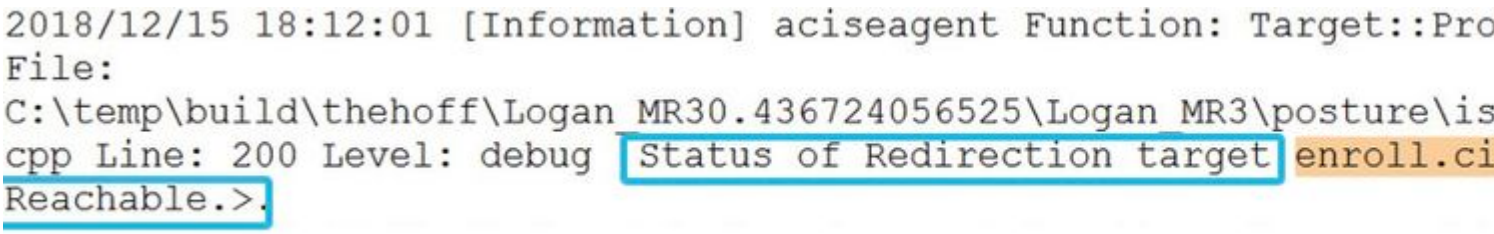
```
Line 3575: 2018/12/15 17:48:08                    1251 Level: info  Restarting Dis
Line 3840: 2018/12/15 17:48:59                    1251 Level: info  Restarting Dis
Line 3991: 2018/12/15 17:50:24                    1251 Level: info  Restarting Dis
Line 4214: 2018/12/15 18:00:54   <output omitted>  1251 Level: info  Restarting Dis
Line 4308: 2018/12/15 18:01:14                    1251 Level: info  Restarting Dis
Line 4530: 2018/12/15 18:11:45                    1251 Level: info  Restarting Dis
Line 4642: 2018/12/15 18:12:01                    1251 Level: info  Restarting Dis
```

2. Un paio di righe dopo il riavvio del rilevamento si vede una riga che contiene - Probing no MNT stage targets. Questo è un indicatore dell'avvio del rilevamento della Fase 1:

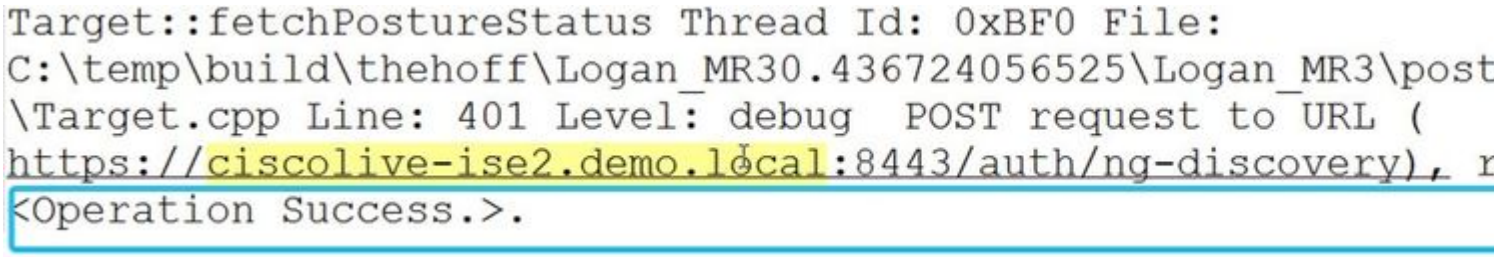
```
SwiftHttpRunner::collectNoMntTargets Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\post
ftHttpRunner.cpp Line: 1157 Level: debug  Probing no MNT sta
Redirection target 192.168.255.1, Redirection target enroll.
Auth-Status target ciscolive-ise2.demo.local with path /auth
Auth-Status target ciscolive-ise1.demo.local with path /auth
```

Si consiglia di evidenziare tutte le sonde basate sul reindirizzamento con lo stesso colore mentre i PSN precedentemente connessi ottenuti dalle destinazioni **ConnectionData.xml** (Auth-Status) devono essere evidenziati in colori diversi, in quanto normalmente i PSN FQDN sono molto simili ed è difficile individuare la differenza.

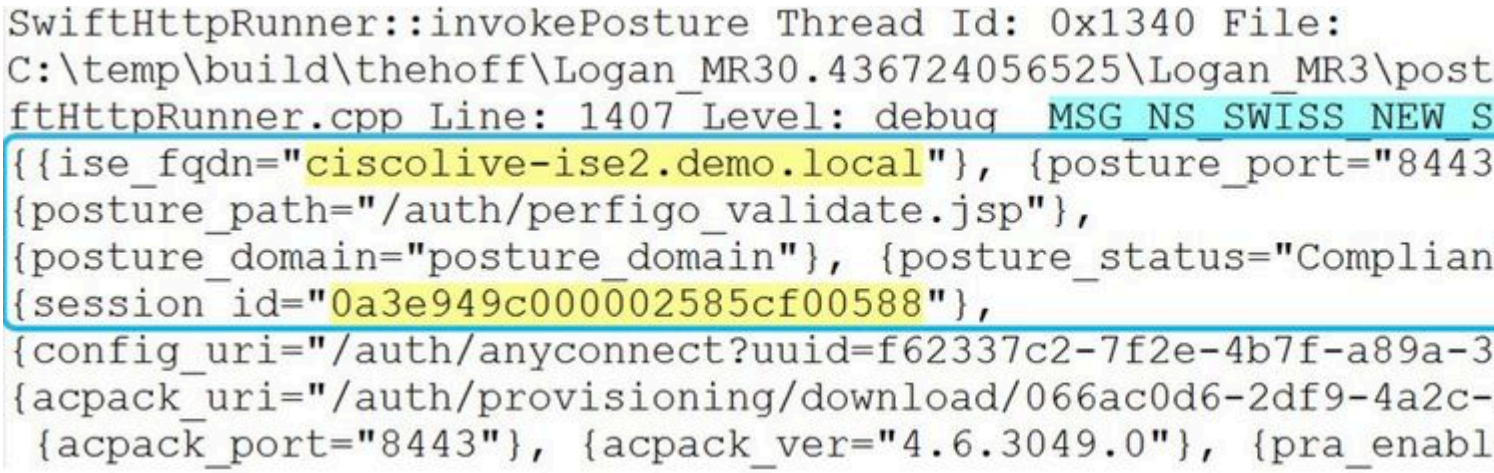
3. Leggere i file di log per vedere un risultato per ciascuna sonda. Come è stato già detto nel caso del problema causato da sessione obsoleta/fantasma tutte le sonde basate sul reindirizzamento devono fallire. Questo è un esempio di come appare la sonda guasta:



4. In un punto qualsiasi del file dopo il riavvio del rilevamento per la fase 1 o 2, viene visualizzata una risposta corretta da uno o più PSN:



5. Un paio di righe dopo c'è una riga con la parola chiave **MSG_NS_SWISS_NEW_SESSION.** Questa riga contiene un ID sessione effettivo selezionato dal PSN come risultato della ricerca della sessione. Usare questo ID sessione per ulteriori informazioni su ISE per capire come questa sessione diventa obsoleta/fantasma:



Indagine sui log ISE

Nel file guest.log con il componente **clientwebapp** abilitato in DEBUG, è possibile visualizzare il PSN che risponde con la sessione obsoleta/fantasma.

PSN riceve una richiesta dall'agente di postura ISE. Questa è una richiesta di AnyConnect a causa del valore User-Agent:

<#root>

```
cisco.cpm.client.posture.PostureStatusServlet -::-
```

Got http request from 192.168.255.228 user agent is: Mozilla/4.0 (compatible; WINDOWS; 1.2.1.6.1.48; Any

```
cisco.cpm.client.posture.PostureStatusServlet -::-
```

```
mac_list
 from http request ==> C0:4A:00:1F:6B:39


cisco.cpm.client.posture.PostureStatusServlet -::-
iplist
 from http request ==> 192.168.255.228


cisco.cpm.client.posture.PostureStatusServlet -::-
Session id from http request -
req.getParameter
(
sessionId
) ==> null
```

La richiesta contiene matrici di indirizzi IP e indirizzi MAC. In questo particolare esempio, ogni matrice contiene un solo valore. Anche il log indica che l'ID sessione della richiesta è null, il che indica che si tratta di una richiesta della sonda non reindirizzata.

In seguito sarà possibile vedere come i valori degli array vengono utilizzati per individuare un ID sessione:

```
<#root>
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently processe
cpm.client.provisioning.utils.ProvisioningUtil -::- the ipAddress that matched the http request remote a
cpm.client.provisioning.utils.ProvisioningUtil -::- the clientMac from the macarray list for the for loo
cisco.cpm.client.posture.PostureStatusServlet -::- Found Client IP matching the remote IP 192.168.255.22
cpm.client.provisioning.utils.ProvisioningUtil -::-
Session = 0a3e949c000000495c216240
```

Dopo la riga con le parole chiave **Inviata risposta http** è possibile visualizzare il contenuto della risposta effettiva:

```
<#root>
cisco.cpm.client.posture.PostureStatusServlet -::- Sent an http response to  192.168.255.228 with X-ISE-
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PDP value is clemea19-ise1.demo.local
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-POSTURE value is /auth/perfigo_validate
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-POSTURE_PORT value is 8443
```

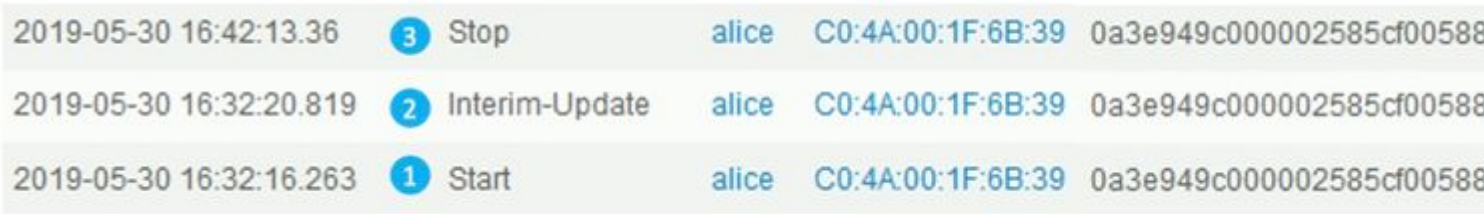
```
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_PORT value is 8443

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-GUESTFLOW value is false

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_CONFIG_URL value is https://clemea19

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_CONFIG_URI value is /auth/anyconnect

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_URL value is https://clemea19-is

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_URI value is /auth/provisioning/

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_VER value is 4.6.3049.0

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-STATUS_PATH value is /auth/status

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-BACKUP_SERVERS value is clemea19-ise2.c

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-SessionId value is 0a3e949c000000495c21

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-PostureDomain value is posture_domain

cpm.client.provisioning.utils.ProvisioningUtil -::-
header X-ISE-POSTURE_STATUS value is Unknown
```

Indagine sui report ISE

Dopo aver individuato l'ID della sessione non aggiornata/fantasma, è possibile esaminare il report di Contabilità Radius per comprendere meglio le cause che hanno portato la sessione a diventare non aggiornata/velata:

- Passare a Operazioni > Rapporti > Endpoint e utenti > Rapporto Contabilità Radius ed eseguire questo rapporto per 7 giorni. Utente ID endpoint come chiave di filtro.

Esempio di report che mostra come è stata lasciata una sessione obsoleta su ciscolive-ise2:



1. L'avvio dell'accounting per la sessione è stato inviato a PSN ciscolive-ise2
2. L'aggiornamento temporaneo per la sessione è stato elaborato nello stesso PSN.
3. Il messaggio di interruzione dell'accounting per l'ID di sessione con problemi è stato inviato a un PSN diverso (ciscolive-ise1).

Un modo rapido per identificare quando il problema è stato causato dall'assenza del riavvio del rilevamento

In questo caso, è possibile seguire la stessa logica del problema precedente. L'unica differenza è che è necessario concentrarsi sull'ora di inizio dell'ultima scansione. Per questo tipo di problema, la data e l'ora

dell'ultima analisi sono già trascorse.

Normalmente, quando l'utente finale rileva un problema, viene visualizzata una scansione eseguita qualche tempo fa. Nei log ISE Radius Live, sono visualizzati i recenti tentativi di autenticazione dall'endpoint problematico.

La demo mostra la registrazione dei passi necessari per l'identificazione del problema:

Risoluzione avanzata dei problemi relativi all'assenza di riavvio del rilevamento

L'approccio è molto simile alla sezione Advanced Troubleshoot Stale/Phantom Session. L'elemento principale per la risoluzione dei problemi è l'analisi del bundle DART. All'interno del bundle DART, è possibile ricercare i riavvii di individuazione come mostrato per il problema precedente e confermare che non vi è stato alcun riavvio di individuazione nel momento in cui il problema è stato segnalato.

Sul lato ISE, esaminare il report sull'autenticazione Radius Live Logs/ Radius per verificare che sia stato generato il failover tra i PSN o un nuovo ID sessione da NAD.

Soluzione

Approccio classico - Prevenzione dei problemi

Storicamente ISE non aveva una funzione in grado di risolvere i problemi descritti in questo documento, quindi l'unico modo è stato affidarsi alla serie di best practice implementate sulla rete e dal lato ISE ridurre al minimo i rischi.

Procedure ottimali per ridurre al minimo il numero di sessioni obsolete o fantasma nell'implementazione ISE

Implementa Sempre La Postura Basata Sul Reindirizzamento, Quando Possibile

Un comune argomento contrario a questa raccomandazione è la cattiva esperienza dell'utente, in quanto vengono visualizzati popup nel sistema operativo o nei browser che indicano il reindirizzamento, mentre il modulo di postura AnyConnect ISE in background esegue un processo di valutazione.

Per risolvere questo problema, è possibile reindirizzare SOLO le richieste di rilevamento del modulo ISE Posture e consentire in modo selettivo tutto il resto del traffico.

Nell'esempio viene mostrato come reindirizzare un ACL progettato per reindirizzare solo le richieste HTTP all'host di individuazione (10.1.1.1 nell'esempio) e all'indirizzo enroll.cisco.com (172.16.1.80):

```
ip access-list extended REDIRECT-DH-ENROLL

 permit tcp any host 10.1.1.1 eq www

 permit tcp any host 172.16.1.80

 deny   ip any any
```

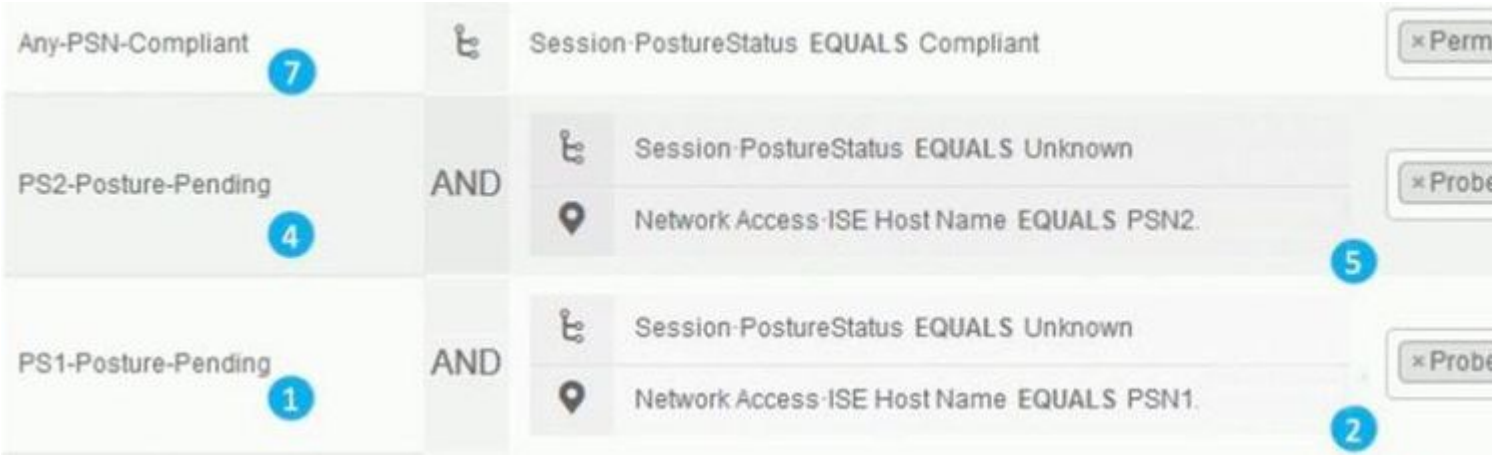
Per mantenere un livello accettabile di sicurezza, questo ACL di reindirizzamento può essere combinato con un ACL di DACL assegnato da ISE.

Stato in sospeso Consente le connessioni solo a PSN in cui l'endpoint è stato autenticato

Questo approccio è utile per gli ambienti in cui il reindirizzamento dell'URL non è supportato (ad esempio le implementazioni con NAD di terze parti).

Come soluzione, è necessario implementare più criteri di autorizzazione **PosturePending** (uno per PSN). Ogni criterio deve contenere come condizione il nome del PSN in cui è stata eseguita l'autenticazione. Nel profilo di autorizzazione assegnato a ogni criterio è necessario bloccare l'accesso a tutti i nomi di servizio (PSN) ad eccezione del nodo in cui è stata eseguita l'autenticazione.

Creare criteri di autorizzazione per la distribuzione su 2 nodi:



â€ƒ

1. Criterio di postura **in sospeso** per PSN1.

2. Nome PSN1 utilizzato come condizione nel criterio.

3. Profilo di autorizzazione con ACL che blocca l'accesso a tutti i PSN ad eccezione di PSN1.

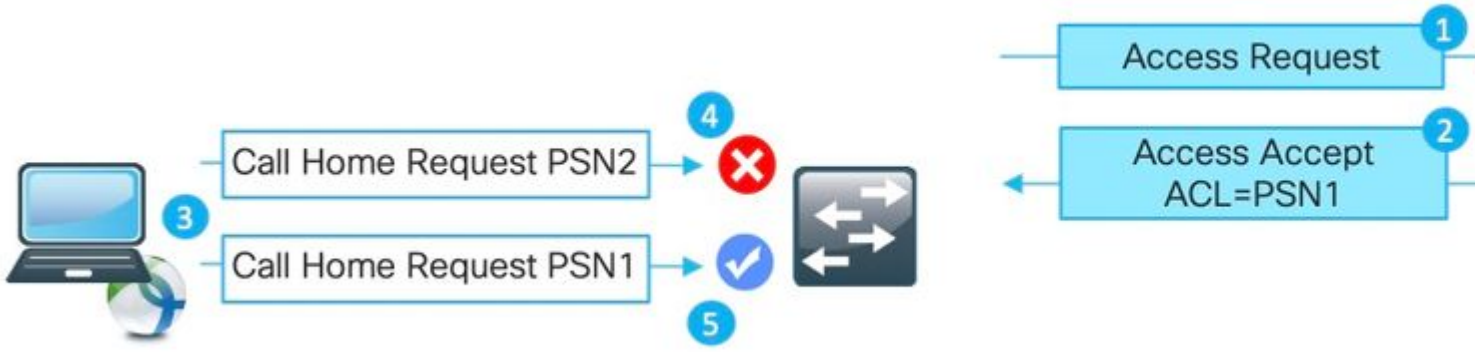
4. Criterio di postura **in sospeso** per PSN2.

5. Nome PSN2 utilizzato come condizione nel criterio.

6. Profilo di autorizzazione con ACL che blocca l'accesso a tutti i PSN ad eccezione di PSN2.

7. Criteri di autorizzazione 'Conforme' postura.

La figura spiega come funziona questo approccio:



1. L'autenticazione ha raggiunto PSN1.

2. Come risultato dei criteri di autorizzazione configurati, PSN1 assegna un profilo di autorizzazione che blocca l'accesso a tutti gli altri nodi ad eccezione di PSN1.

3. Il modulo di postura AnyConnect ISE riavvia il processo di rilevamento.

4. Probe su PSN2 bloccato da NAD come da un ACL assegnato in precedenza.

5. Probe su PSN1 consentito dall'ACL assegnato su NAD.

Best practice per il servizio di bilanciamento del carico

- Abilitato la persistenza su LB per l'autenticazione e l'accounting con Calling-Station-ID come chiave di persistenza. Per maggiori informazioni sulle best practice di IBM per ISE, fare clic qui.
- Utilizzare un timer di persistenza più lungo di una giornata lavorativa media per coprire il momento in cui il PC entra in sospensione (ad esempio, 10 ore anziché 8).
- Se viene implementata la riautenticazione, utilizzare un timer di riautenticazione leggermente inferiore al timer di persistenza (ad esempio, 8 ore se la persistenza è configurata per 10 ore). In questo modo, l'intervallo di persistenza viene prolungato con la riautenticazione.

Postura su caso di utilizzo VPN

- Assicura che l'intervallo di aggiornamento intermedio di accounting sia maggiore o uguale a vpn-session-timeout. In questo modo si evita il flapping di accounting tra PSN su sessioni VPN a lungo termine.

In questo esempio viene mostrato l'intervallo di aggiornamento della contabilità provvisoria configurato per 20 ore. Ciò non impedisce l'aggiornamento provvisorio iniziale che trasporta l'indirizzo IP assegnato all'endpoint.

```
aaa-server ISE protocol radius

 interim-accounting-update periodic 20

group-policy SSL-VPN attributes

 vpn-idle-timeout 1200

 vpn-session-timeout 1200
```

È possibile implementare best practice per ridurre al minimo l'impatto dovuto all'assenza del riavvio del modulo di rilevamento della postura ISE

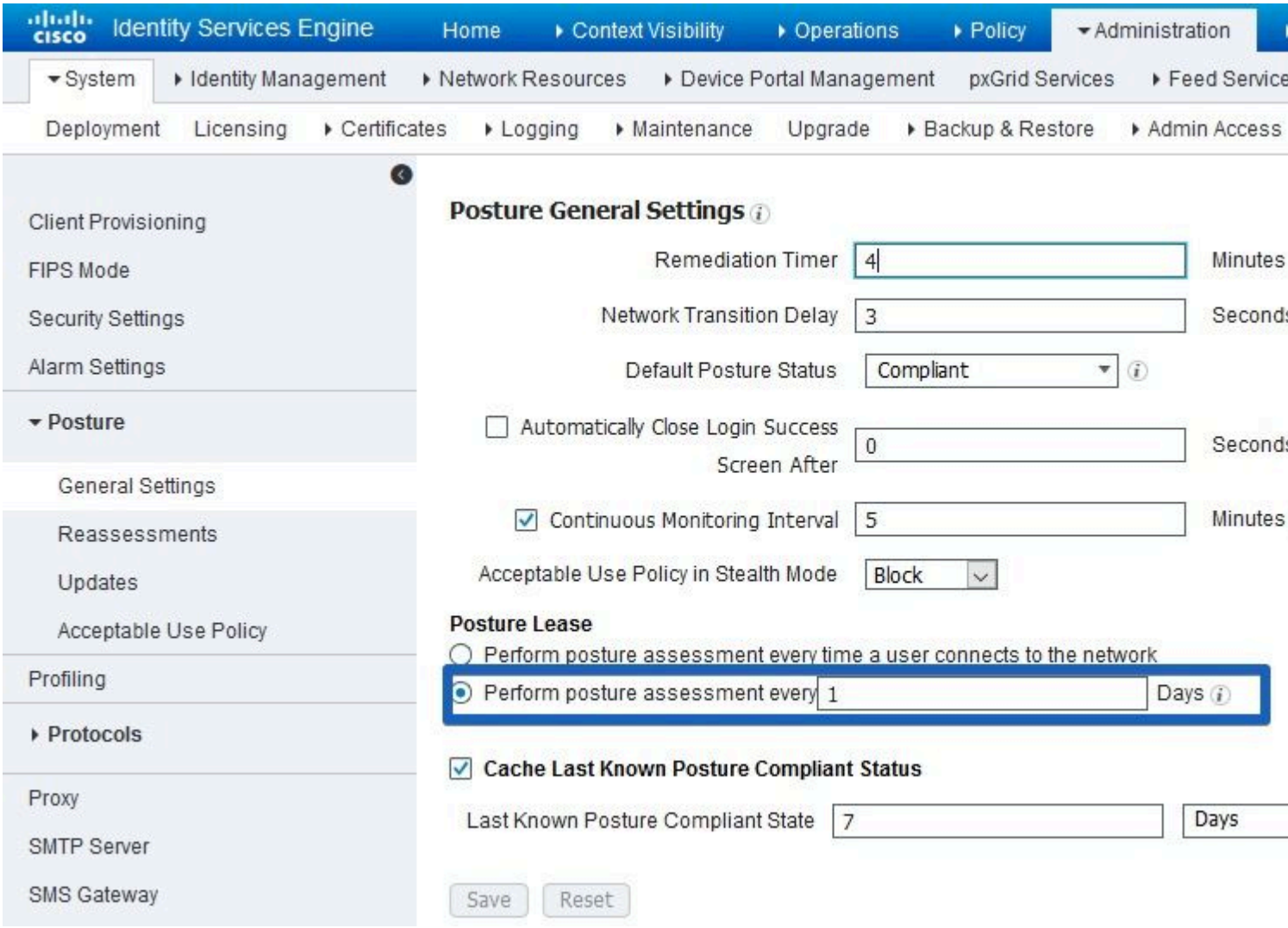
Abilita lease postura

Questa funzionalità di ISE contrassegna l'endpoint come conforme per un periodo definito (1-365 giorni). Il valore di lease della postura è un attributo dell'endpoint, il che significa che è archiviato in ISE DB. Tutti gli attributi dell'endpoint che includono il lease di postura vengono replicati su tutti i nodi nell'implementazione ISE.

Quando PSN ottiene una nuova sessione per il lease della postura dell'endpoint può essere utilizzato immediatamente per contrassegnare la sessione come **conforme**.

Per prendere questa decisione, il numero di serie del servizio utilizza 3 valori. Tali valori sono:

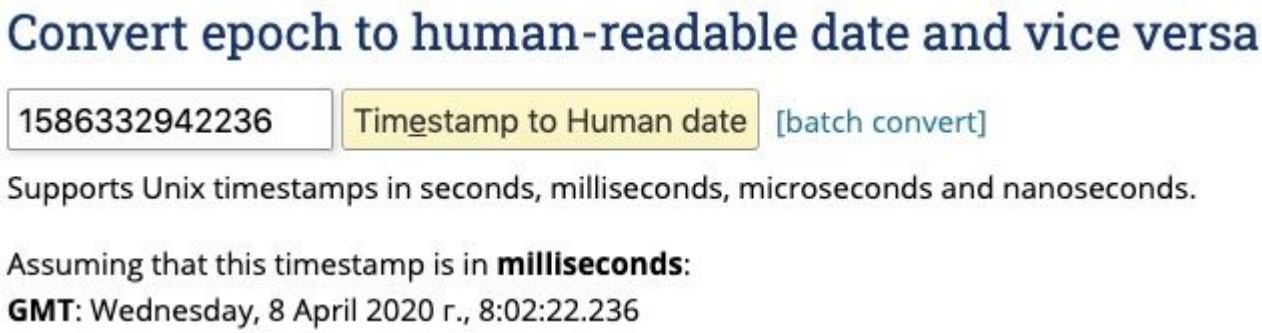
- Quantità di giorni definita per il leasing della postura nelle impostazioni ISE: **passare ad Amministrazione > Sistema > Postura > Impostazioni generali**:



- Valore dell'attributo PostureExpiry: si tratta di un attributo endpoint effettivo che contiene un timestamp Epoch. Il valore di PostureExpiry viene inserito inizialmente al primo tentativo riuscito di postura per l'endpoint dopo il lease di postura abilitato dall'amministratore ISE. In seguito questo valore viene aggiornato al successivo tentativo di postura riuscito che si verifica dopo la scadenza del lease.

È possibile visualizzare PostureExpiry in Context Visibility > Endpoints mentre uno degli endpoint posturati è aperto:

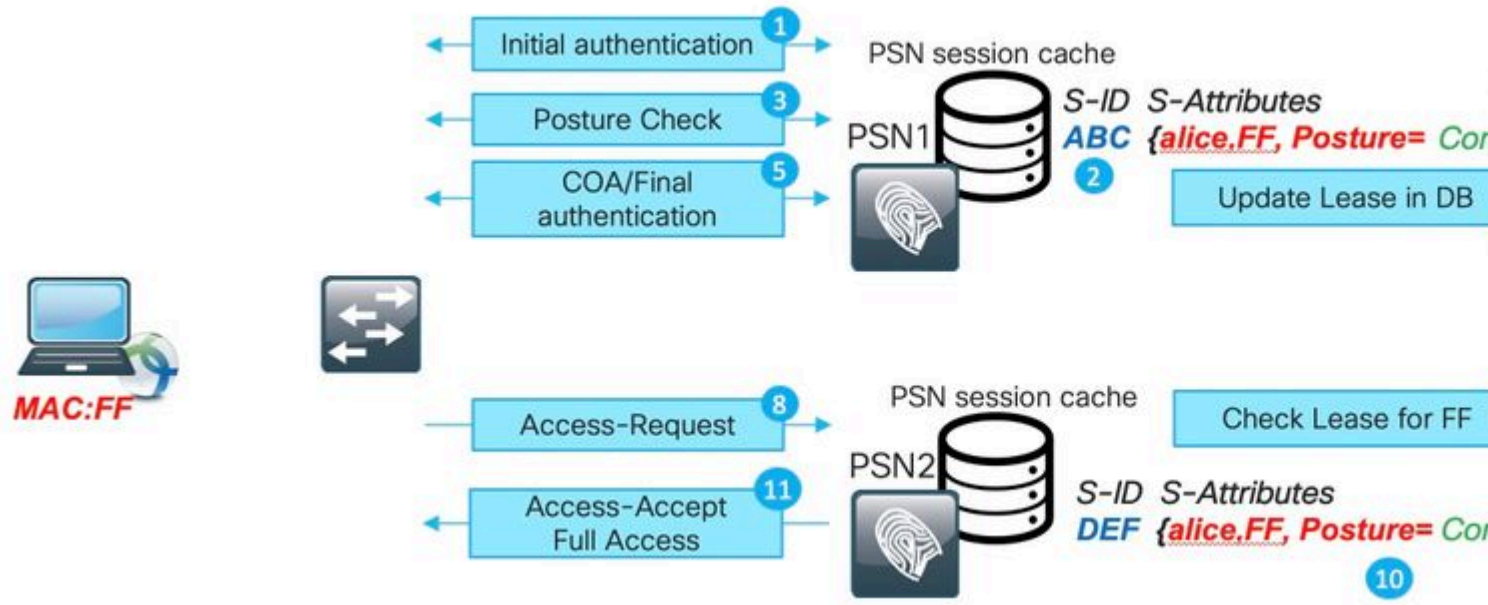
Questo valore può essere convertito nel timestamp leggibile dall'uomo, ad esempio qui - https://www.epochconverter.com/



- Ora di sistema PSN nel momento in cui viene eseguita la nuova autenticazione

Quando l'autenticazione per un endpoint con lease di postura raggiunge il numero PSN, utilizza PostureExpiry e la data di sistema per ottenere il numero di giorni trascorsi dall'ultimo controllo di postura riuscito. Se il valore risultante rientra in un intervallo di lease di postura definito nelle impostazioni, la sessione ottiene lo stato **Conforme**. Se il valore risultante è superiore al valore di lease, alla sessione viene assegnato lo stato **Sconosciuto**. In questo modo la postura viene eseguita nuovamente ed è possibile salvare il nuovo valore di PostureExpiry.

Nella figura viene illustrato il processo in cui si verifica il failover:



1. L'autenticazione iniziale viene eseguita con PSN1.

2. Sessione ABC creata nella cache della sessione.

3. La valutazione della postura avviene.

4. Lo stato della sessione cambia in **Conforme**

5. Il COA attivato dalla modifica dello stato della postura determina la riautenticazione dell'endpoint per applicare il livello di accesso successivo.

6. Valore di PostureExpiry salvato nell'endpoint.

7. Dati dell'endpoint replicati nell'implementazione.

8. L'autenticazione successiva raggiunge PSN2.

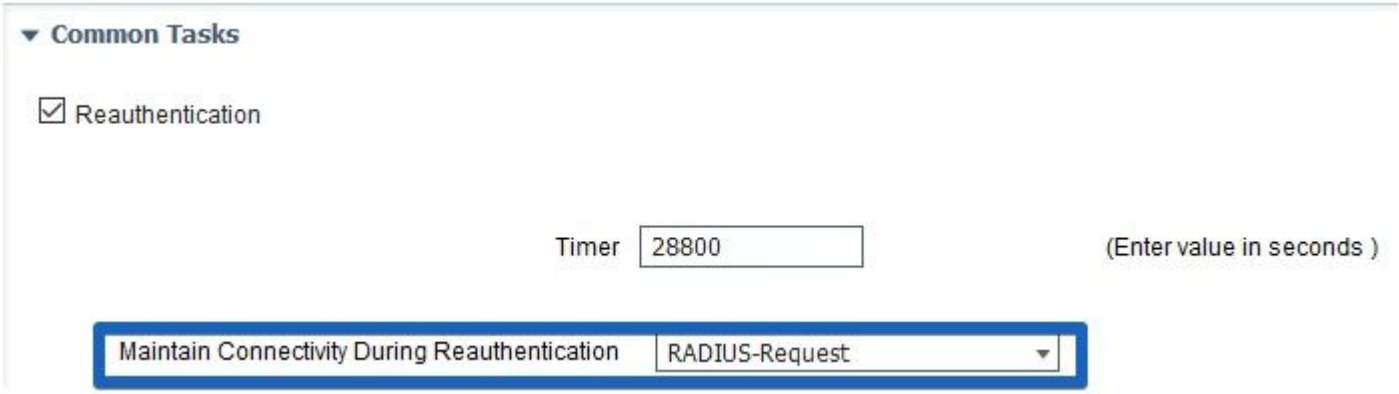
9. PSN2 verifica se l'endpoint rientra in un lease di postura valido.

11. Sessione aggiunta alla cache delle sessioni come **conforme**.

12. A causa del lease valido, la sessione è stata creata con lo stato di postura **Conforme**.

Implementazione della riautenticazione

Eseguire sempre il push del timer di riautenticazione da ISE con **RADIUS-Request** selezionato in **Mantieni connettività durante la riautenticazione.** Questa impostazione garantisce che NAD mantenga lo stesso ID sessione durante la riautenticazione.



.

Ambienti con load balancer

È possibile implementare le stesse procedure ottimali descritte nella sezione relativa alle sessioni obsolete/fantasma.

È possibile utilizzare subnet diverse per gli stati In sospeso e Conforme

Quando la progettazione della rete offre la possibilità di utilizzare diverse subnet con stati **In sospeso** e **Conforme**, questo approccio garantisce che ogni modifica nello stato della postura determini la modifica del gateway predefinito.

Valutazione della postura utilizzata nello stesso intervallo del timer di riautenticazione

La valutazione della postura può essere abilitata con un intervallo uguale al timer di riautenticazione. In tal caso, quando il PSN originale non diventa disponibile, l'errore PRA riavvia il processo di rilevamento.

Approccio moderno - Condivisione dello stato di postura

Come parte di un miglioramento implementato, descritto nell'ID bug Cisco CSCvi35647patch 6 per ISE 2.6, è stata fornita una nuova funzionalità che implementa la condivisione dello stato della postura della sessione su tutti i nodi nell'implementazione di ISE. Questo miglioramento è integrato nelle future versioni: ISE 2.7, patch 2 e ISE 3.0.

Questa nuova funzionalità si basa sul meccanismo LSD (Light Session Directory), introdotto ad ISE 2.6. Nelle versioni più recenti, questa funzionalità è stata rinominata LDD (Light Data Distribution) Radius Session Directory. Light Data Distribution è abilitato per impostazione predefinita e consente la condivisione di un contesto di sessione limitato tra i nodi ISE. Non esiste una replica completa del contesto di sessione tra i PSN, ma solo una quantità limitata di attributi condivisi per ogni sessione.

L'idea principale alla base di Light Session Directory è quella di rimuovere la necessità di eseguire chiamate API a MNT dispendiose in termini di risorse quando uno dei nodi nella distribuzione deve capire chi è il proprietario della sessione corrente. La ricerca principalmente del proprietario è necessaria all'avvio del flusso COA. Con LDD ogni PSN può trovare un proprietario effettivo della sessione dalla cache della directory di sessione Radius locale.

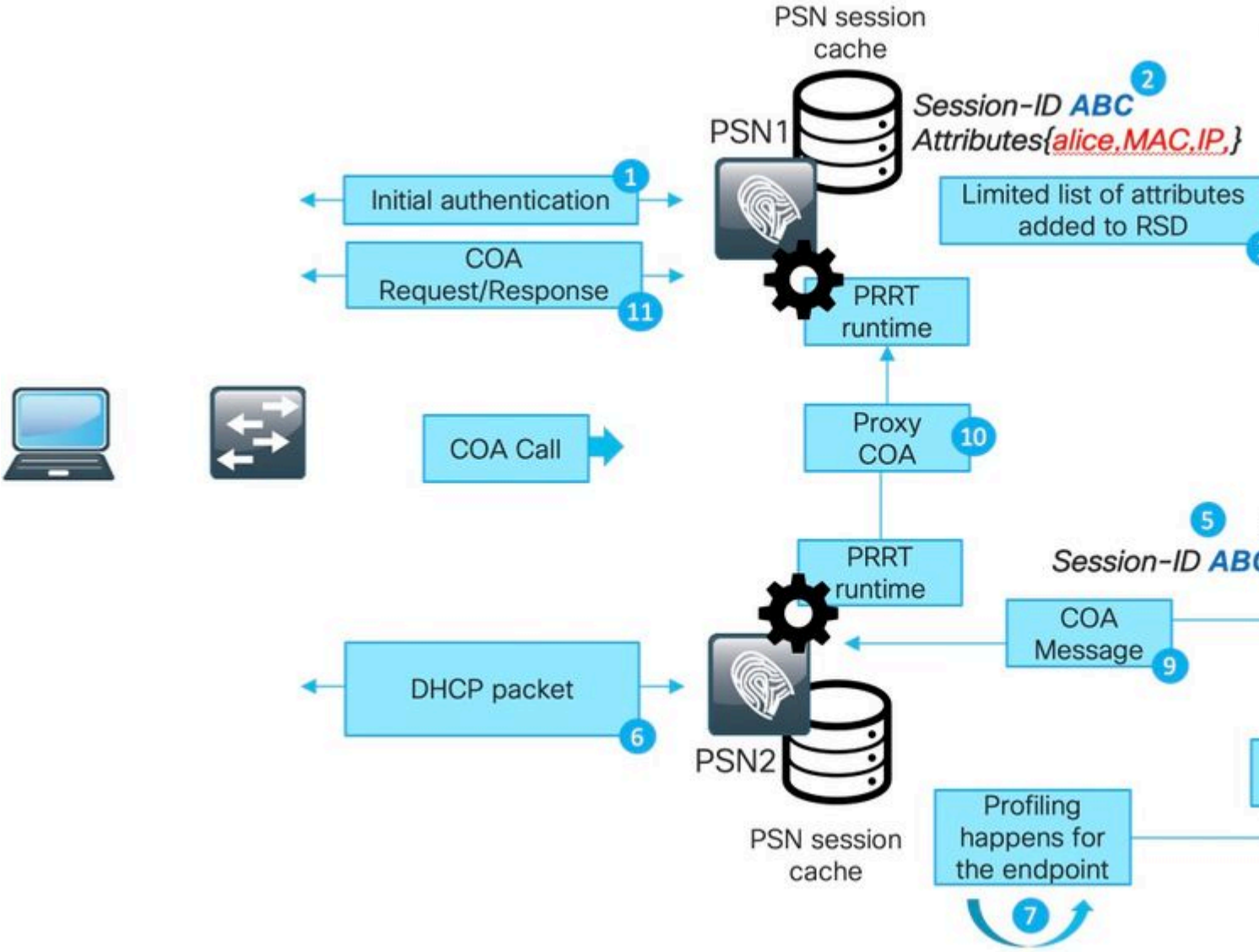
Light Data Distribution Architecture

Questa funzionalità contiene i seguenti elementi:

- Cache Radius Session Directory (RSD) - questa cache esiste su ogni nodo ISE e memorizza tutte le sessioni attive presentate nell'implementazione ISE. Ogni sessione dispone di una quantità limitata di attributi nella cache. Esempi di attributi memorizzati nella directory di sessione Radius per ciascuna sessione:
    - ID sessione.
    - MAC endpoint.
    - CallingStationID.
    - Endpoint IP.
    - IP PSN - PSN in cui è stata eseguita l'autenticazione.
    - FQDN PSN - come sopra.
    - Indirizzo IP-NAS.
    - Indirizzo NAS-IPv6.
    - Stato: Autenticato, Avviato, Arrestato.
- RabbitMQ exchange - Si è formato uno scambio in cui il publisher, la coda correlata e il consumer vengono presentati su ogni nodo nell'implementazione ISE. Ciò assicura che la topologia a maglia completa si formi tra tutti i nodi ISE.
- Autore: la directory di sessione Radius rappresenta un autore. Quando una nuova autenticazione elaborata correttamente da PSN viene creata una nuova sessione nella cache della sessione PSN. Per questa sessione, nella directory di sessione Radius viene inserito un set limitato di attributi.
- Consumer - su tutti gli altri nodi Radius Session Directory rappresenta un consumer.

Nota: la terminologia e l'architettura generale di RabbitMQ non rientrano in questo ambito del documento.

Nella figura viene illustrato il funzionamento del flusso del certificato di autenticità (COA) con la cache RSD:



1. L'autenticazione iniziale viene eseguita con PSN1.

2. Sessione ABC creata nella cache della sessione.

3. Gli attributi obbligatori vengono salvati in RSD.

4. Sessione condivisa su RabbitMQ con tutti gli altri nodi ISE.

5. La sessione viene creata nella cache RSD su tutti i nodi ISE.

6. Nuovi dati del profilo ricevuti su PSN2.

7. L'endpoint viene riprofilato e, in caso di modifica che richiede l'esecuzione del certificato di autenticità (COA), PSN2 procede con il passaggio successivo.

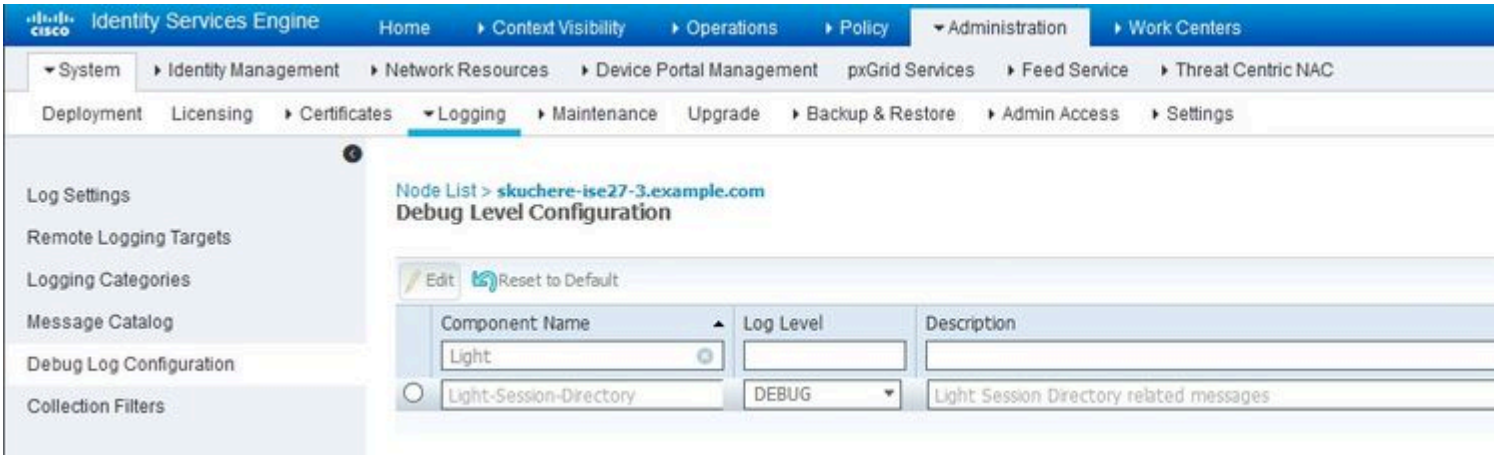
8. Chiamata API interna inviata alla cache RSD per eseguire il processo COA.

9. Dati dalla cache RSD utilizzati per preparare un messaggio COA proxy (un COA che va da un nodo ISE a un altro, contiene tutti i dettagli che il nodo di destinazione può utilizzare per inviare una richiesta CAO a NAD). Il messaggio COA viene prima trasferito internamente a PRT Runtime (server AAA effettivo all'interno di ISE).

10. PSN2 invia un messaggio COA a PSN1.

11. PSN1 invia un messaggio COA a NAD.

Per risolvere i problemi di comunicazione su LDD sull'ISE, è possibile abilitare il componente **Light Session Director** nel comando DEBUG:



esempio di messaggio di debug dal file lsd.log per la creazione e la pubblicazione di sessioni nel PSN originale:

```
DEBUG  [pool-45-thread-6][] cisco.cpm.lsd.service.LSDRedisClient -:::::- Mapping Session ID 0a3e949800000

DEBUG  [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.LSDNetAccessEventListener -:::::- Publishing sessi

DEBUG  [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.SessionPublisher -:::::- Forwarding session 07a26b
```

Su tutti gli altri nodi ISE, è possibile vedere come è stata usata una sessione:

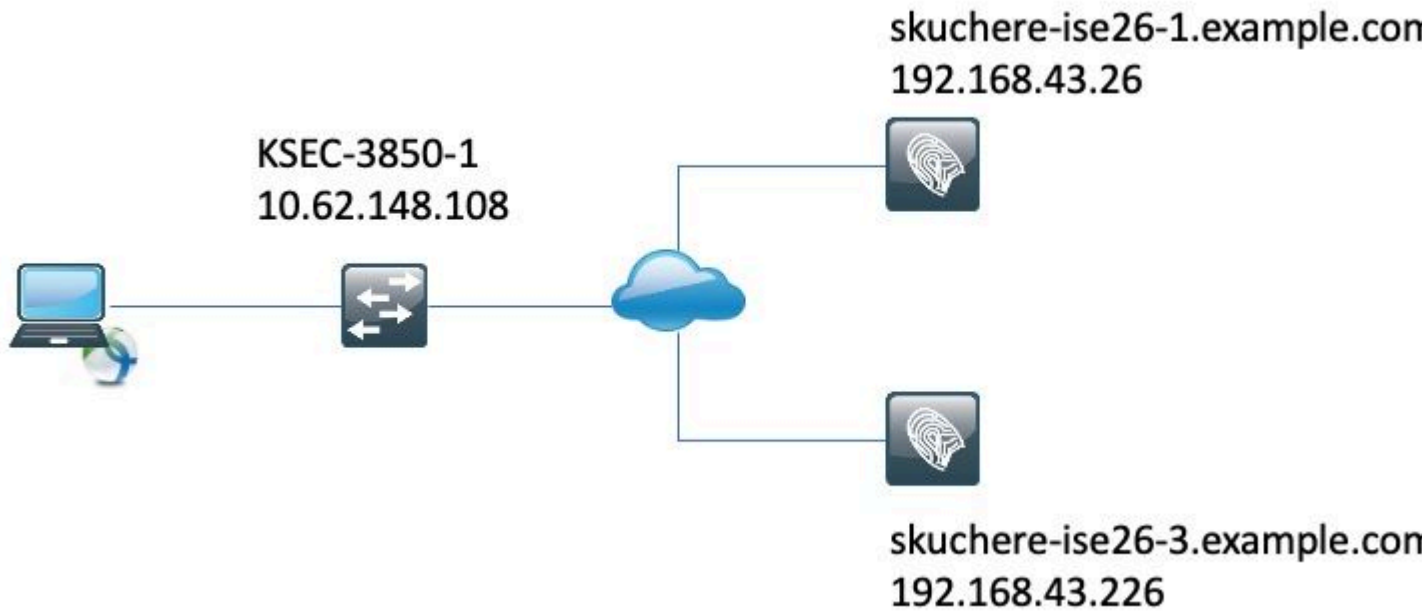
```
[pool-35-thread-38][] cisco.cpm.lsd.service.SessionConsumer -:::::- Consumer is processing : sessionID:[0
```

Condivisione dello stato di postura su RSD

La condivisione dello stato di postura tra i nodi risolve il problema che presenta il sintomo simile a 'Il modulo di postura AnyConnect ISE è conforme mentre lo stato della sessione su ISE è in sospeso' quando la causa principale è una sessione non aggiornata/fantasma o una riautenticazione su un numero PSN diverso con un ID sessione originale che non ha attivato il riavvio del rilevamento. Non appena la sessione diventa conforme, queste informazioni vengono inserite nell'RSD della sessione e in seguito possono essere utilizzate da ogni PSN della distribuzione.

La feature descritta non è ancora in grado di risolvere altri problemi d'angolo. Ad esempio, uno scenario in cui NAD esegue la riautenticazione sullo stesso PSN ma con un ID sessione diverso. Tali scenari possono essere gestiti seguendo le procedure ottimali descritte nel presente documento.

La figura mostra la topologia utilizzata per un test di condivisione dello stato della postura:



Condivisione dello stato di postura su RSD - Sessione non aggiornata/fantasma

Per creare una sessione obsoleta, l'autenticazione è stata inizialmente eseguita sullo skuchere-ise26-1 e versioni successive. NAD è stato riconfigurato per inviare l'accounting allo skuchere-ise26-3. Dopo che un messaggio di accounting è stato inoltrato al PSN errato ed è stato riconfigurato per inviare l'accounting allo skuchere-ise26-1.

La figura mostra una relazione contabile che prova la presenza della sessione fantasma su skuchere-ise26-3:

Stop	3.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1
Interim-Update	2.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-3
Start	1.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1

1. Messaggi Accounting-Start elaborati da skuchere-ise26-1.

2. Contabilità provvisoria-Aggiornamento per la stessa sessione elaborato da skuchere-ise26-3.

3. La sessione si concluderà in seguito con il skuchere-ise26-1.

Dopo qualche tempo, l'endpoint si connette nuovamente alla rete ma il reindirizzamento non funziona più. Nel file guest.log di PSN - skuchere-ise26-3 è possibile visualizzare questi messaggi di log con il componente **client-webapp** abilitato in DEBUG:

```
2020-04-08 13:30:48,217 DEBUG [https-jsse-nio-192.168.43.226-8443-exec-4][] cisco.cpm.client.posture.Uti
```

Quando il PSN rileva che contiene una sessione non aggiornata/fittizia per l'endpoint, non risponde al modulo di postura ISE e ciò consente di ottenere la risposta corretta dal PSN in cui è stata eseguita l'ultima autenticazione.

Come soluzione al problema di sessione obsoleta/fantasma ora al momento della ricerca della sessione, il

PSN controlla la presenza di una nuova sessione per l'endpoint nell'RSD. Se RSD contiene un ID di sessione diverso da quello di PSN nella cache di sessione locale, si presume che la sessione presentata nella cache di sessione sia obsoleta.

Condivisione dello stato di postura su RSD - Failover tra PSN

Per riprodurre questo scenario, è stato abilitato un timer di riautenticazione breve nel profilo di autorizzazione assegnato all'endpoint nello stato conforme. In seguito NAD è stato riconfigurato per inviare l'autenticazione e l'accounting a un altro PSN (skuchere-ise26-3). Alla scadenza del timer di riautenticazione, la stessa sessione è stata non autenticata sul diverso numero PSN.

La figura mostra un report di autenticazione che mostra il failover per la sessione sana da skuchere-ise26-1 a skuchere-ise26-3:

1. L'autenticazione avviene su skuchere-ise26-1, il profilo di autorizzazione con reindirizzamento è assegnato.

2. Costo del lavoro dopo una valutazione positiva della postura.

3. Autenticazione successiva quando viene assegnato il profilo di autorizzazione per lo stato di conformità.

4. L'autenticazione ha raggiunto un numero PSN diverso ma ottiene comunque il profilo di autorizzazione per lo stato di conformità.

La sessione ottiene lo stato di conformità sul nuovo PSN dopo il failover in ise-psc.log con i componenti **epm-pip** e **nsf-session** abilitati in DEBUG:

<#root>

```
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -:::::-
```

Looking up session 0A3E946C000000896011D045 for attribute Session Session.PostureStatus

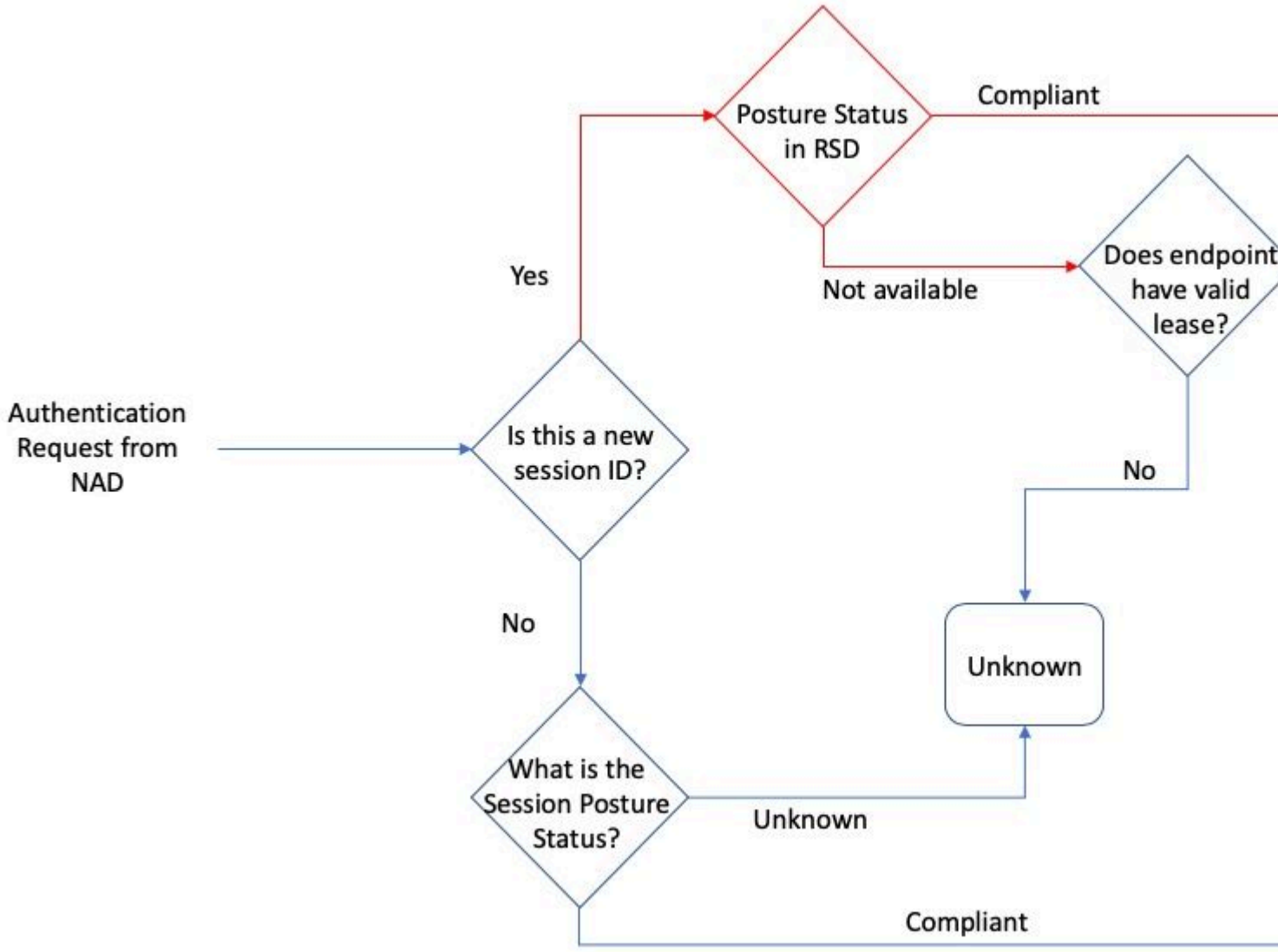
```
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution cont
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP com
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution cont
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::- Looking up sessio
2020-04-09 11:06:42,176 DEBUG [SessionLifecycleNotifier][] cpm.nsf.session.internal.LRUAgingAlogrithm -:
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::- Returning for ses
IndexValues: {}

2020-04-09 11:06:42,177 DEBUG [Thread-7979][] cisco.cpm.posture.pip.PostureStatusPIP -::::-
```

set postureStatus based on posture LSD dictionary: Compliant

```
2020-04-09 11:06:42,177 DEBUG [Thread-7979][] cisco.cpm.posture.pip.PostureStatusPIP -::::-
```

PostureStatusPIP for mac 00-50-56-B6-0B-C6 - Attribute Session.PostureStatus value is Compliant

Il problema originale è stato risolto con l'aggiunta di una logica supplementare nel processo di selezione dello stato della postura. La figura mostra ciò che è stato modificato (le modifiche sono evidenziate in rosso):



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).