Probleemoplossing voor ISE-sessiebeheer en -houding

Inhoud

Inleiding

Dit document beschrijft het probleem met de gemeenschappelijke posterijen van Identity Service Engine (ISE): **"AnyConnect ISE-postermodule toont compatibele..."**

Achtergrondinformatie

Dit document beschrijft het probleem met de gemeenschappelijke posterijen van Identity Service Engine (ISE) - **AnyConnect ISE-postermodule toont compatibiliteit terwijl de sessiestatus van ISE in behandeling is.**

Hoewel de symptomen altijd hetzelfde zijn, kunnen er meerdere grondoorzaken van dit probleem zijn.

Vaak wordt het oplossen van problemen bij een dergelijk probleem extreem tijdrovend, wat ernstige gevolgen heeft.

Dit document verklaart:

- Probleemmanifestatie vanuit het perspectief van de eindgebruiker en de beheerder van ISE.
- Gemeenschappelijke problematische scenario's.
- De theorie achter ISE, AnyConnect en netwerkbewerkingen die het probleem veroorzaken.
- Algoritmen voor snelle probleemidentificatie.
- Klassieke oplossingen voor veelvoorkomende probleemscenario's.
- Posture status delen via de Radius sessiemap.

Voor een betere uitleg van de later beschreven concepten raadpleegt u:

[ISE-poortstijlvergelijking voor Pre en Post 2.2](#)

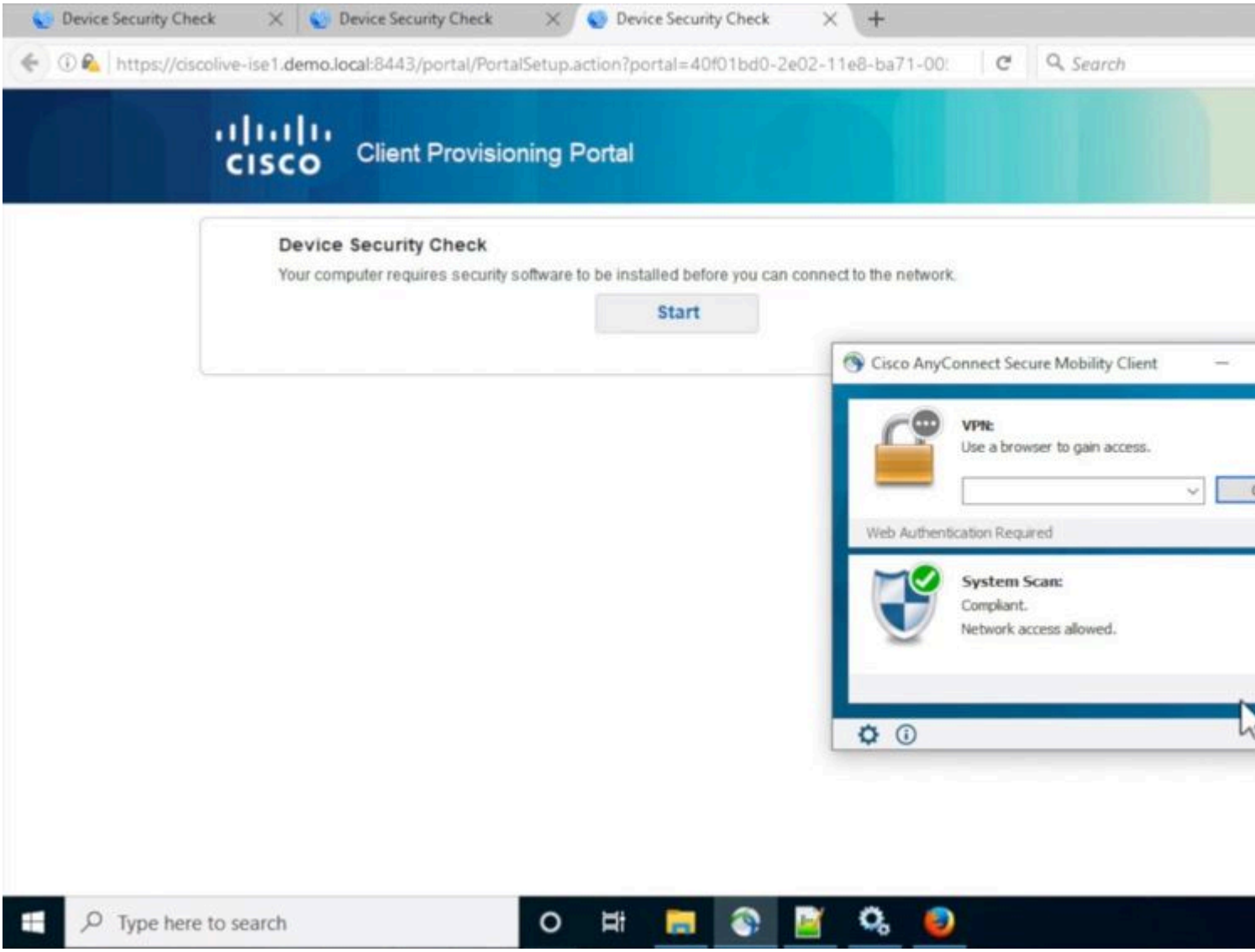
[ISE onder het vergrootglas. Hoe problemen met ISE op te lossen - BRKSEC-3229](#)

Probleem

Ervaring voor eindgebruiker

Deze kwestie komt normaal gesproken tot uiting in het ontbreken van netwerktoegang of constante omleidingen naar het ISE-client provisioningportal in de browser, terwijl tegelijkertijd AnyConect ISE-postermodule posterstatus als **conform** toont**.**

Typische eindgebruikerservaring:

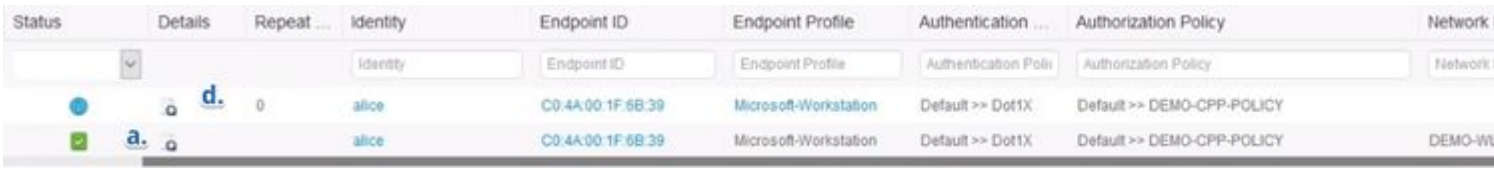


ISE-beheerervaring

Normaal, in eerste triage van deze kwestie, voert ISE admin Radius Live logboeken onderzoek uit om ervoor te zorgen dat er een daadwerkelijke authenticatie is die de ISE raakt.

Het eerste symptoom dat in deze fase wordt ontdekt wijst op een wanverhouding in een postuur status tussen endpoint en ISE zoals in de bewegende logboeken of de rapporten van de Radiusverificatie laatste succesvolle authentificatie voor het eindpunt toont **Hangende** postuur status.

Typische ISE-beheerervaring:



- Laatste succesvolle verificatie voor Alice.
- De status van de sessie is **hangend.**
- Laatste sessie voor Alice.
- De sessie gebeurtenis toont de status van de houding als **conform.**

> **Opmerking**: c. en d. worden niet altijd in de bewegende logbestanden getoond wanneer de beschreven kwestie zich manifesteert. Session event met postuur status **Compliant** is gebruikelijker voor scenario's die worden veroorzaakt door de verouderde of spooksessies die later in dit document worden beschreven.

Veelvoorkomende probleemscenario's

Deze kwestie manifesteert zich normaal in twee problematische scenario's en elk van hen heeft meerdere grondoorzaken. De scenario's:

- AnyConnect ISE-postermodule is tijdens het posteringsproces waarbij de verkeerde posteringstatus werd weergegeven, verkeerd geïnformeerd door het Policy Service Node (PSN). In dit geval behandelen we normaal gesproken een verouderde of spooksessie in het PSN-sessiecache.
- AnyConnect ISE toont de status van de vorige detectiecyclus omdat de huidige verificatie geen detectieproces heeft geactiveerd. ISE postermodule in AnyConnect heeft een beperkt aantal gebeurtenissen die het detectieproces activeren en mogelijk dat tijdens de verificatie of herverificatie geen van deze gebeurtenissen is gedetecteerd.

Probleem met statische/spooksessie

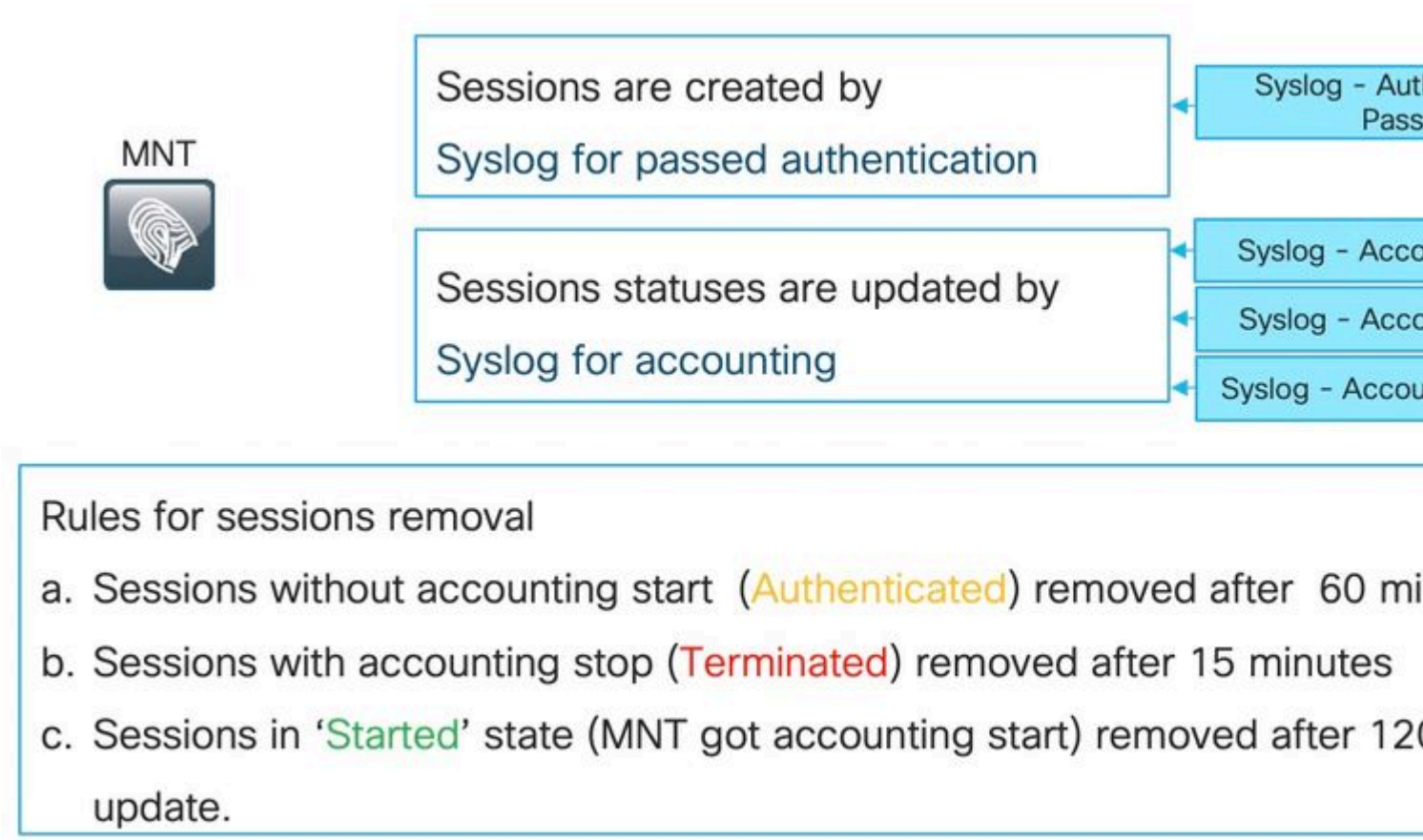
Om het probleem beter te begrijpen, moet u de ISE-sessiebeheerlogica en het AnyConnect-detectieproces onderzoeken.

ISE-sessiebeheerlogica

In ISE-implementatie zijn twee personen verantwoordelijk voor het sessiebeheerproces: PSN en Monitoring Node (MNT).

Om dit probleem goed op te lossen en te identificeren, is het van cruciaal belang om de theorie van sessiebeheer op beide persona's te begrijpen.

MNT- en sessiebeheer



Zoals uitgelegd in deze afbeelding, MNT-knooppunt maakt seizoenen op basis van de doorgegeven authenticatie Syslog-berichten die afkomstig zijn van PSN's.

De latere sessiestatus kan door de Syslog worden bijgewerkt voor de boekhouding.

Session verwijdering op MNT gebeurt in 3 scenario's:

- Sessies zonder accounting beginnen ongeveer 60 minuten nadat ze zijn gemaakt. Er wordt elke 5 minuten een foute taak uitgevoerd om de sessiestatus te controleren en te reinigen.
- Afgesloten sessie verwijderd ongeveer 15 minuten nadat de accounting stop is verwerkt door dezelfde cron job.
- Dezelfde cron op elke uitvoering verwijdert ook sessies die meer dan 5 dagen (120 uur) in de 'Started' staat zijn geweest. Een begintoestand betekent dat de MNT-knooppunt zowel verificatie als accounting verwerkt om Syslog voor de sessie te starten.

Voorbeelden van Syslog-berichten van PSN. Die berichten worden ingelogd op poortserver.log wanneer runtime-aaa component is ingeschakeld in DEBUG. De delen in vet kunnen worden gebruikt om onderzoek regelmatige uitdrukkingen te construeren.

Verificatie succesvol doorlopen:

<#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

Begin 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

Voorlopige boekhoudkundige bijwerking :

<#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

Boekhoudstop :

<#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

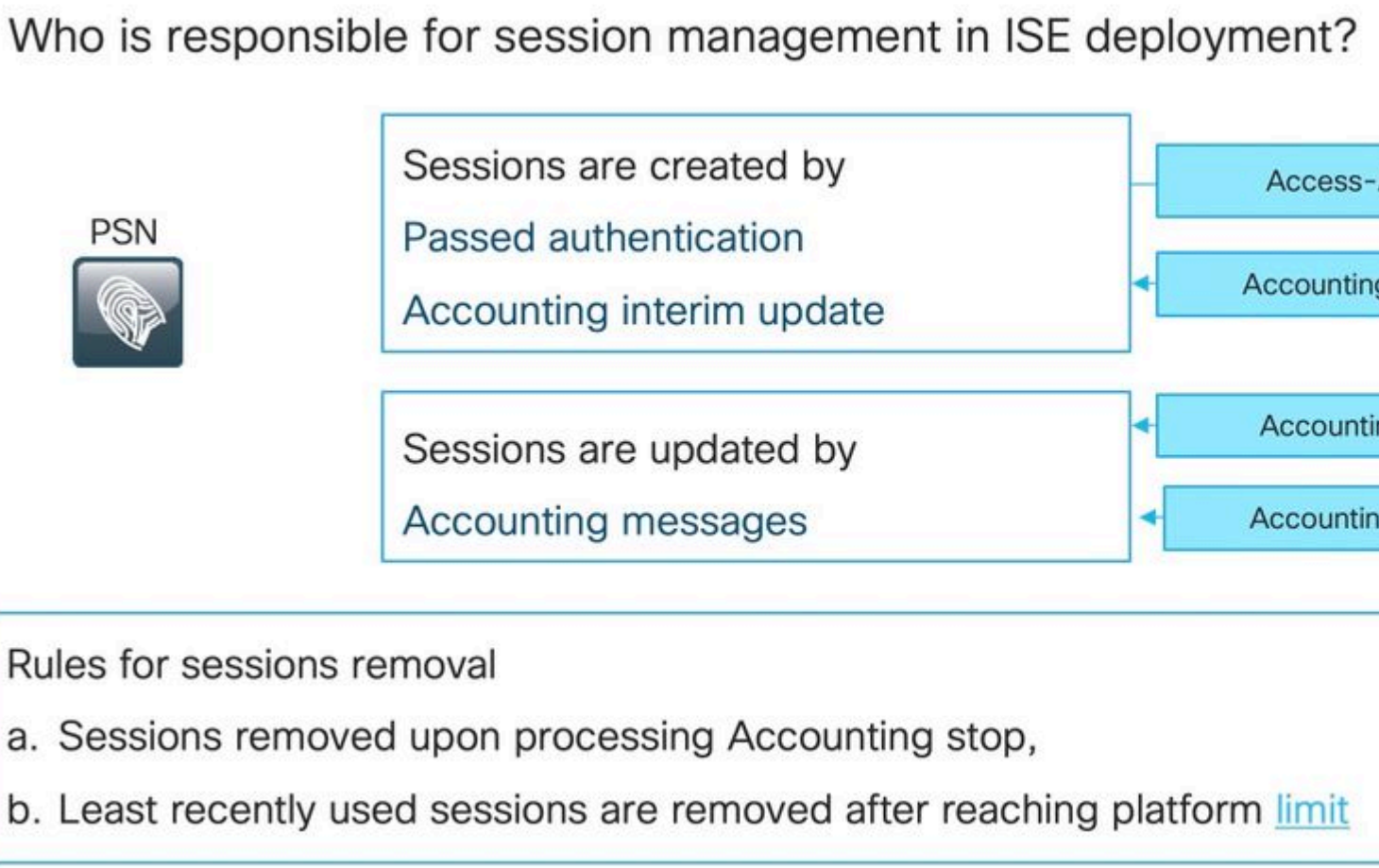
PSN- en sessiebeheer

Wat is het PSN-sessiecache?

Een in-memory database die alle actieve sessies van specifieke PSN opslaat. Session cache is altijd lokaal voor de node en er is geen mechanisme in ISE dat replicatie van de volledige sessiestatus van de ene knooppunt naar de andere kan uitvoeren.

Voor elke actieve sessie-ID slaat PSN alle attributen op die tijdens de verificatie-/autorisatiefase zijn verzameld, zoals interne/externe gebruikersgroepen, NAD-kenmerken (Network Access Device), certificaatkenmerken, enzovoort. Deze kenmerken worden door PSN gebruikt om verschillende beleidstypen te selecteren, zoals Verificatie, autorisatie, clientprovisioning, houding.

Session cache volledig verwijderd wanneer services op het knooppunt of knooppunt zelf opnieuw worden gestart.



De huidige logica van de zittingsverwerking leidt tot een nieuwe ingang in het zittingsgeheim in twee scenario's, kunnen de recentere details van bestaande zittingen van boekhoudingsberichten worden bijgewerkt die uit NADs komen:

- De sessie is op het PSN geverifieerd.
- PSN kreeg een tussentijdse boekhoudkundige update voor de sessie die niet bestaat in het sessiecache.

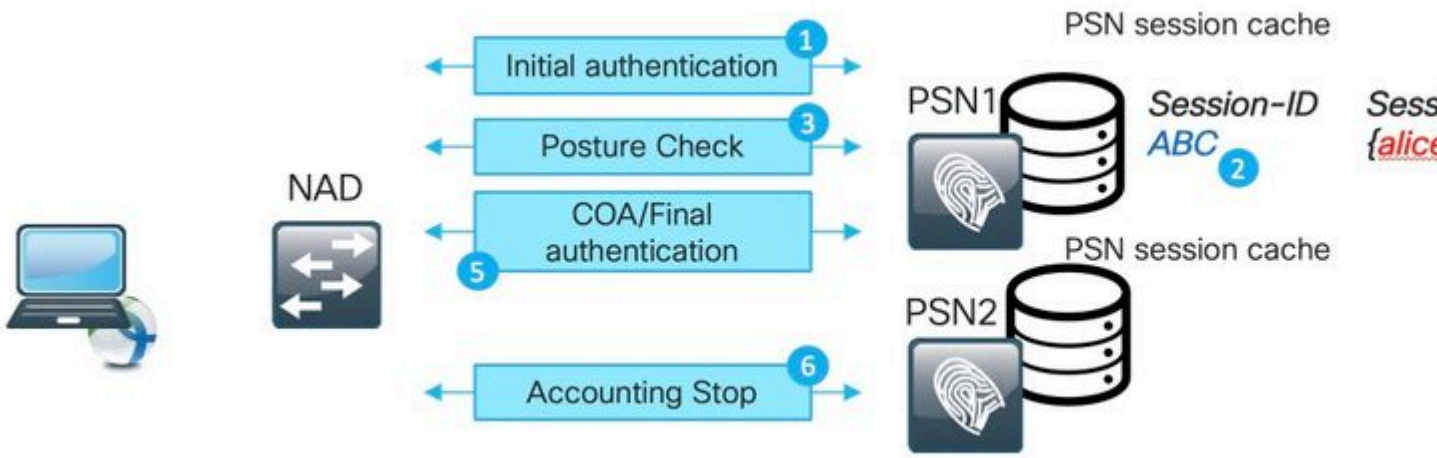
Als het gaat om sessieverwijdering, implementeert PSN deze logica:

- Session cache-ingang verwijderd onmiddellijk na verwerking van het accounting stop bericht.
- PSN begint de minst recent gebruikte sessies te verwijderen wanneer een knooppunt **de limiet** van actieve sessies bereikt.

Verouderde sessie op PSN

Bij ISE-implementatie is de boekhoudstop voor een bestaande sessie verwerkt door de PSN, die de werkelijke verificatie niet heeft uitgevoerd:

Voorbeeld van de vervelende sessie:



1. Succesvolle verificatie vindt plaats op PSN voor ABC-sessie.

2. PSN maakt een ingang in het sessiecache.

3. Houdbaarheidsbeoordeling vindt plaats.

4. Sessie gemarkeerd als **conform**.

5. Een wijziging van de autorisatie (COA) die wordt veroorzaakt door een wijziging van de status leidt tot een nieuwe authenticatie van het eindpunt om het volgende toegangsniveau toe te passen.

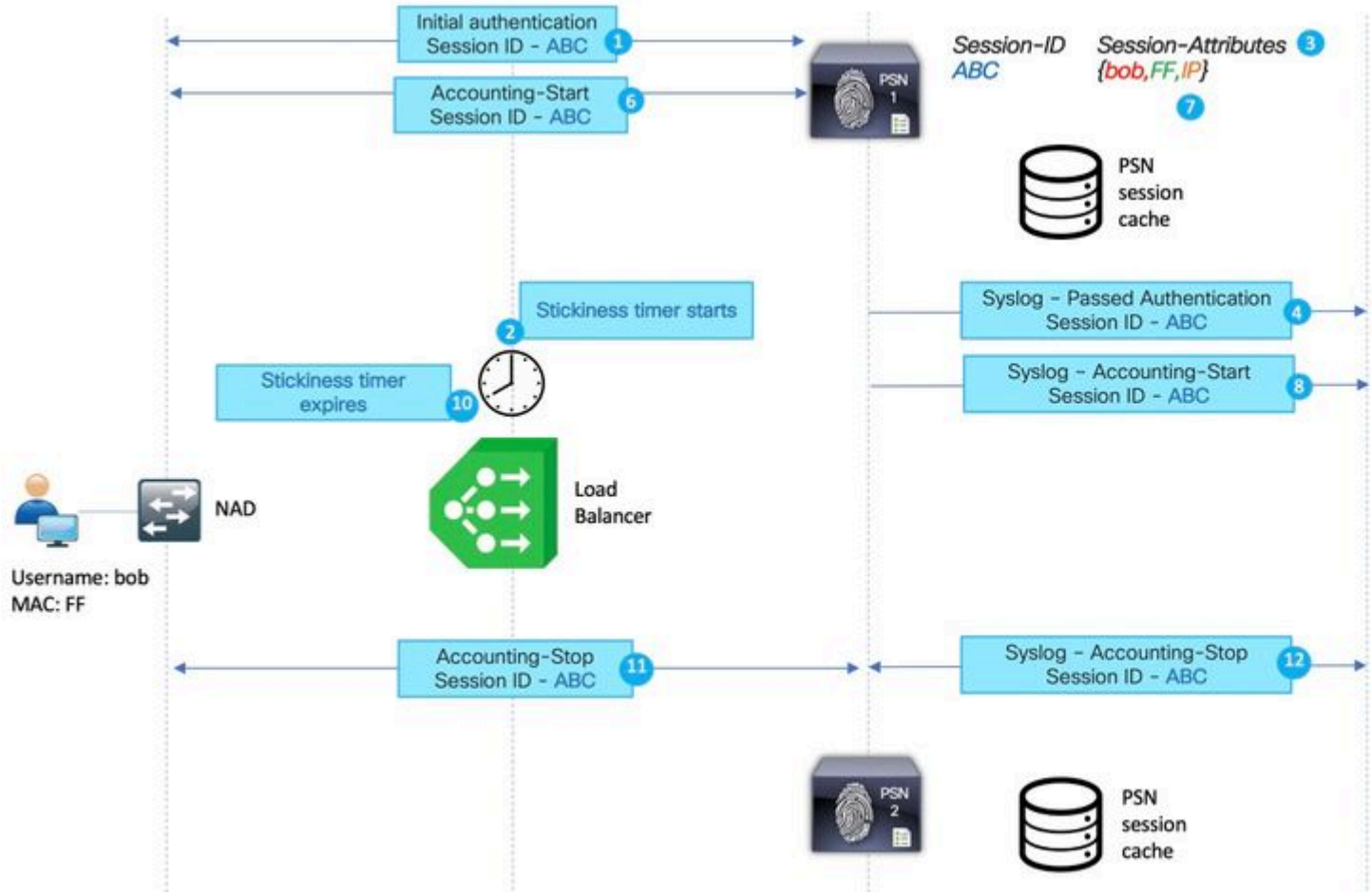
6. Accounting stop voor sessie ABC komt naar PSN2.

Na stap 6 sessie, wordt ABC vastgezet in de verbale status op de PSN1 omdat er geen accounting stop bericht verwerkt op dit PSN om het te verwijderen. De sessie wordt lange tijd verwijderd als de implementatie geen hoge aantal verificatiepogingen ondervindt.

De verouderde sessie verschijnt in het PSN-sessiecache in deze scenario's:

- De boekhoudstop kwam tot de verkeerde PSN toe te schrijven aan het verloop van de stickiness tijdopnemer op de ladingsverdeler.
- De verkeerde configuratie op het NAD is niet dezelfde PSN geconfigureerd voor verificatie en accounting.
- Tijdelijke connectiviteitsproblemen op het netwerkpad dat NAD-failover naar het volgende PSN veroorzaakt.

Voorbeeld van een verouderde sessie in een taakverdeling (LB)-omgeving:



1. Eerste verificatie voor de sessie ABC uitgevoerd door PSN 1.

2. Met deze verificatie wordt een kleverheidstimer op de taakverdeling gestart.

3. PSN 1 maakt een ingang voor de sessie ABC in de lokale cache.

4. Syslog-bericht voor doorgegeven verificatie naar MNT-knooppunt.

5. Inschrijving voor sessie ABC gemaakt in MNT sessiemap met de status **Geverifieerd**.

6. Boekhoudkundige start-bericht voor sessie ABC landt op PSN 1.

7. Session cache-ingang voor sessie ABC bijgewerkt met informatie van Accounting-Start.

8. Syslog-bericht voor accounting-start overgebracht naar MNT-knooppunt.

9. Sessiestatus bijgewerkt naar **Starten**.

10. De kleverheidstimer verloopt op de taakverdeling.

11. Accounting-Stop voor sessie ABC door de taakverdeler doorgestuurd naar PSN 2.

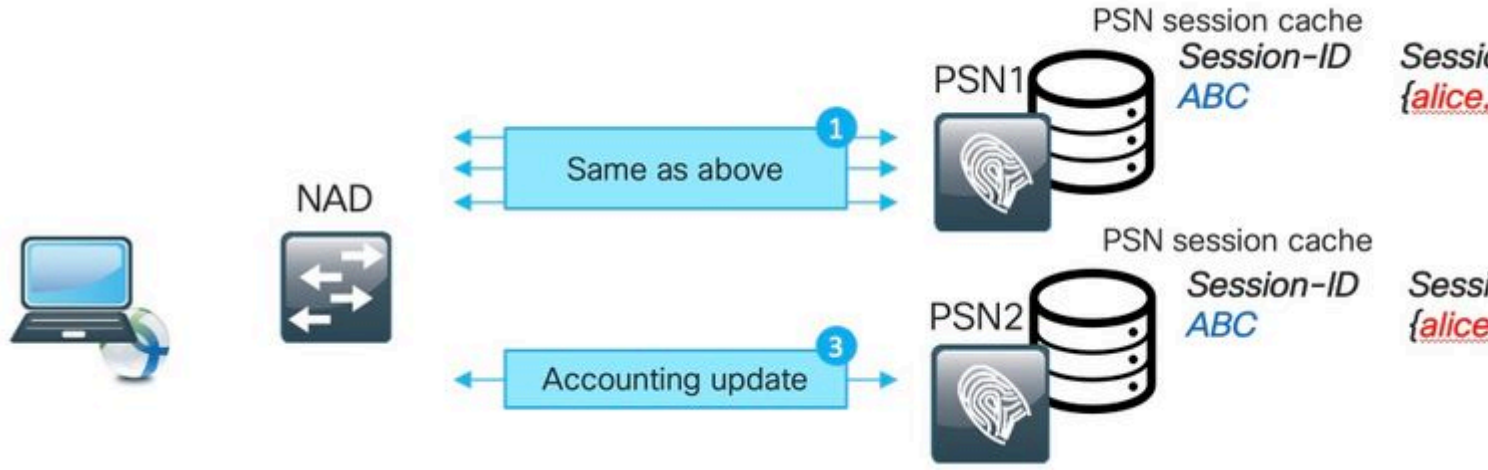
12. Syslog-bericht voor accounting-stop doorgestuurd door PSN 2 naar MNT.

13. Sessie ABC gemarkeerd als beëindigd op MNT.

Fantoomsessie op het PSN

De fantoomsessie is een scenario wanneer de tussentijdse boekhoudkundige update naar de PSN komt die geen verificatie voor deze specifieke sessie uitvoerde. In dit scenario wordt een nieuwe ingang gecreëerd in het PSN-sessiecache en als PSN geen accountingstop-bericht krijgt voor deze sessie, wordt de ingang niet verwijderd tenzij PSN de limiet van actieve sessies bereikt.

Voorbeeld van de fantoomsessie:



1. Dezelfde stappen als beschreven in het voorbeeld van een verouderde sessie vindt plaats op PSN1 voor de sessie ABC.

2. Session ABC heeft een status **conform** in het PSN1-sessiecache.

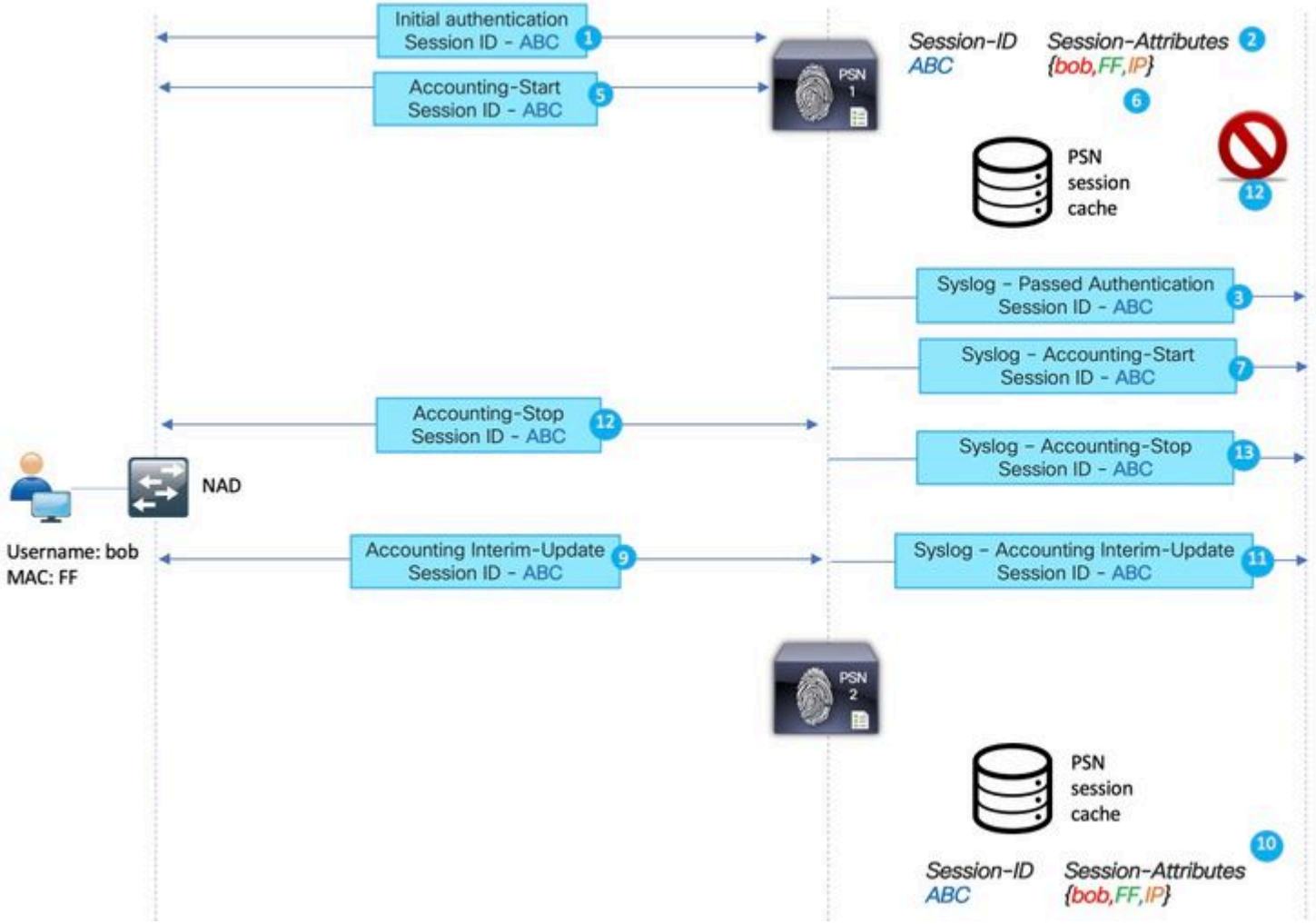
3. Accounting tussentijdse update voor sessie ABC hits PSN2.

4. Session entry voor sessie ABC gemaakt op PSN2. Sinds de sessie die is gemaakt op basis van het rekeningbericht, heeft het een beperkt aantal attributen. Posterstatus is bijvoorbeeld niet beschikbaar voor ABC-sessie. Ook zaken als gebruikersgroepen en andere specifieke kenmerken van vergunningen ontbreken.

De spooksessie verschijnt in het PSN-sessiecache in deze scenario's:

- Korte onderbreking van de netwerkdoorvoer.
- Misbruik van netwerktoegangsapparaat.
- Fout bij gedrag of verkeerde configuratie bij taakverdeling.

Voorbeeld van een spooksessie voor het scenario met tijdelijke problemen op het netwerkpad naar PSN1:



1. Eerste verificatie voor de sessie ABC uitgevoerd door PSN.

2. PSN1 maakt een ingang voor de sessie ABC in de lokale cache.

3. Syslog-bericht voor doorgegeven verificatie naar MNT-knooppunt.

4. Inschrijving voor sessie ABC gemaakt in TimesTen DB met de staat **Geverifieerd**.

5. Boekhoudkundige start-bericht voor sessie ABC landt op PSN 1.

6. Session cache-ingang voor sessie ABC bijgewerkt met informatie van Accounting-Start.

7. Syslog-bericht voor accounting-start overgebracht naar MNT-knooppunt.

8. Sessiestatus bijgewerkt naar **Starten**.

9. Tussentijdse bijwerking van de boekhouding voor de sessie die ABC naar PSN2 doorstuurde.

10. PSN2 maakt een ingang voor de sessie ABC in de lokale cache.

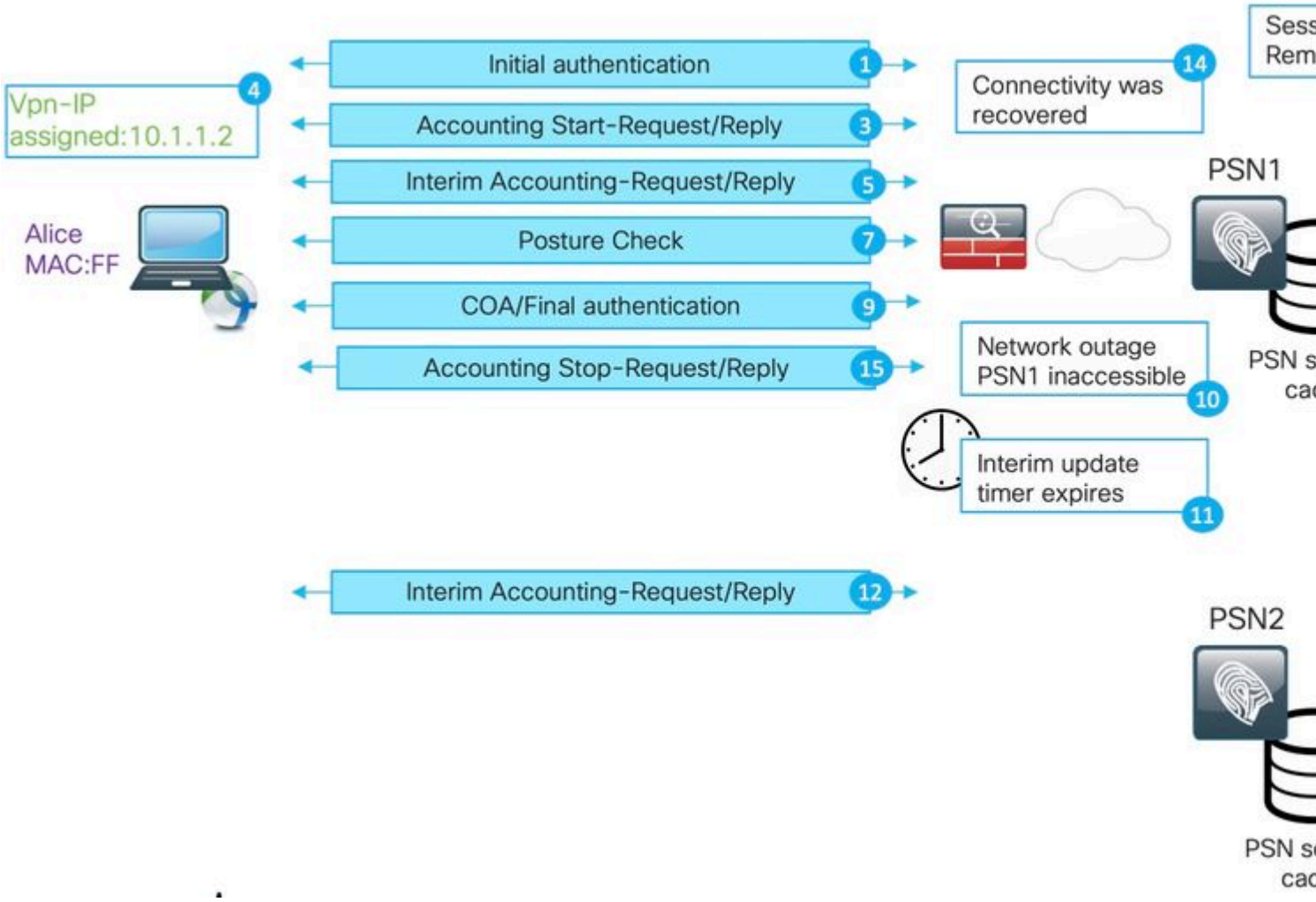
11. Accounting-Stop voor sessie die ABC doorstuurt naar PSN1.

12. Inschrijving voor sessie ABC verwijderd uit de sessiecache op PSN1.

13. Syslog-bericht voor accounting-stop doorgestuurd door PSN 1 naar MNT.

14. Sessie ABC gemarkeerd als beëindigd op MNT.

Het scenario van de fantoomsessie zoals deze is gemaakt voor de langdurige VPN-verbinding:



1. Eerste verificatie op PSN1.

2. Session ABC gemaakt in het sessiecache.

3. De boekhouding begint het bericht dat door PSN wordt verwerkt.

4. Het nieuwe IP-adres dat is toegewezen aan de adapter Virtual Private Network (VPN).

5. Tussentijdse boekhoudkundige update met IP-adresinfo landt op PSN.

6. IP-adresinformatie toegevoegd aan het sessiecache.

7. Bij PSN1 vindt een bepaling van de houding plaats.

8. De status van de post wordt bijgewerkt in de sessie.

9. COA push uitgevoerd door ISE, dit leidt tot nieuwe toegangsniveau toe te wijzen.

10. Uitval op het netwerkpad waardoor PSN1 niet toegankelijk is.

11. Na het verstrijken van het interim-updateinterval detecteert ASA/FTD dat PSN1 ontoegankelijk is.

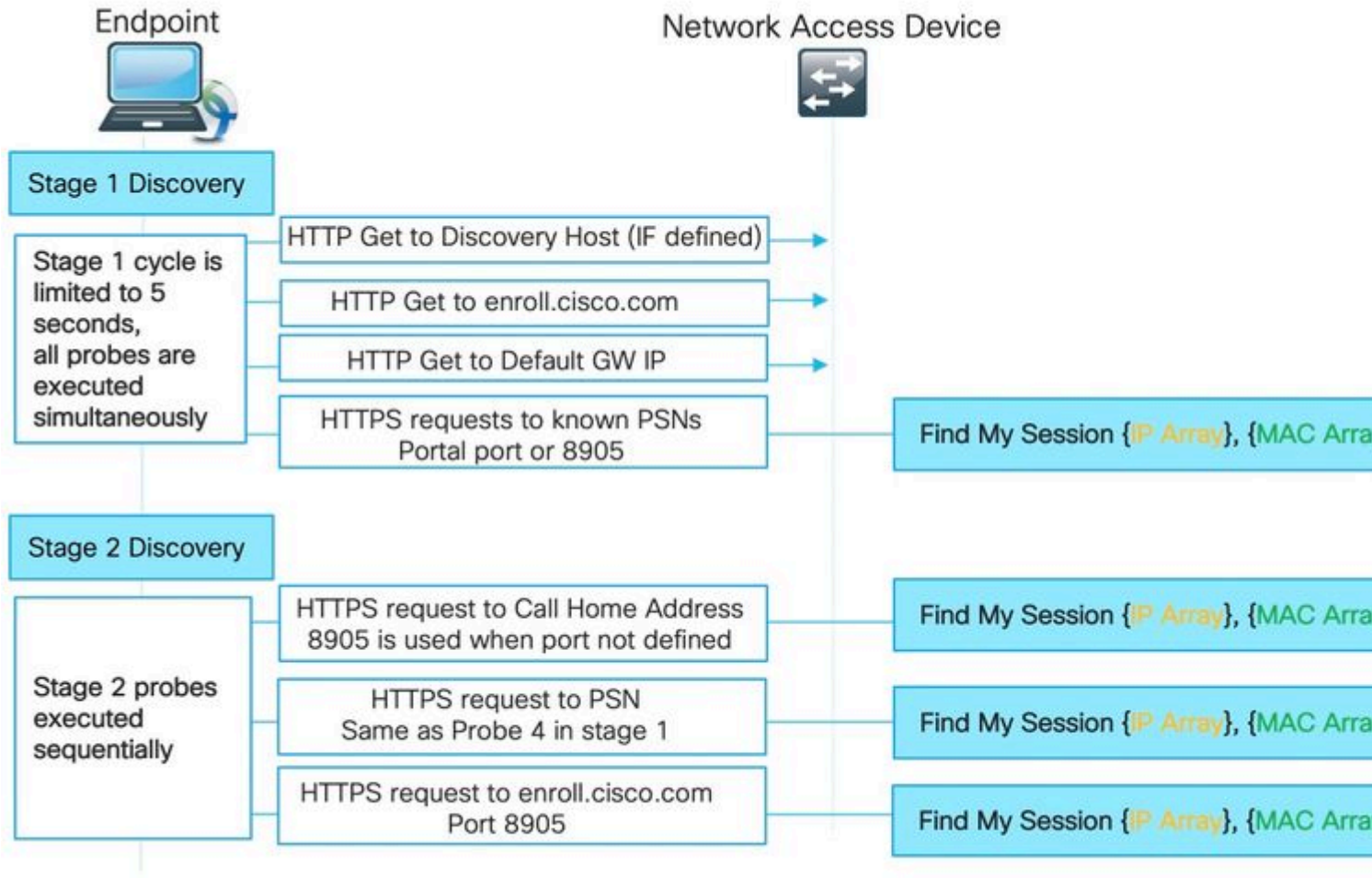
12. Tussentijdse boekhoudkundige update komt naar PSN2.

13. De fantoomsessie die in het PSN2-sessiecache is gemaakt.

Als later PSN1 toegankelijk wordt (14) worden alle volgende boekhoudberichten doorgestuurd (15,16) en blijft ABC voor een onbepaalde tijd in het PSN2-sessiecache.

Hoe oud Sessies en spooksessie het postuur-proces doorbreken?

Om te begrijpen hoe de verouderde sessie en de spooksessie de houding verbreken, kunt u het AnyConnect ISE-proces voor het detecteren van de poortmodule bekijken:



Fase 1 ontdekking :

Tijdens deze fase, de postuur module van ISE 4 gelijktijdige problemen om van PSN te vinden die een authentificatie voor het eindpunt uitvoerden.

Eerst worden 3 sondes in de figuur omgeleid op basis van (standaard GW IP. IP van de ontdekkingsgastheer (indien bepaald) en enroll.cisco.com IP) - Die sondes richten altijd de agent aan het recht PSN aangezien de omleiding URL wordt genomen van NAD zelf.

Probe nummer 4 wordt naar alle primaire servers verzonden die in het **ConnectionData.xml-**bestand worden gepresenteerd. Dit bestand dat is gemaakt na de eerste succesvolle poging tot postuur en latere bestandsinhoud kan worden bijgewerkt als client migreert tussen PSN's. Op Windows-systemen is de bestandslocatie - **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.**

Aangezien alle fase 1 sondes gelijktijdig worden uitgevoerd, wordt resultaat van sonde 4 gebruikt slechts als alle andere 3 sondes ontbraken of de module van de post van ISE niet in staat was om juiste communicatie met PSN te vestigen die in redirect URL binnen 5 seconden is teruggekeerd.

Wanneer sonde 4 landt op de PSN bevat het een lijst van actieve IP en MAC adressen die op het eindpunt worden ontdekt. PSN gebruikt deze gegevens om een sessie voor dit eindpunt te vinden in de lokale cache. Als PSN een verouderde of fantoomsessie voor eindpunt heeft, kan dit resulteren in een verkeerde houding status die later op de client-side wordt weergegeven.

Wanneer een agent meerdere antwoorden krijgt voor sonde 4 (**ConnectionData.xml** kan meer dan één primaire PSN bevatten) wordt het snelste antwoord altijd gebruikt.

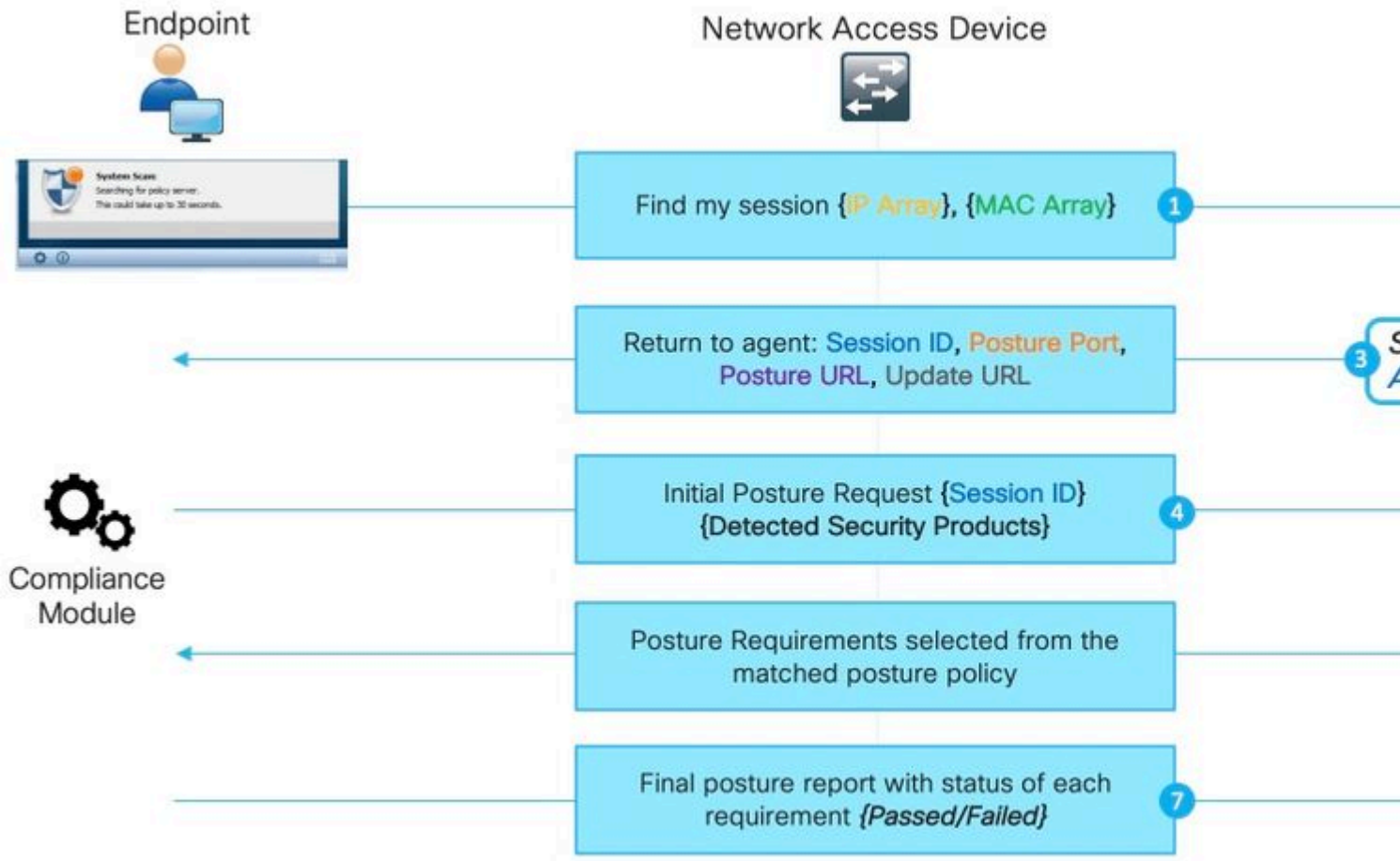
Detectie fase 2:

Alle fase 2 detectiesondes zijn redirect-less wat betekent dat elke sonde een sessie-lookup op de bestemming PSN teweegbrengt. Als PSN de sessie niet kan vinden in het lokale sessiecache, moet het MNT lookup uitvoeren (alleen op MAC-adres gebaseerd) om een sessieeigenaar te vinden en de naam van de eigenaar terug te geven aan de agent.

Aangezien alle sondes sessieraadpleging veroorzaken, kan fase 2 ontdekking nog meer worden beïnvloed door problemen als gevolg van verouderde of fantoomsessies.

Als PSN aan stadium 2 krijgt, leidt de ontdekkingssonde die in het zittingscachegeheugen bestaat tot een verouderde of spookingang voor het zelfde eindpunt. Dit resulteert in de verkeerde postuur status die aan de eindgebruiker is geretourneerd.

In het voorbeeld wordt getoond hoe houding zich voordoet als PSN een verouderde sessie of fantoomsessie houdt:



Opmerking: het is belangrijk om te onthouden dat deze kwestie alleen kan manifesteren wanneer alle op redirect-gebaseerde ontdekkingssondes falen of wanneer niet-redirect houding is geïmplementeerd.

---

1. Elk van **Zoek mijn sessie** sondes uitgegeven door de ISE postuur module.

2. PSN voert sessierelaadpleging uit in het sessiecache. Als de sessie gevonden moet worden, doet zich een verouderde of spooksessie voor.

3. PSN voert selectie van clientprovisioningbeleid uit. Bij een spooksessie met een gebrek aan authenticatie-/autorisatiekenmerken en alle beleid dat door de klant is geconfigureerd, zijn zeer specifiek (beleid wordt bijvoorbeeld gemaakt voor specifieke Active Directory-groepen) is PSN niet in staat om een juiste client provisioningbeleid toe te wijzen. Dit kan zich manifesteren in de foutmelding: "Bypassing AnyConnect scan uw netwerk is geconfigureerd om Cisco NAC Agent te gebruiken".

- In het geval dat het beleid van de cliëntlevering generisch is (de attributen beschikbaar in de spookzitting zijn genoeg om beleid met configuratie aan te passen AnyConnect) antwoorden PSN met details nodig voor de voortzetting van het beoordelingsproces.
- Bij deze stap ook wanneer we kunnen omgaan met verouderde sessies PSN antwoorden onmiddellijk met postuur status **Voldoet** en alle volgende stappen worden niet uitgevoerd. PSN stuurt geen COA omdat het van mening is dat de sessie al in overeenstemming is. In Radius Live logs wordt er geen sessie-event weergegeven met **de** status **Compliant**.

4. Voor het spooksessiescenario gaat de ISE-poortmodule verder met het verzoek voor een eerste postuur. Dit verzoek bevat informatie over alle security en patchbeheerproducten die op het eindpunt zijn

gedetecteerd.

5. PSN gebruikt informatie van de aanvraag en sessiekenmerken om goed postuur beleid aan te passen. Omdat de fantoomsessie op dit moment een gebrek aan attributen heeft, hebben we geen beleid om bij te passen. In zo'n geval, PSN antwoordt op het eindpunt dat het volgzaam is aangezien dit een standaard ISE gedrag in het geval van niet postuur beleidsmatch is.

> **Opmerking**: wanneer er een of ander generiek beleid is dat kan worden geselecteerd uit spooksessiekenmerken, gaan we verder met stap 6.

---

6. PSN retourneert het geselecteerde postuur beleid terug naar de agent.

> **Opmerking**: Wanneer geen beleid kan worden geselecteerd, geeft PSN de status Compliant terug.

---

7. De agent retourneert de status voor elk beleid/vereiste zoals doorgegeven of mislukt.

8. Rapporteer de evaluatie op ISE en sessiestatuswijzigingen in **Conformiteit.**

> **Opmerking**: In het geval van postuur problemen veroorzaakt door de fantoomsessie, de ISE-beheerder mogelijk een aantal mislukte postuur-CoAâ€™s opmerken, zoals in dat geval COA-verzoeken worden uitgevoerd vanuit de verkeerde PSNâ€™s en voor verkeerde sessie-IDâ€™s.

Detectieproces start niet op een nieuwe verificatiepoging

ISE postermodule ontworpen om een beperkte hoeveelheid gebeurtenissen op het eindpunt te monitoren om een detectieproces te starten. Lijst van gebeurtenissen die aanleiding geven tot de ontdekking:

- Eerste installatie van de ISE-poortmodule.
- Aanmelden door gebruiker.
- Aan de macht.
- Verandering van interfacestatus.
- Ga verder na de slaap.
- Standaard gateway (DG) wijzigen.
- Zie Herbeoordeling van de houding (PRA) falen Cisco bug-id CSCvo69557

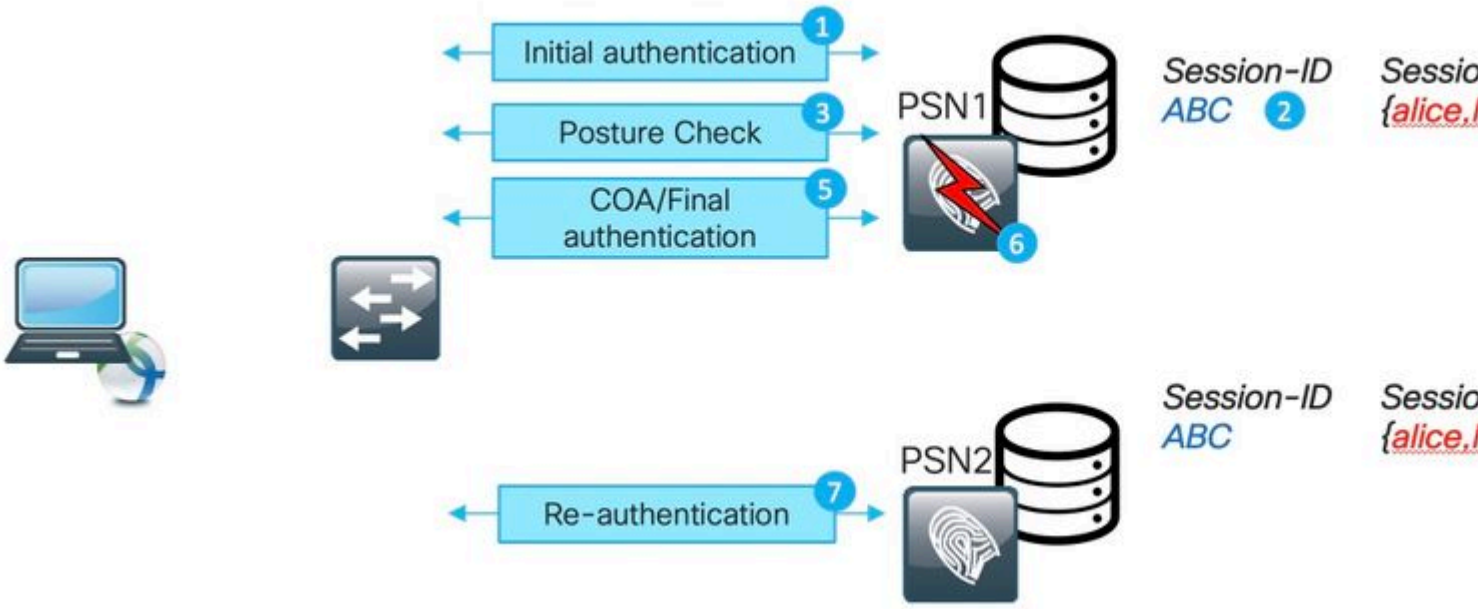
Nieuwe dot1x-verificatie, pc-ontgrendeling, wijziging van IP-adres worden niet gedetecteerd door de ISE-poortmodule.

De ISE-postermodule kan in deze scenario's geen nieuwe verificatie- of herverificatiepoging detecteren:

- Herauthenticatie raakt verschillende PSN (door LB beslissingen of problemen met originele PSN).
- NAD genereert nieuwe sessie-id bij herverificatie.

Verificatie opnieuw op verschillende PSN

Voorbeeld van herverificatie op verschillende PSN veroorzaakt door de stroomonderbreking van het oorspronkelijke PSN. Het scenario met lastverdeler lijkt erg op elkaar. In het geval van SLB moet opnieuw worden geauthenticeerd op de verschillende PSN als gevolg van het verlopen van de stickiness timer.



1. Eerste verificatie op PSN1.

2. Session ABC gemaakt in het PSN1-sessiecache.

3. Houdbaarheidsbeoordeling uitgevoerd met PSN1.

4. De positie van ABS van de zitting beweegt zich aan **Volgzaam.**

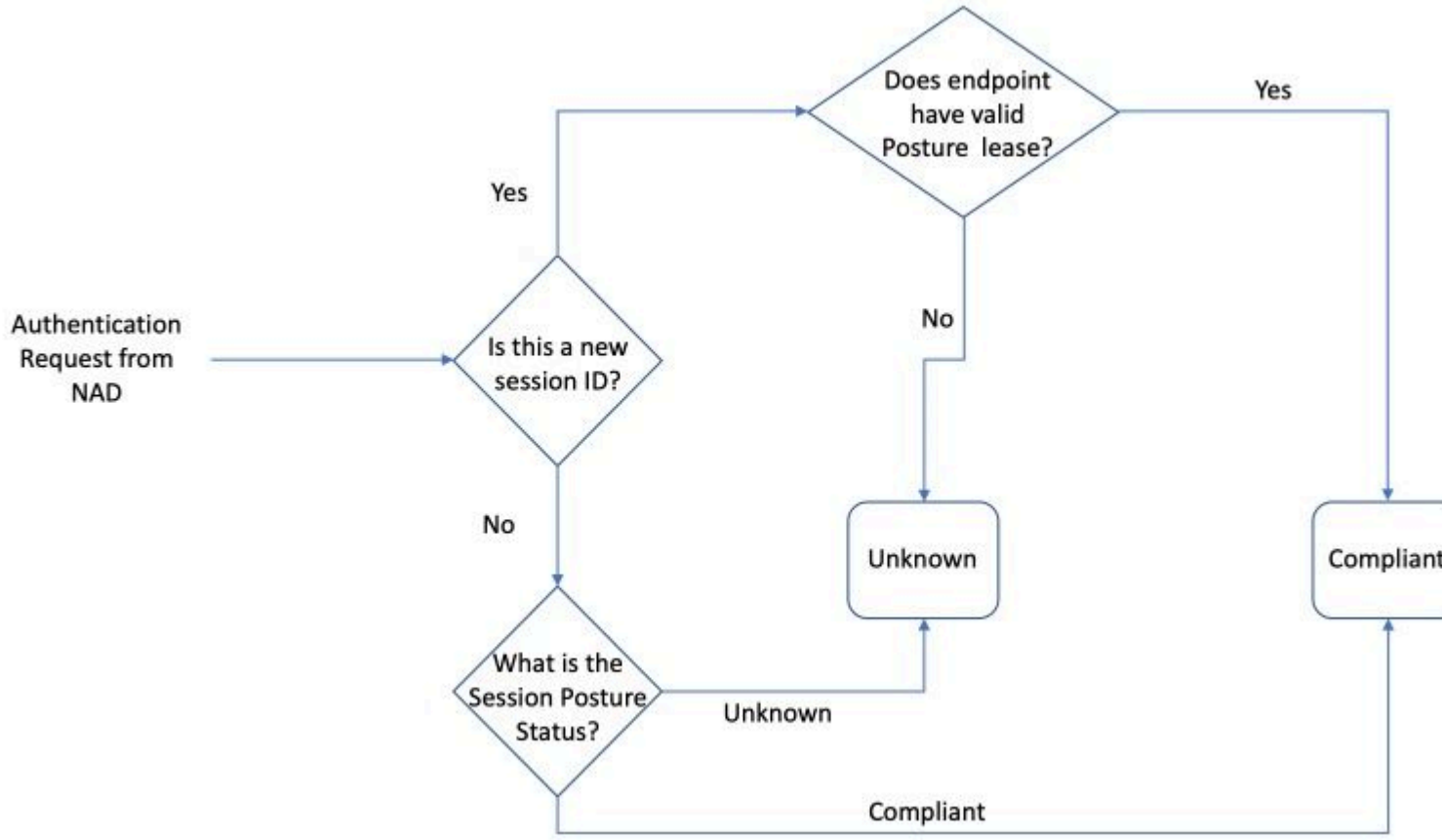
5. Een COA die wordt geactiveerd door een wijziging van de status leidt tot een nieuwe authenticatie van het eindpunt om het volgende toegangsniveau toe te passen.

6. PSN1 wordt niet beschikbaar.

7. Herverificatie voor sessie ABC hits PSN2.

8. Omdat het een nieuwe sessie is voor de PSN2-status van de sessie wordt **Hangende.**

Eerste postuur status toegewezen door PSN aan de sessie:



Opmerking: State-machine beschrijft alleen een eerste selectie van de postuur status. Elke sessie die aanvankelijk als Onbekend werd gemarkeerd, kan later conform of niet-conform worden op basis van de evaluatie van het rapport die van de ISE-postermodule is ontvangen.

NAD genereert nieuwe sessie-id bij herverificatie

Dit zou kunnen gebeuren in de twee meest voorkomende scenario's:

- Herverificatie is niet correct geconfigureerd aan de ISE-zijde. De oplossing voor dit probleem wordt later in dit document besproken.
- Misgedrag van NAD-kant - normaal houdt NAD dezelfde sessie-ID bij tijdens de poging tot herverificatie. Mocht u ontdekt hebben dat NAD een sessie-ID heeft gewijzigd bij herverificatie, dan is dit een mogelijk buggy gedrag dat onderzocht moet worden op de NAD zelf.

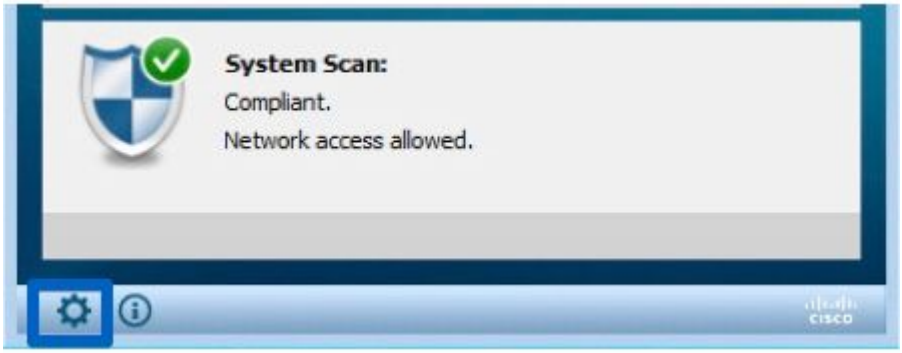
De nieuwe sessie-ID kan worden gegenereerd in een aantal andere hoekscenario's. In sommige gevallen kan draadloos roaming er bijvoorbeeld de oorzaak van zijn. Het belangrijkste is dat ISE PSN altijd een nieuwe sessie in postuur **hangende** staat plaatst tenzij de postuur lease is geconfigureerd. De posterijen worden later in dit document beschreven.

Snelle manier om vast te stellen wanneer het probleem is veroorzaakt door de Stale/Phantom-sessie

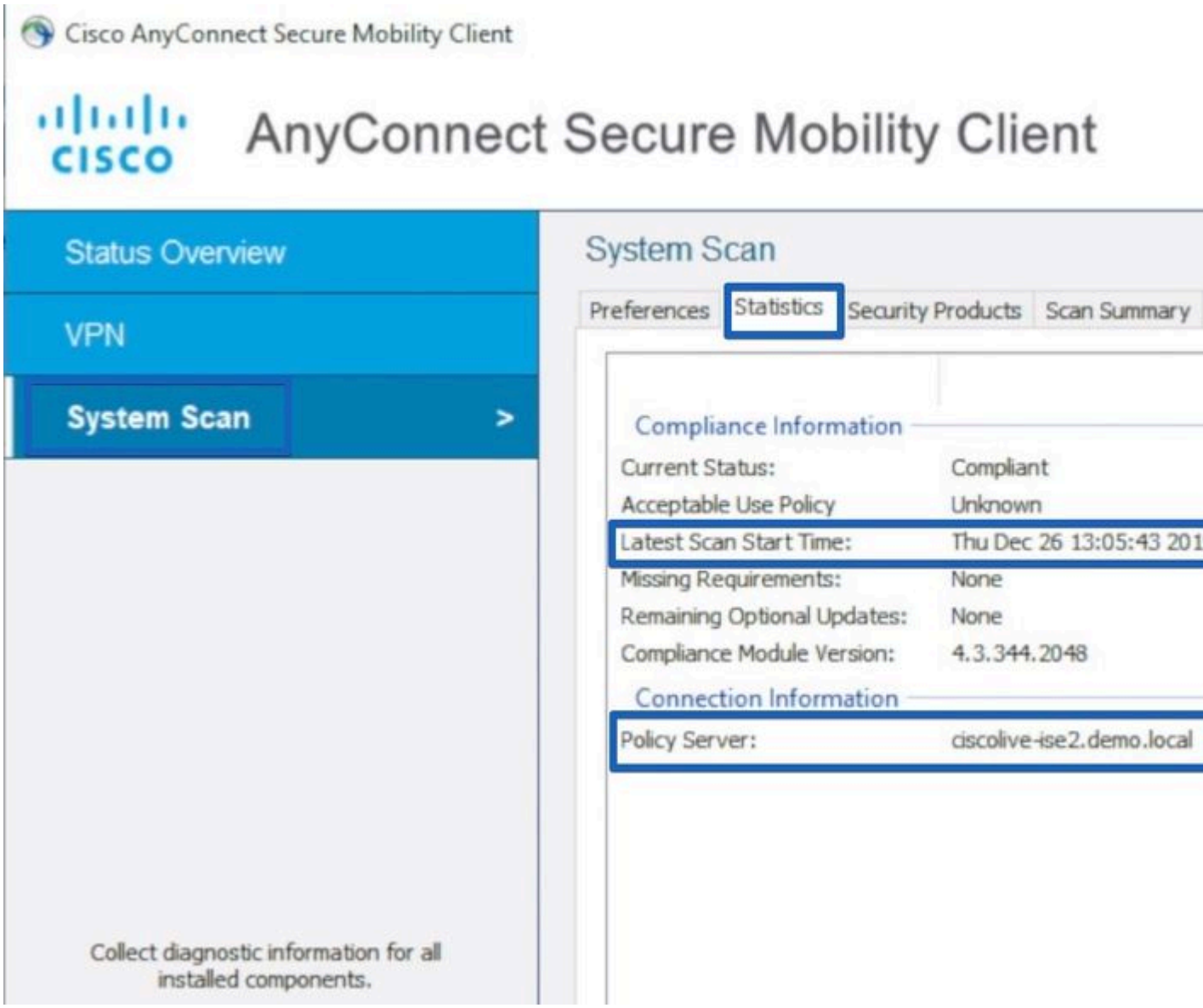
Om te bepalen of AnyConnect naleving laat zien terwijl het in de omleidingsstaat wordt veroorzaakt door de verouderde/spookzitting, moeten wij toegang tot het eindpunt krijgen terwijl het in de problematische staat is.

1. Onderzoek de Details van de Systeemscan:

1. Druk op het tandwielpictogram in AnyConnect UI



2. Navigeer in het nieuwe venster naar het tabblad Scannen en het tabblad Statistieken



Let hier op twee elementen:

- Nieuwste starttijd voor scannen - het tijdstempel hier moet sluiten op het tijdstip waarop het probleem is ontdekt.

- Policy Server - dit veld gaf de naam aan van de beleidsserver die een postuur beoordeling deed voor het eindpunt. De FQDN moet vanuit hier worden vergeleken met FQDN van Redirect-URL (voor basispostuur omleiden) of met de PSN-naam die is ontleend aan de laatste verificatiepoging (voor een postuur zonder omleiding).

2. Vergelijk Policy Server FQDN van System Scan Statistics met de nodenaam die verificatie deed voor endpoint:

In het gegeven voorbeeld is er een wanverhouding tussen de naam die erop wijst dat PSN met naam ciscolive-ise2 een stapelbare of spooksessie voor dit eindpunt houdt.

In de demo zijn de stappen opgenomen die nodig zijn voor de identificatie van het probleem:

Geavanceerde probleemoplossing van statische/spooksessie

Het vorige voorbeeld is om de kwestie van een vervelende of spookzitting van het probleem van het ontdekkingsproces te onderscheiden dat niet begon. Tegelijkertijd moeten we de sessie identificeren die het probleem heeft veroorzaakt, om beter te begrijpen hoe het nu precies een vervelende of spooksessie wordt.

Terwijl in sommige scenario's vervelende en spooksessies niet kunnen worden vermeden. We moeten ervoor zorgen dat er geen verouderde / spooksessies worden gecreëerd in de omgeving als gevolg van een aantal van de best practices die niet worden geïmplementeerd.

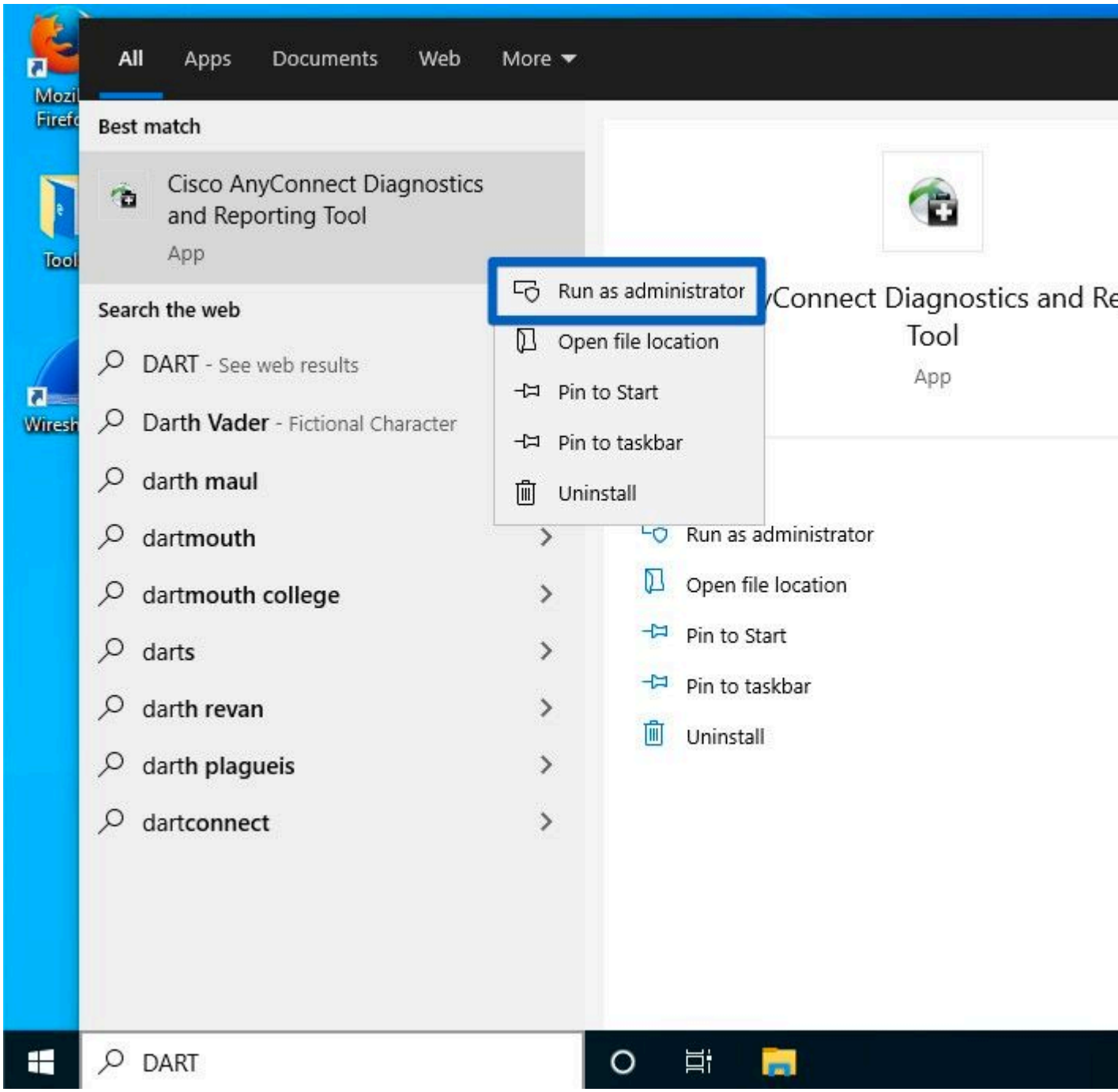
DART-bundelverzameling

Analyseer een DART-bundel die is genomen van het eindpunt dat het probleem reproduceert.

- Houd alleen belangrijke logbestanden in het DART. Het wordt aanbevolen om de logbestanden te wissen voordat het probleem wordt gereproduceerd.

Om dit te bereiken, moet het DART bundelhulpprogramma beginnen als beheerder en logopmaak uitvoeren.

1. Op Windows Navigate om te beginnen en te beginnen met het typen van DART, klik met de rechtermuisknop en kies - **Uitvoeren als beheerder**



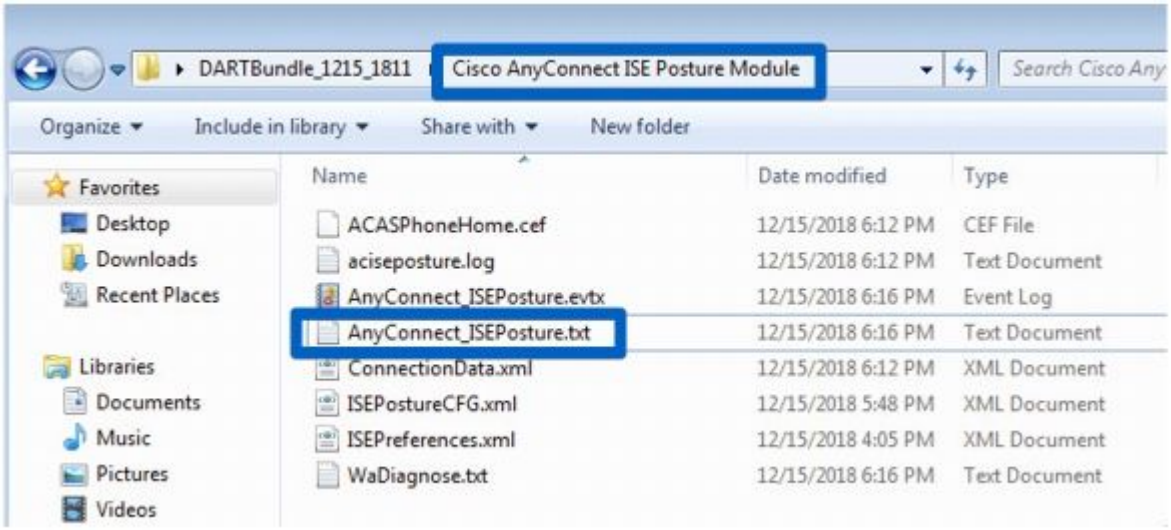
2. Druk op Volgende op het eerste wizard scherm

3. Druk op Alle logbestanden wissen op het volgende scherm van de wizard

4. Nadat het probleem is gereproduceerd kan DART worden verzameld van hier; druk op **Volgende**.

DART-bundelanalyse

Nadat de DART-bundel is verzameld, moeten we deze verwijderen en ons richten op het bestand **AnyConnect_ISEPosture.txt** dat zich bevindt in de map **Cisco AnyConnect ISE-poortmodule**. Dit bestand bevat alle gebeurtenissen die met de ontdekking te maken hebben.



1. Start probleemoplossing en identificeer alle momenten waarop de detectie opnieuw wordt gestart. De trefwoorden die u wilt zoeken, zijn **Discovery** of HTTP-detectie **opnieuw starten**. Blader hier naar de lijn met de herstart van de ontdekking die op het problematische moment plaatsvond:

```
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. Een paar lijnen na de ontdekking herstart je ziet een lijn die bevat - Probing geen MNT-podiumdoelen. Dit is een indicator van stadium 1 ontdekkingsbegin:

```
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
```

Het is aan te raden om alle omleiding gebaseerde sondes met dezelfde kleur te markeren, terwijl eerder verbonden PSNâ€™s genomen van **ConnectionData.xml** (Auth-Status targets) moeten worden gemarkeerd in verschillende kleuren omdat PSN FQDNâ€™s meestal erg vergelijkbaar zijn en het is moeilijk om het verschil te herkennen.

3.Lees de logbestanden om een resultaat te zien voor elke sonde. Zoals al is gezegd in het geval van de kwestie veroorzaakt door vervelende/spooksessie, moeten alle omgeleide sondes falen. Dit is een voorbeeld van hoe de mislukte sonde eruit ziet:

```
2018/12/15 18:12:01 [Information] aciseagent Function: Target::Pro
File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\is
cpp Line: 200 Level: debug Status of Redirection target enroll.ci
Reachable.>.
```

4. Ergens in het bestand na de ontdekking van de herstart voor fase 1 of fase 2, ziet u een succesvol antwoord van een of meer PSN's:

```
Target::fetchPostureStatus Thread Id: 0xBF0 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\post
\Target.cpp Line: 401 Level: debug  POST request to URL (
https://ciscolive-ise2.demo.local:8443/auth/ng-discovery), r
<Operation Success.>.
```

5. Een paar regels later is er een regel met het trefwoord **MSG_NS_SWISS_NEW_SESSION.** Deze regel bevat een feitelijke sessie-ID die door PSN is geselecteerd als resultaat van het zoeken naar de sessie. Gebruik deze sessie-ID voor verder onderzoek naar ISE om erachter te komen hoe deze sessie vervelend/fantoomloos wordt:

```
SwiftHttpRunner::invokePosture Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\post
ftHttpRunner.cpp Line: 1407 Level: debug  MSG_NS_SWISS_NEW_S
{{ise_fqdn="ciscolive-ise2.demo.local"}, {posture_port="8443
{posture_path="/auth/perfigo_validate.jsp"},
{posture_domain="posture_domain"}, {posture_status="Complian
{session_id="0a3e949c000002585cf00588"},
{config_uri="/auth/anyconnect?uuid=f62337c2-7f2e-4b7f-a89a-3
{acpack_uri="/auth/provisioning/download/066ac0d6-2df9-4a2c-
 {acpack_port="8443"}, {acpack_ver="4.6.3049.0"}, {pra_enabl
```

Onderzoek op ISE-logbestanden

In de guest.log met **clientwebapp** component ingeschakeld in DEBUG, de PSN die antwoordt met de Stale/Phantom sessie kan worden gezien.

PSN krijgt een verzoek van de ISE postuur agent. U kunt zien dat dit een verzoek is van AnyConnect vanwege de waarde voor 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
```

Het verzoek bevat arrays van IP adressen en MAC adressen. In dit voorbeeld heeft elke array slechts één waarde. Eveneens laat het logboek zien dat sessie-ID van het verzoek ongeldig is, wat aangeeft dat dit een verzoek van de non-redirect gebaseerde sonde is.

Later kunt u zien hoe waarden uit arrays worden gebruikt om een sessie-ID te vinden:

<#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
```

Na de regel met de trefwoorden **Verzonden http response** kunt u de inhoud zien van het echte antwoord:

<#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
```

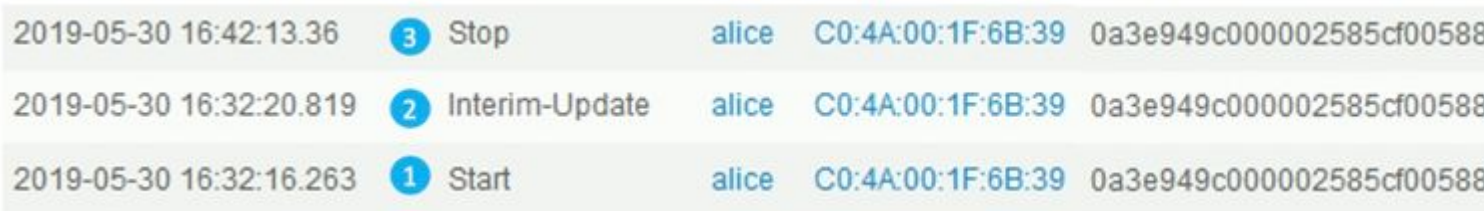
```
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_PORT value is 8443

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
```

Onderzoek naar ISE-verslagen

Nadat u het ID van de vervelende/spooksessie kent, kunt u het Radius-accountingrapport onderzoeken om een beter begrip te krijgen van wat deze sessie heeft veroorzaakt tot vervelend/spookbeeld:

- Navigeer naar Operations > Rapporten > Eindpunten en Gebruikers > Radius-accounting rapport en voer dit rapport 7 dagen uit. Gebruiker een eindpunt-ID als filtertoets.

Voorbeeld van een rapport dat laat zien hoe oud de sessie is op ciscolive-ise2:



1. De boekhoudkundige start van de sessie kwam bij de PSN ciscolive-ise2
2. De tussentijdse update voor de sessie werd op hetzelfde PSN verwerkt.
3. Het rekenschap geven stopbericht voor problematische zitting ID kwam aan verschillende PSN (ciscolive-ise1).

Een snelle manier om te bepalen wanneer het probleem is veroorzaakt door het ontbreken van een herstart van de detectie

Hier is dezelfde logica van toepassing als bij de vorige kwestie. Het enige verschil is dat u zich moet richten op de laatste starttijd voor scannen. Voor dit soort problemen is de tijdstempel van de laatste scan ergens in het verleden.

Normaal gesproken wanneer de eindgebruiker een probleem ontdekt, wordt er een scan gezien die enige tijd geleden heeft plaatsgevonden. Tijdens de Live-logbestanden van de ISE-straal worden recente verificatiepogingen vanaf het problematische eindpunt waargenomen.

In de demo zijn de stappen opgenomen die nodig zijn voor de identificatie van het probleem:

Geavanceerde probleemoplossing - geen herstart van detectie

De benadering hier is zeer gelijkaardig aan de Geavanceerde sectie van de Oplossing van het Probleemverhaal/van de Spookzitting. Het belangrijkste element van probleemoplossing is het DART bundelonderzoek. Binnen de DART bundel, kunt u zoeken naar ontdekkings herstart zoals het voor het vorige probleem is getoond en bevestigen dat er geen ontdekking herstart was op het moment dat het probleem werd gemeld.

Aan de kant van ISE, focus op Radius Live Logs/Radius authenticatie rapport om te bevestigen dat er was failover tussen PSNs of nieuwe sessie-ID is gegenereerd door NAD.

Oplossing

Klassieke benadering - emissievermijding

Van oudsher was er geen eigenschap op ISE die problemen kon oplossen die in dit document worden beschreven, dus de enige manier was om te vertrouwen op de reeks beste praktijken die worden geïmplementeerd op het netwerk en de ISE-zijde de minimaliseren risico's.

Beste praktijken die de hoeveelheid verhaal of spooksessies in de plaatsing van ISE kunnen minimaliseren

Voer waar mogelijk altijd een omleidingsgerichte houding uit

Een tegenargument tegen deze aanbeveling is een slechte gebruikerservaring als pop-ups in het besturingssysteem of browsers worden gezien die wijzen op omleiding terwijl AnyConnect ISE-postermodule op de achtergrond een beoordelingsproces uitvoert.

Als oplossing hiervoor is het mogelijk om alleen ISE Posture module detectietests om te leiden en selectief al het andere verkeer toe te laten.

In het voorbeeld wordt ACL getoond die is ontworpen om alleen HTTP-verzoeken naar Discovery Host (10.1.1.1 in dit voorbeeld) en enroll.cisco.com (172.16.1.80) om te leiden:

```
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
```

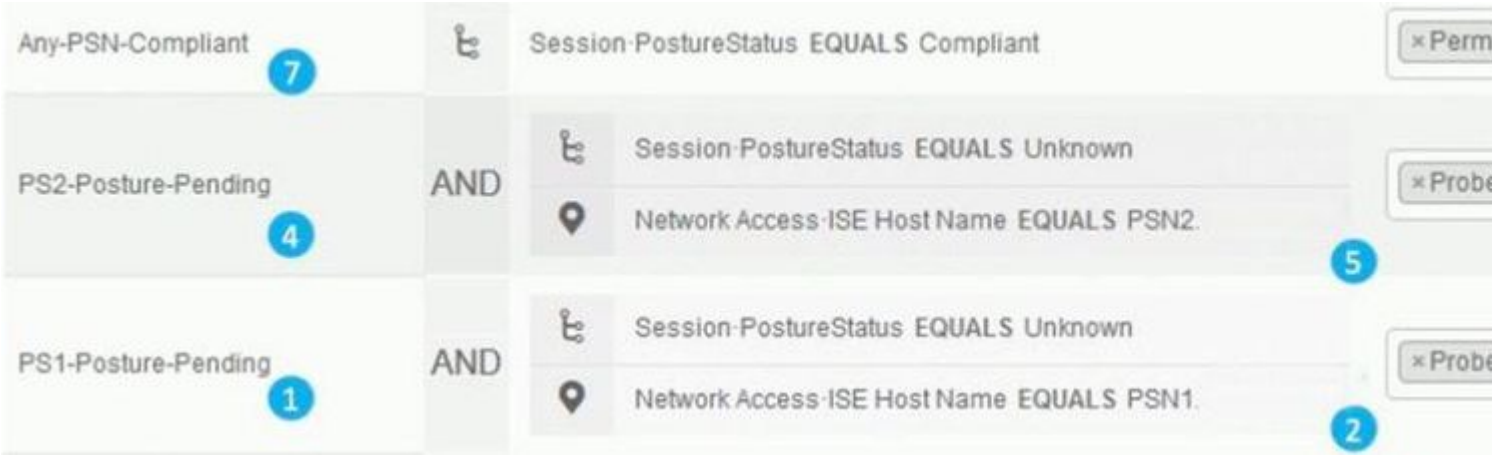
Om een acceptabel beveiligingsniveau te behouden, kunnen dergelijke omleidingen van ACL worden gecombineerd met DACL die is toegewezen via ISE.

In wachtstand kunt u alleen verbindingen maken met PSN waarbij eindpunt is geverifieerd

Deze benadering is nuttig voor omgevingen waar url-omleiding niet wordt ondersteund (bijvoorbeeld implementaties met de NAD's van derden).

Als oplossing moet u meerdere beleidsregels voor **PosturePending** autorisatie implementeren (één per PSN). Elk beleid moet als één van de voorwaarden de naam van PSN bevatten waar de authentificatie plaatsvond. In het autorisatieprofiel dat is toegewezen aan elke beleidstoegang, moeten alle PSN's worden geblokkeerd, behalve de knooppunt waar de verificatie heeft plaatsgevonden.

Beleid voor autorisatie maken voor implementatie van 2 knooppunten:



â€ƒ

1. Positie **in behandeling** bij PSN1.

2. De naam PSN1 wordt als voorwaarde in het beleid gebruikt.

3. Autorisatieprofiel met ACL die de toegang tot alle PSN behalve PSN1 blokkeert.

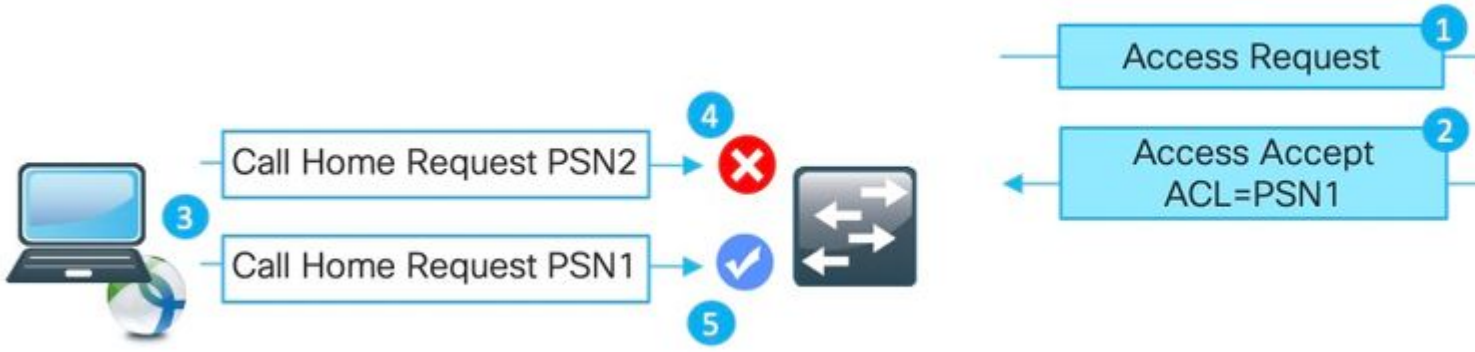
4. Positie **in behandeling** bij PSN2.

5. De naam PSN2 wordt gebruikt als voorwaarde in het beleid.

6. Autorisatieprofiel met ACL die de toegang tot alle PSN behalve PSN2 blokkeert.

7. Posture 'Compliant' autorisatiebeleid.

In deze afbeelding wordt uitgelegd hoe deze benadering werkt:



1. Verificatie bereikt PSN1.

2. Als gevolg van een geconfigureerd autorisatiebeleid kent PSN1 een autorisatieprofiel toe dat de toegang tot alle andere knooppunten behalve PSN1 blokkeert.

3. De AnyConnect ISE-positiemodule start het detectieproces opnieuw.

4. Sonde naar PSN2 geblokkeerd door het NAD zoals door een eerder toegewezen ACL.

5. Sonde aan PSN1 toegestaan door ACL toegewezen op NAD.

Best practices voor taakverdeling

- Toegelaten kleverigheid op LB voor authentificatie en boekhouding met Calling-Station-ID als kleverheidssleutel. Klik hier voor meer informatie over de best practices van LB voor ISE.
- Gebruik een stickiness timer langer dan een gemiddelde werkdag om het moment te bedekken waarop de pc in slaap valt (bijvoorbeeld 10 uur in plaats van 8 uur).
- Als opnieuw authenticeren is geïmplementeerd, gebruikt u een herverificatietimer die iets lager is dan de stickiness timer (bijvoorbeeld 8 uur als de stickiness 10 uur is ingesteld). Dit waarborgt dat het kleverheidsinterval door re-authentificatie wordt verlengd.

Posture over VPN use-case

- Zorgt ervoor dat de accounting-interim update interval hoger of gelijk is aan de VPN-sessie-timeout. Dit beschermt tegen boekhoudkundige flappen tussen PSNs op lang levende VPN-sessies.

Dit voorbeeld toont het tussentijdse boekhoudkundige updateinterval dat voor 20 uren wordt gevormd. Dit voorkomt niet dat de eerste tussentijdse update die IP-adres draagt dat is toegewezen aan het eindpunt.

```
aaa-server ISE protocol radius

 interim-accounting-update periodic 20

group-policy SSL-VPN attributes

 vpn-idle-timeout 1200

 vpn-session-timeout 1200
```

Er kunnen best practices worden geïmplementeerd om de impact van de afwezigheid van de herstart van de detectie van de ISE-poortmodule te minimaliseren

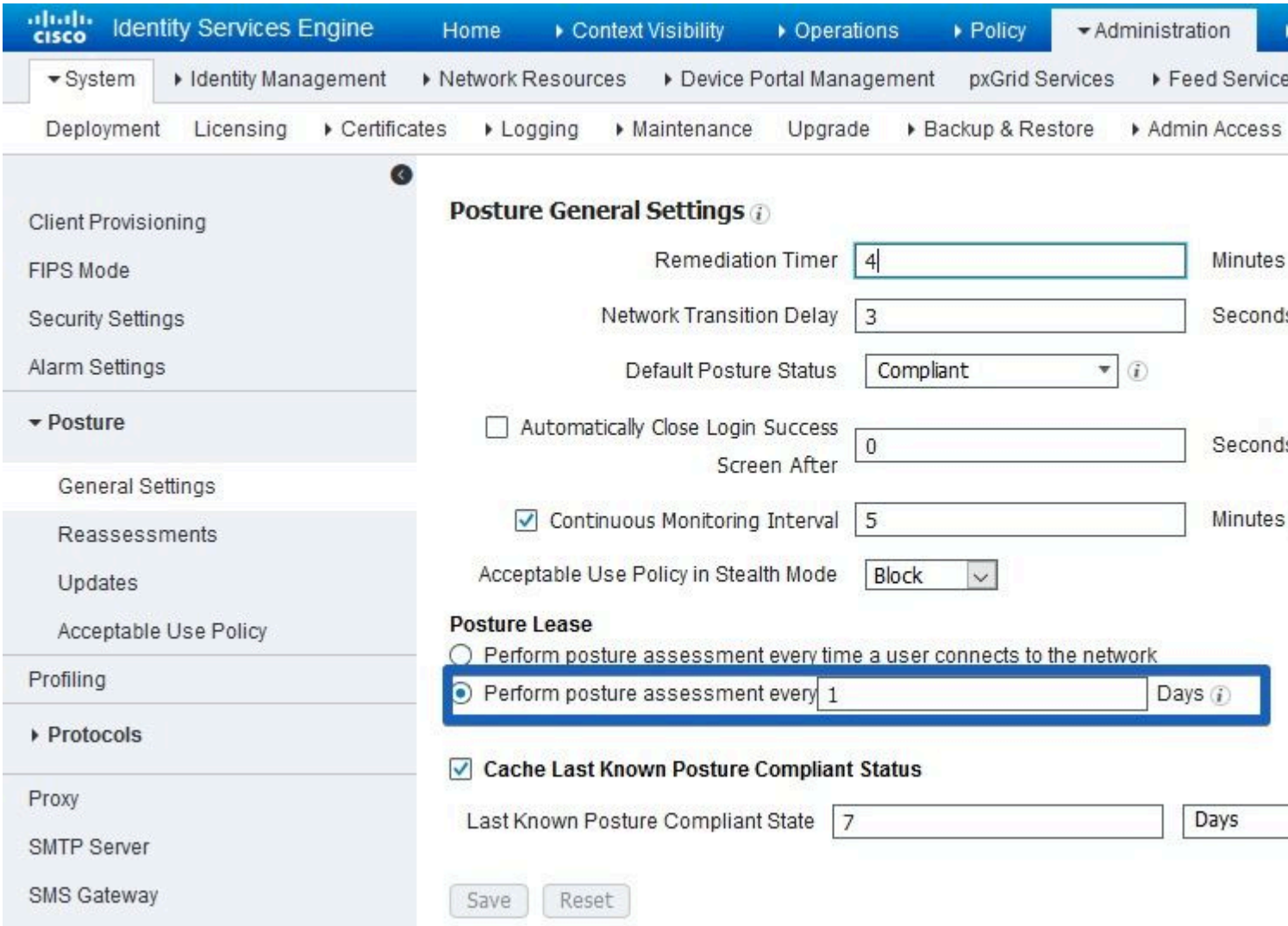
Posture lease inschakelen

Dit is een functie op ISE die eindpunt markeert als een conforme voor een bepaalde periode (1-365 dagen). Posture lease value is een endpoint attribuut dat betekent dat het is opgeslagen ISE DB. Alle endpointkenmerken die postuur-lease omvatten, worden over alle knooppunten in de ISE-implementatie gerepliceerd.

Wanneer PSN een nieuwe sessie voor de endpointpostuur krijgt, kan deze worden gebruikt om de sessie meteen als **conform** te markeren.

Om dit besluit te nemen gebruikt PSN 3 waarden. Deze waarden zijn:

- Het aantal dagen dat is gedefinieerd voor posteringshuur in ISE-instellingen: **Navigeren naar Beheer > Systeem > Posterijen > Algemene instellingen**:



- Waarde van PostureExpiry attribuut - dit is een werkelijk eindpuntattribuut dat een Epoch timestamp bevat. De waarde van PostureExpiry is aanvankelijk bevolkt op de eerste succesvolle postuur poging voor eindpunt nadat de beheerder van ISE postuur huur toeliet. Later deze waarde bijgewerkt op de volgende succesvolle postuur poging die gebeurt na afloop van de leaseovereenkomst.

U kunt een PostureExpiry in Context Visibility > Endpoints zien terwijl één van de gepostuleerde eindpunten wordt geopend:

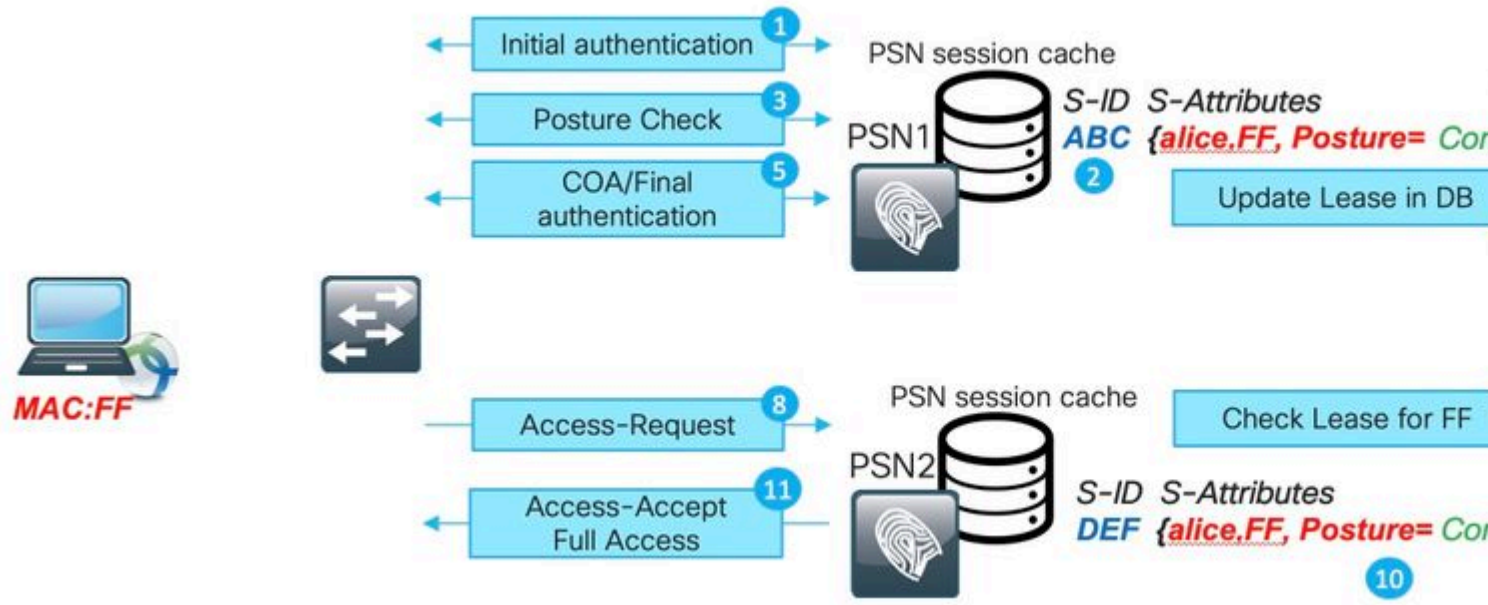
PostureExpiry	1586332942236
PostureOS	Windows 10 Professional 64-bit

Deze waarde kan in de door de mens leesbare tijdstempel worden omgezet, bijvoorbeeld hier - https://www.epochconverter.com/

- De tijd van het PSN-systeem op het moment dat nieuwe verificatie plaatsvindt

Wanneer de authenticatie voor een eindpunt met postuur leasehits PSN gebruikt het PostureExpiry en systeemdatum om een aantal dagen te krijgen die van de laatste succesvolle postuur controle overgingen. Als de resultaatwaarde binnen een posture-leaseinterval valt dat in instellingen is gedefinieerd, krijgt de sessie een **conforme** status. Als de resultaatwaarde hoger is dan de leasewaarde krijgt de sessie een **Onbekende** status. Hierdoor wordt de houding opnieuw uitgevoerd en kan een nieuwe PostureExpiry waarde worden opgeslagen.

Het getal verklaart het proces bij failover:



1. De eerste verificatie gebeurt met PSN1.

2. Session ABC gemaakt in het sessiecache.

3. Houdbaarheidsbeoordeling vindt plaats.

4. Sessiestatus verandert in **conform**

5. Een COA die wordt geactiveerd door een wijziging van de status leidt tot een nieuwe authenticatie van het eindpunt om het volgende toegangsniveau toe te passen.

6. De waarde van PostureExpiry die in het eindpunt wordt opgeslagen.

7. Endpoint data gerepliceerd over de implementatie.

8. Volgende verificatie bereikt PSN2.

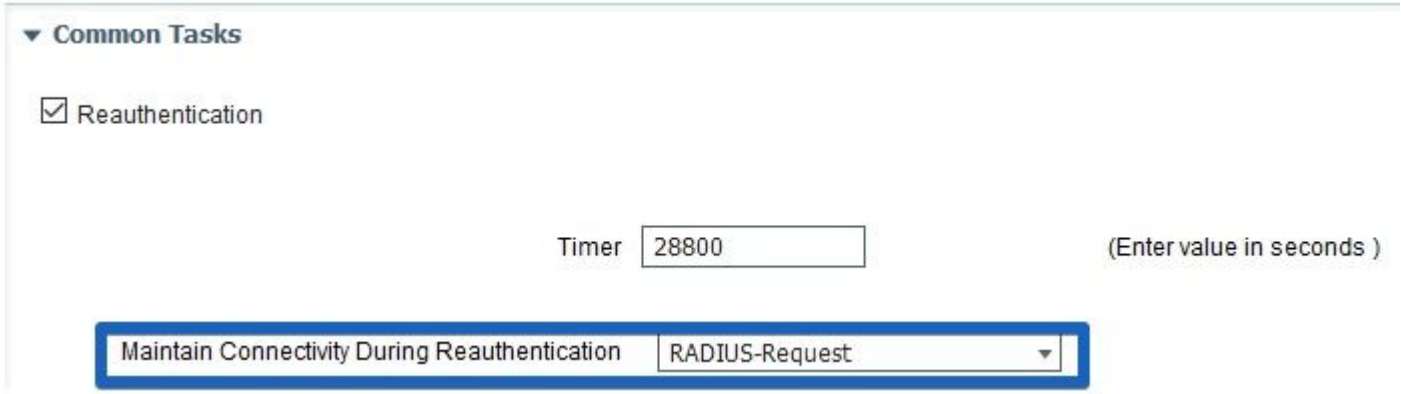
9. PSN2 controleert als het eindpunt binnen een geldige posteriehuur is.

11. Sessie toegevoegd aan het sessiecache als **conform**.

12. Vanwege de geldige lease, de sessie gemaakt met status **conform**.

Implementatie van herverificatie

Druk altijd op herverificatietimer van ISE met **RADIUS-Aanvraag** geselecteerd in **Connectiviteit behouden tijdens herverificatie.** Deze instelling zorgt ervoor dat NAD dezelfde sessie-ID bij herverificatie bewaart.



.

Omgevingen met taakverdeling

Dezelfde set best practices kan worden geïmplementeerd die in de sectie Stale/Phantom Session werden uitgelegd.

Verschillende subnetten kunnen worden gebruikt voor wachtende en compatibele staten

Wanneer het netwerkontwerp de mogelijkheid biedt om verschillende subnetten te gebruiken die **hangende** en **conforme** staten zijn, garandeert deze benadering dat elke verandering in de status van de houding resulteert in de standaardgateway.

Standaardevaluatie gebruikt in dezelfde interval als een herverificatieteller

Houdingsevaluatie kan worden ingeschakeld met een interval dat gelijk is aan de herverificatietimer. In een dergelijk geval wordt het detectieproces opnieuw gestart wanneer de oorspronkelijke PSN niet beschikbaar is voor PRA-storing.

Moderne aanpak - Positie staat delen

Als deel van een geïmplementeerde verbetering die in Cisco bug-id CSCvi35647patch 6 voor ISE 2.6 is beschreven, is er een nieuwe functie die de status van het delen van de sessiestatus op alle knooppunten in ISE-implementatie implementeert. Deze verbetering is geïntegreerd in toekomstige releases: ISE 2.7 patches 2 en ISE 3.0.

Deze nieuwe functie is gebaseerd op Light Session Directory (LSD) mechanisme dat is geïntroduceerd in ISE 2.6. In de nieuwere versies is deze functionaliteit hernoemd naar Light Data Distribution (LDD) Radius Session Directory. Light Data Distribution is standaard ingeschakeld en maakt het delen van een beperkte sessiecontext tussen ISE-knooppunten mogelijk. Er is niet zoiets als volledige sessiecontextreplicatie tussen PSN's, slechts een beperkte hoeveelheid attributen gedeeld voor elke sessie.

Het belangrijkste idee achter Light Session Directory is om de noodzaak te verwijderen om dure API-oproepen naar MNT uit te voeren wanneer een van de knooppunten in de implementatie moet uitzoeken wie de huidige sessieeigenaar is. Meestal eigenaar zoeken is nodig wanneer Cacao stroom start. Met LDD kan elke PSN een eigenlijke eigenaar van de sessie vinden vanuit het lokale Radius Session Directory cache.

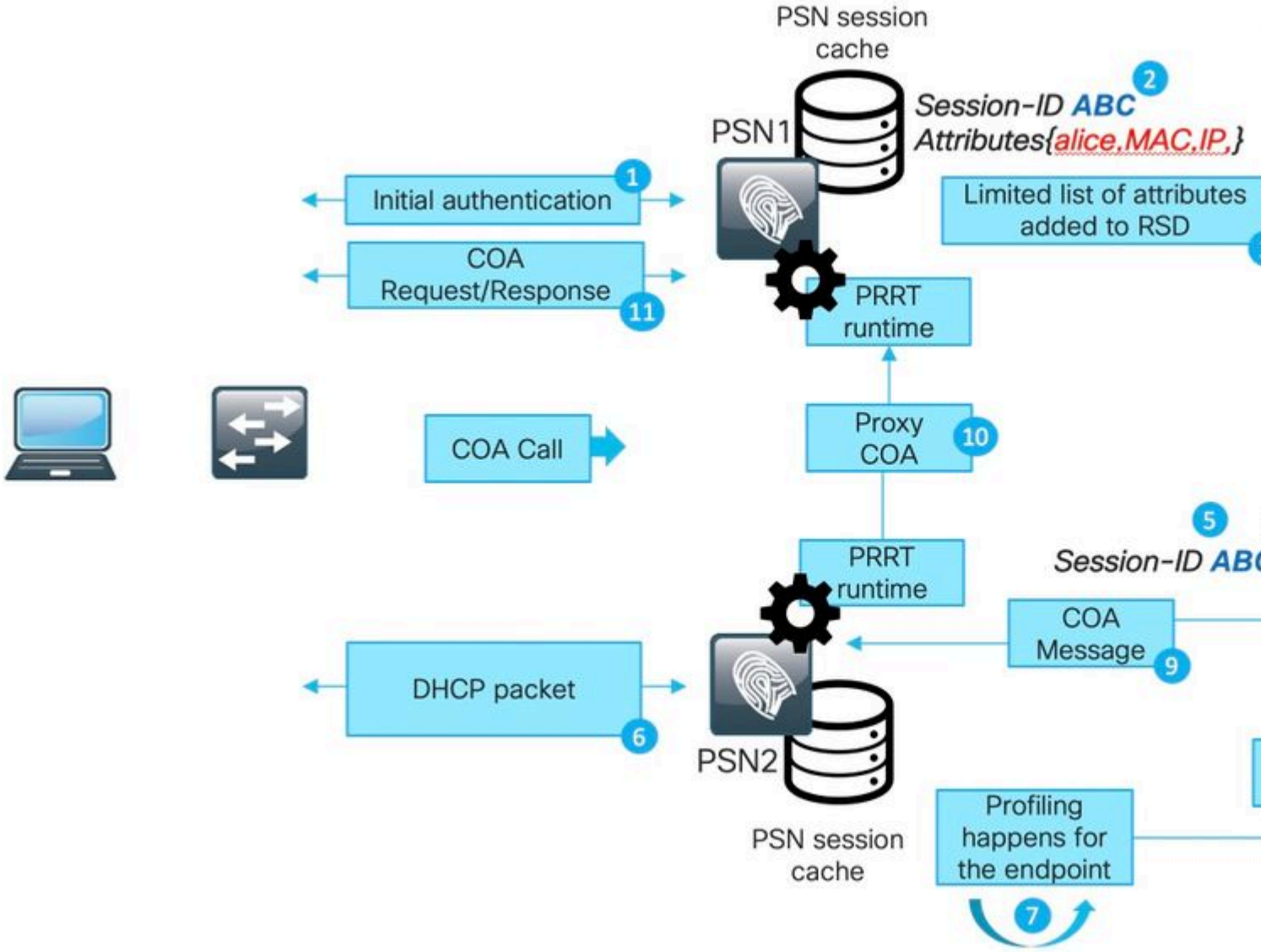
Architectuur voor lichtgegevensdistributie

Deze functionaliteit bevat de volgende elementen:

- Radius Session Directory (RSD) cache - deze cache bestaat op elke ISE-knooppunt en slaat alle actieve sessies op die in ISE-implementatie worden gepresenteerd. Elke sessie heeft een beperkte hoeveelheid attributen in de cache. Voorbeelden van de eigenschappen die zijn opgeslagen in de Radius Session Directory voor elke sessie:
    - Sessie-ID.
    - Endpoint MAC.
    - Nummerherkenning.
    - Endpoint IP
    - PSN IP - PSN waar verificatie heeft plaatsgevonden.
    - PSN FQDN - hetzelfde als hierboven.
    - NAS-IP-adres.
    - NAS-IPv6-adres.
    - Status - geverifieerd, gestart, gestopt.
- RabbitMQ exchange - Er is een uitwisseling gevormd waarin Uitgever, gerelateerde Wachtrij en Consument worden gepresenteerd op elke knooppunt in ISE-ontwikkeling. Dit waarborgt dat de topologie met volledige mesh tussen alle ISE-knooppunten vormde.
- Uitgever - de Radius Session Directory vertegenwoordigt hier een uitgever. Wanneer een nieuwe succesvolle verificatie verwerkt door PSN nieuwe sessie wordt gemaakt in het PSN-sessiecache. Voor deze sessie wordt een beperkte set kenmerken in de Radius Session Directory geplaatst.
- Consumer - op alle andere knooppunten Radius Session Directory vertegenwoordigt een consument.

Opmerking: algemene RabbitMQ-terminologie en -architectuur vallen buiten het bereik van dit document.

De figuur legt uit hoe COA flow werkt met RSD cache:



1. De eerste verificatie gebeurt met PSN1.

2. Session ABC gemaakt in het sessiecache.

3. De vereiste eigenschappen worden opgeslagen in RSD.

4. Sessie gedeeld via RabbitMQ met alle andere ISE-knooppunten.

5. Session wordt gemaakt in RSD cache op alle ISE-knooppunten.

6. Nieuwe profielgegevens worden geleverd op PSN2.

7. Endpoint wordt opnieuw geprofileerd en in het geval van de verandering die vereist dat COA uitvoering PSN2 gaat met de volgende stap.

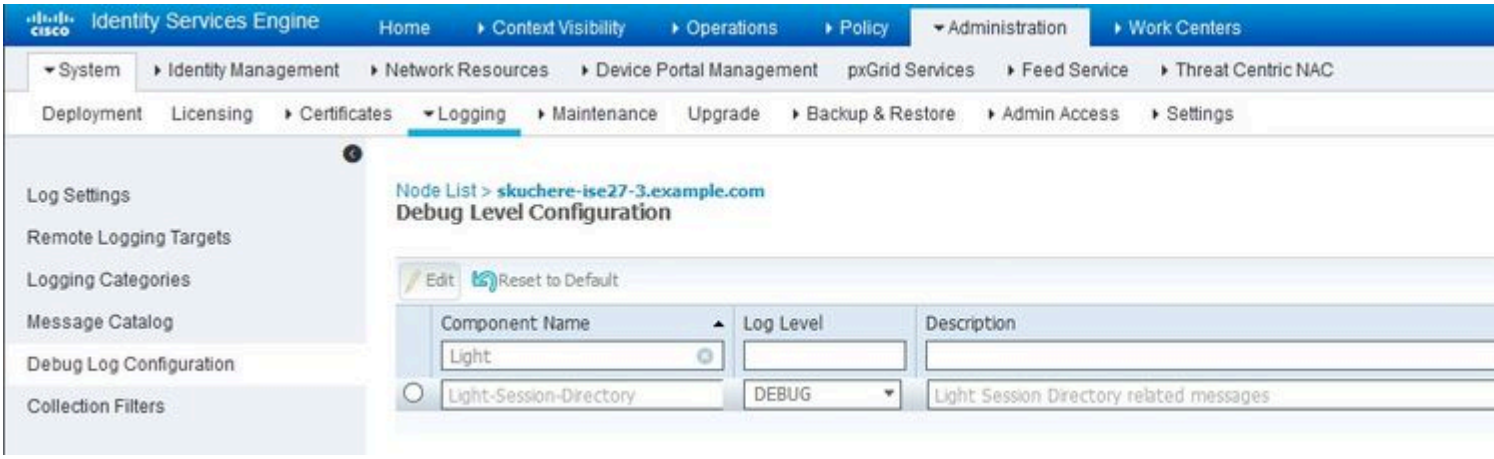
8. Een interne API-oproep die naar RSD-cache wordt gestuurd om COA uit te voeren.

9. Gegevens van het RSD-cachegeheugen dat wordt gebruikt om een Proxy-COA-bericht voor te bereiden (een COA die van de ene ISE-knooppunt naar de andere gaat, bevat alle details die de bestemmingsknooppunt kan gebruiken om een CAO-verzoek terug te sturen naar NAD). COA-bericht eerst intern overgedragen naar PRTR Runtime (Actual AAA-server binnen ISE).

10. PSN2 stuurt een COA bericht naar PSN1.

11. PSN1 stuurt een COA-bericht naar NAD.

Om de communicatie via LDD op de ISE op te lossen, kunt u de **Light Session Director**-component inschakelen voor DEBUG:



Een voorbeeld van debug-bericht uit lsd.log-bestand voor het maken en publiceren van sessies op de oorspronkelijke PSN:

```
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
```

Op alle andere ISE-knooppunten ziet u hoe een sessie is geconsumeerd:

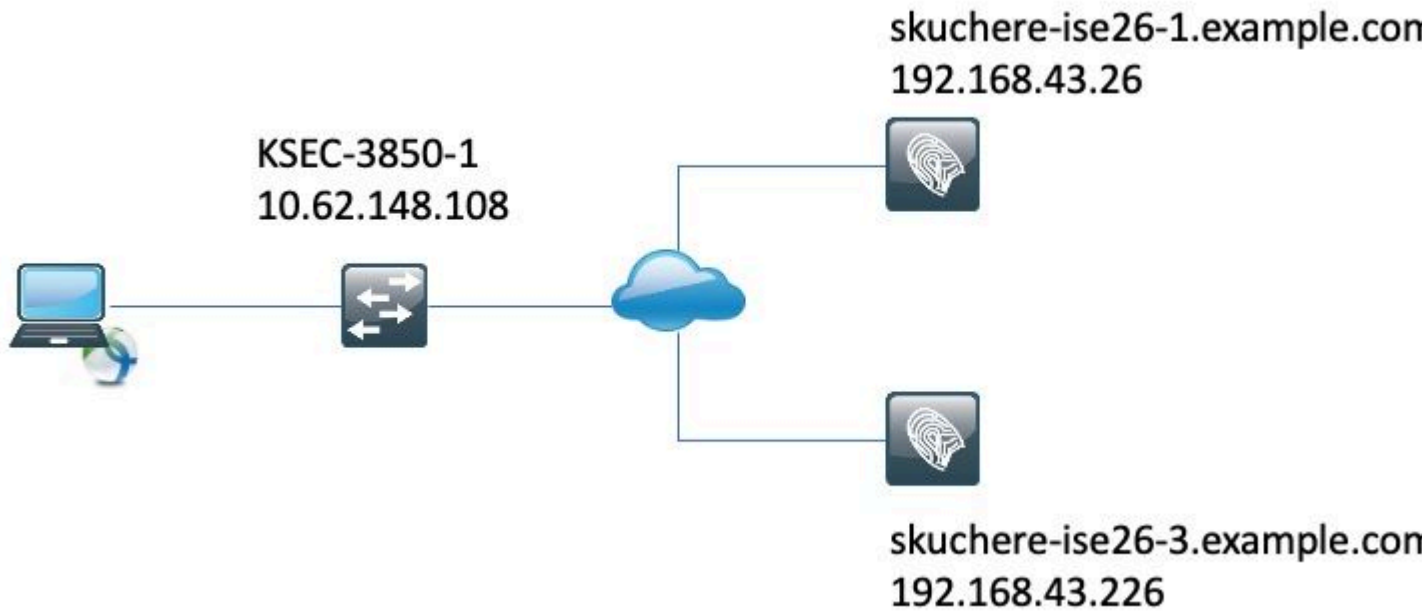
```
[pool-35-thread-38][] cisco.cpm.lsd.service.SessionConsumer -:::::- Consumer is processing : sessionID:[0
```

Positie Status Sharing via RSD

Posture status delen tussen de knooppunten lost het probleem op dat het symptoom heeft zoals 'AnyConnect ISE postuur module toont compatibele terwijl de sessiestatus op ISE hangende is' wanneer de worteloorzaak is of Stale/Phantom sessie of Re-authenticatie op verschillende PSN met een originele sessie-ID die niet ontdekking opnieuw starten. Zodra de sessie conform wordt, wordt deze informatie geplaatst in de sessie RSD, en later kan het worden gebruikt door elke PSN in de implementatie.

Er zijn nog enkele andere hoekcases die de beschreven functie niet kan oplossen. Bijvoorbeeld een scenario wanneer NAD opnieuw verificatie uitvoert op hetzelfde PSN maar met een andere sessie-ID. Dergelijke scenario's kunnen worden behandeld met de beste praktijken die in dit document worden beschreven.

Het cijfer toont de topologie aan die voor een test van het delen van de postuur wordt gebruikt:



Posture Status delen via RSD - Stale/Phantom Session

Om een verouderde sessie authenticatie te maken is eerst uitgevoerd op de skuchere-ise26-1 en later en is opnieuw geconfigureerd om accounting naar skuchere-ise26-3 te sturen. Nadat een boekhoudbericht is doorgestuurd naar de verkeerde PSN en opnieuw is ingesteld om de boekhouding terug te sturen naar skuchere-ise26-1.

De figuur toont een boekhoudkundig rapport dat de aanwezigheid van de fantoomsessie op skuchere-ise26-3 bewijst:

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. Door skuchere-ise26-1 verwerkte berichten voor het opstarten van een accounting.

2. tussentijdse boekhoudkundige update voor dezelfde sessie verwerkt door skuchere-ise26-3.

3. De sessie eindigt later op skuchere-ise26-1.

Na enige tijd verbindt het eindpunt opnieuw met het netwerk, maar de omleiding werkt niet meer. In de guest.log van PSN - skuchere-ise26-3, kunt u deze logberichten zien met **client-webapp** component ingeschakeld 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
```

Wanneer PSN detecteert dat het een stapelbare/spooksessie houdt voor het eindpunt, antwoordt het niet op de ISE postuur module en dit stelt ons in staat om het juiste antwoord te krijgen van de PSN waar de laatste authenticatie plaatsvond.

Als oplossing voor het probleem van de vervelende/spooksessie nu op het moment van de sessieraadpleging controleert PSN de aanwezigheid van een nieuwe sessie voor het eindpunt in de RSD. Als RSD sessie-ID anders bevat dan wat PSN in het lokale sessiecache heeft, wordt ervan uitgegaan dat de sessie die in het sessiecache wordt gepresenteerd, verouderd is.

Posture Status Sharing over RSD - failover tussen PSNs

Om dit scenario te reproduceren is een korte herverificatietimer ingeschakeld in het autorisatieprofiel dat is toegewezen aan het eindpunt in de compatibele staat. Later werd NAD hergeconfigureerd om authenticatie en accounting naar een andere PSN (skuchere-ise26-3) te sturen. Na het verlopen van de verificatietimer is dezelfde sessie niet geverifieerd op de verschillende PSN.

De figuur toont een authenticatierapport dat de failover voor de sinaasappe toont van skuchere-ise26-1 tot skuchere-ise26-3:

1. Verificatie vindt plaats op skuchere-ise26-1, autorisatieprofiel met omleiding is toegewezen.

2. CVA na een geslaagde beoordeling van de houding.

3. Volgende verificatie wanneer een autorisatieprofiel voor de compatibele status is toegewezen.

4. Verificatie raakt verschillende PSN, maar krijgt nog steeds een autorisatieprofiel voor de compatibele staat.

De sessie krijgt compatibele status op de nieuwe PSN na failover in ise-psc.log met **epm-pip** en **nsf-sessie** componenten ingeschakeld 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

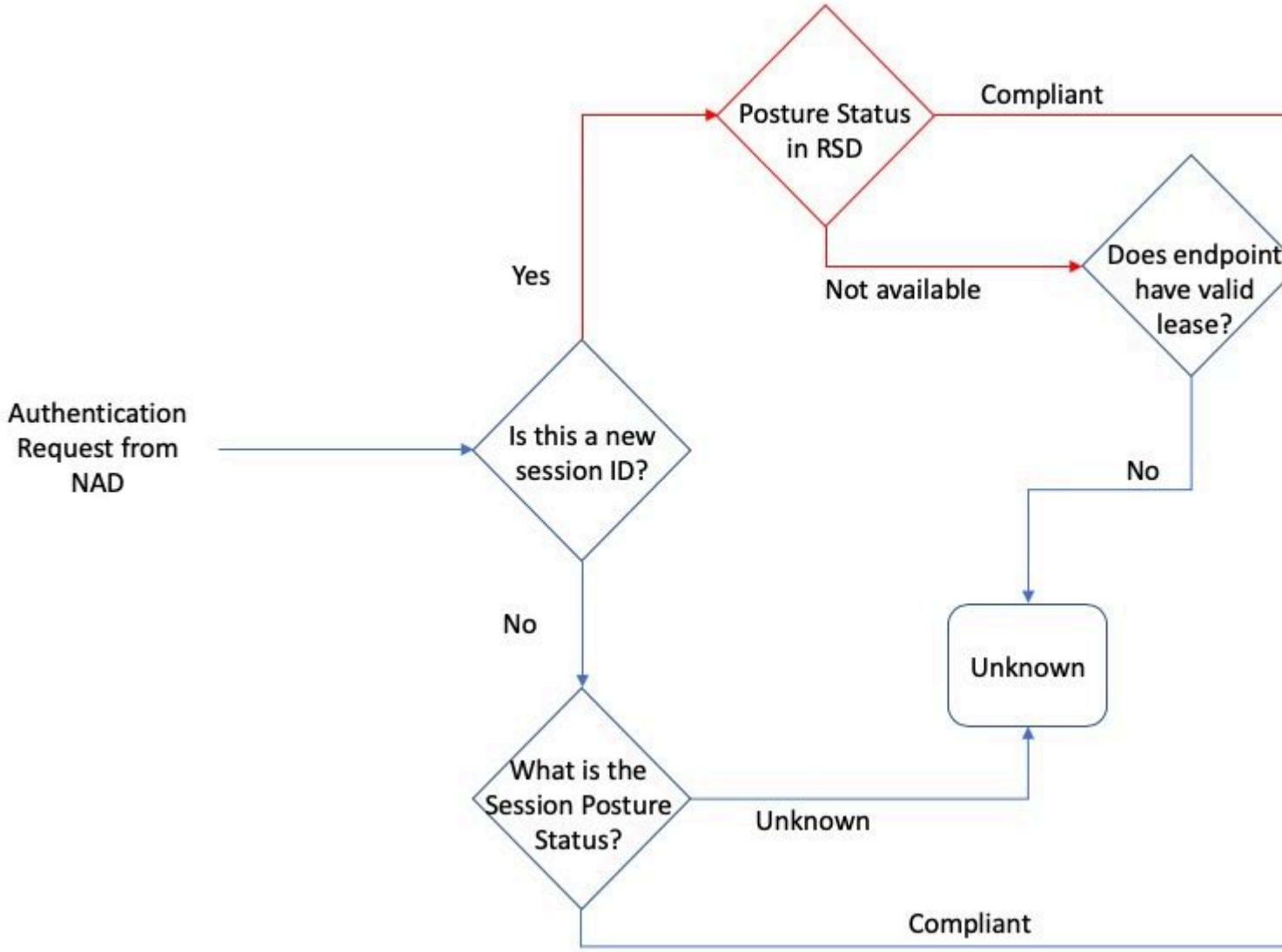
```
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution cont
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP com
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- 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

Het oorspronkelijke probleem is opgelost door extra logica toe te voegen aan het proces voor de selectie van de postuur. Het getal toont aan wat er is veranderd (wijzigingen gemarkeerd in rood):



Over deze vertaling

Cisco heeft dit document vertaald via een combinatie van machine- en menselijke technologie om onze gebruikers wereldwijd ondersteuningscontent te bieden in hun eigen taal. Houd er rekening mee dat zelfs de beste machinevertaling niet net zo nauwkeurig is als die van een professionele vertaler. Cisco Systems, Inc. is niet aansprakelijk voor de nauwkeurigheid van deze vertalingen en raadt aan altijd het oorspronkelijke Engelstalige document (link) te raadplegen.