Fehlerbehebung bei ISE-Sitzungsmanagement und Status

Inhalt

Einleitung

In diesem Dokument wird das häufige Problem mit Identity Service Engine (ISE)-Statusservices beschrieben: "Das AnyConnect **ISE-Statusmodul erfüllt ...".**

Hintergrundinformationen

In diesem Dokument wird das häufige Problem mit Identity Service Engine (ISE)-Statusservices beschrieben: Das AnyConnect **ISE-Statusmodul ist während der Wartezeit des Sitzungsstatus auf der ISE kompatibel.**

Obwohl die Symptome immer gleich sind, kann dieses Problem mehrere Ursachen haben.

Häufig ist die Behebung eines solchen Problems sehr zeitaufwendig, was schwerwiegende Auswirkungen hat.

In diesem Dokument wird Folgendes erläutert:

- Problempunkt aus Sicht der Endbenutzer und ISE-Administratoren.
- Häufige problematische Szenarien.
- Die Theorie hinter ISE, AnyConnect und Netzwerkoperationen, die das Problem auslösen.
- Algorithmen zur schnellen Problemerkennung.
- Klassische Lösungen für gängige Problemszenarien.
- Statusfreigabe über das Radius-Sitzungsverzeichnis.

Eine genauere Erläuterung der später beschriebenen Konzepte finden Sie unter:

[ISE Posture Style Comparison for Pre and Post 2.2](#)

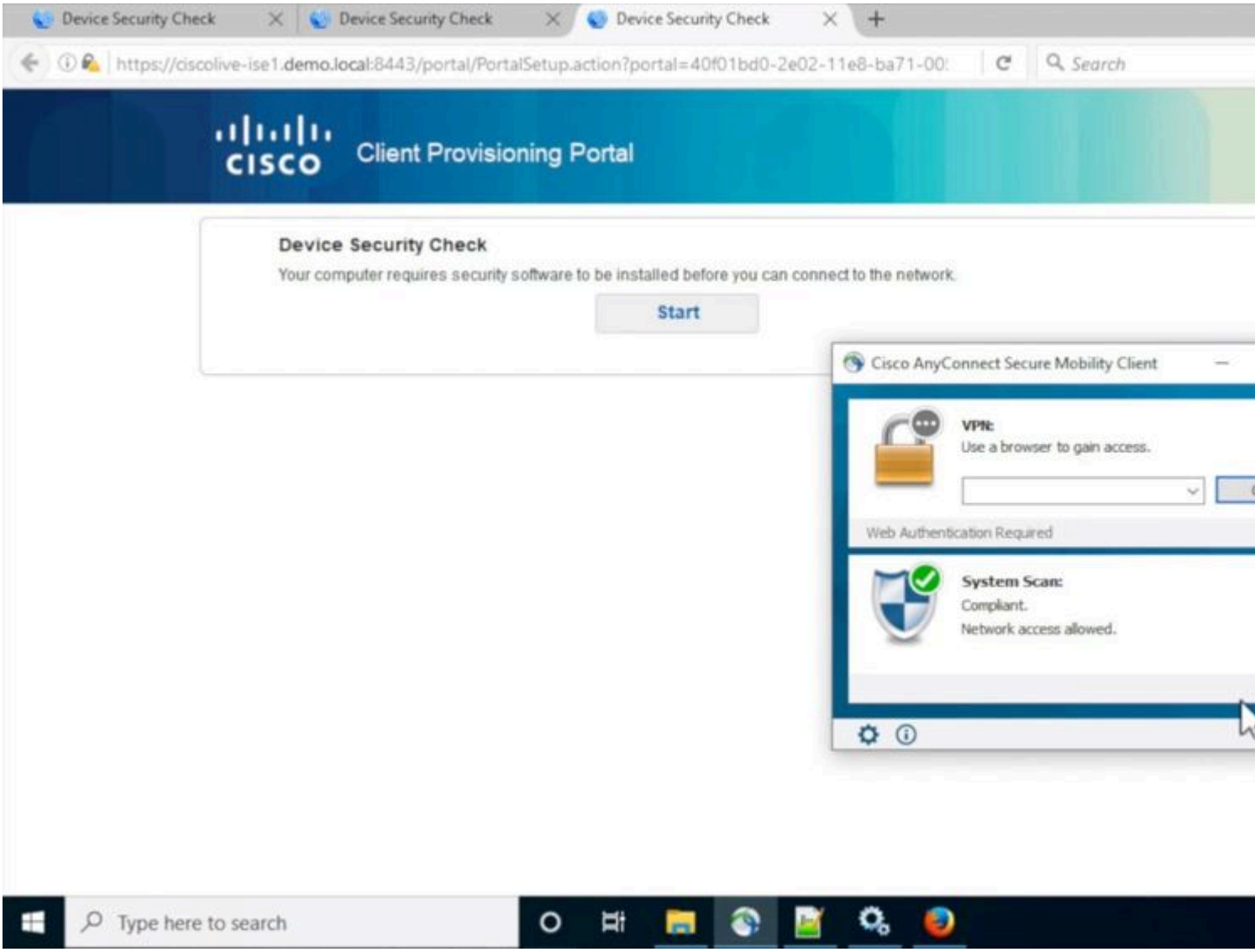
[ISE unter der Lupe. Fehlerbehebung bei ISE - BRKSEC-3229](#)

Problem

Anwendererlebnis

Dieses Problem tritt normalerweise auf, wenn kein Netzwerkzugriff oder ständige Weiterleitungen zum ISE-Client-Bereitstellungsportal im Browser vorhanden sind, während das AnyConnect ISE-Statusmodul den Status als **konform** anzeigt**.**

Typische Endbenutzererfahrung:

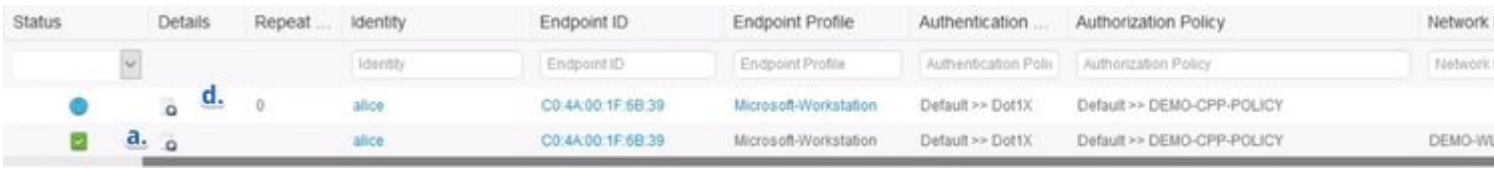


ISE-Administrationserfahrung

Normalerweise führt der ISE-Administrator bei der ersten Triage dieses Problems eine Radius-Live-Protokolluntersuchung durch, um sicherzustellen, dass eine tatsächliche Authentifizierung bei der ISE vorliegt.

Das erste in diesem Stadium erkannte Symptom weist auf eine Diskrepanz in einem Status zwischen Endpunkt und ISE hin, da in den Live-Protokollen oder RADIUS-Authentifizierungsberichten für die letzte erfolgreiche Authentifizierung des Endpunkts der Status **Ausstehender** Status angezeigt wird.

Typische ISE-Administrationserfahrung:



- Letzte erfolgreiche Authentifizierung für Alice.
- Der Status der Sitzung lautet "**Ausstehend".**
- Letzte Veranstaltung für Alice.
- Das Sitzungsereignis zeigt den Status als **konform an.**

Hinweis: c. und d. werden nicht immer in den Live-Protokollen angezeigt, wenn sie als Problemmanifeste beschrieben werden. Das Sitzungsereignis mit dem Status "**Compliant"** tritt häufiger in Szenarien auf, die durch veraltete oder Phantom-Sitzungen verursacht werden und weiter unten in diesem Dokument beschrieben werden.

Häufige Problemszenarien

Dieses Problem tritt normalerweise in zwei problematischen Szenarien auf, von denen jedes mehrere Ursachen hat. Die Szenarien:

- Das AnyConnect ISE-Statusmodul wurde während des Statusvorgangs vom Policy Service Node (PSN) falsch informiert, wodurch ein falscher Status angezeigt wurde. In diesem Fall handelt es sich normalerweise um eine veraltete oder Phantom-Sitzung im PSN-Sitzungscache.
- Die AnyConnect ISE zeigt den Status aus dem vorherigen Erkennungszyklus an, da die aktuelle Authentifizierung keinen Erkennungsvorgang ausgelöst hat. Das ISE-Statusmodul in AnyConnect weist eine begrenzte Anzahl von Ereignissen auf, die den Erkennungsprozess auslösen und möglicherweise passieren, dass bei der Authentifizierung oder erneuten Authentifizierung keines dieser Ereignisse erkannt wurde.

Veraltete/Phantom-Sitzung

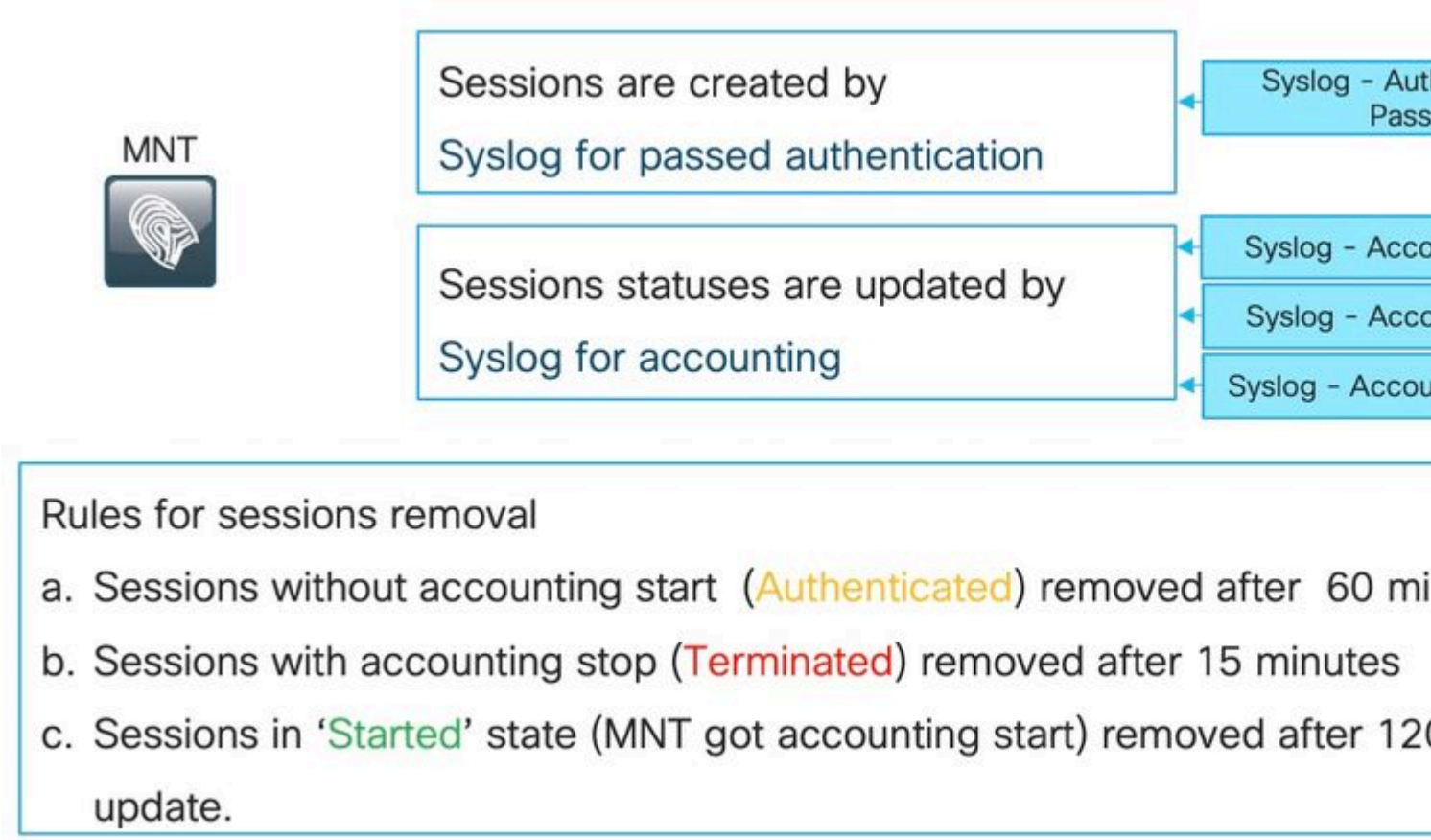
Um das Problem besser zu verstehen, sollten Sie die ISE-Sitzungsmanagementlogik und den erforderlichen AnyConnect-Erkennungsprozess untersuchen.

ISE-Sitzungsmanagement-Logik

Bei der ISE-Bereitstellung sind zwei Personen für den Sitzungsmanagementprozess verantwortlich: PSN und Monitoring Node (MNT).

Um dieses Problem richtig zu beheben und zu identifizieren, ist es wichtig, die Theorie der Sitzungsverwaltung für beide Personen zu verstehen.

MNT- und Sitzungsmanagement



Wie in diesem Bild erläutert, erstellt der MNT-Knoten Jahreszeiten auf der Grundlage der übergebenen Syslog-Authentifizierungsmeldungen, die von PSNs stammen.

Der Status einer späteren Sitzung kann vom Syslog für die Kontoführung aktualisiert werden.

Das Entfernen von Sitzungen auf MNT geschieht in drei Szenarien:

- Sitzungen ohne Accounting-Start wurden ca. 60 Minuten nach ihrer Erstellung entfernt. Alle 5 Minuten wird ein Cron-Job ausgeführt, um den Sitzungsstatus zu überprüfen und zu säubern.
- Die beendete Sitzung wurde ca. 15 Minuten nach der Verarbeitung des Abrechnungsstopps durch denselben Cron-Auftrag entfernt.
- Derselbe Cron bei jeder Ausführung entfernt auch Sitzungen, die sich seit mehr als 5 Tagen (120 Stunden) im Status "Gestartet" befinden. Ein gestarteter Zustand bedeutet, dass der MNT-Knoten sowohl die Authentifizierung als auch die Kontoverwaltung verarbeitet hat, um Syslog für die Sitzung zu starten.

Beispiele für Syslog-Meldungen von PSN. Diese Meldungen werden in prrt-server.log protokolliert, wenn die Komponente runtime-aaa in DEBUG aktiviert ist. Fett formatierte Teile können zum Erstellen von regulären Suchausdrücken verwendet werden.

Authentifizierung bestanden:

<#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, DestinationP

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=F

Anfang der Buchhaltung:

<#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=10.62.148.10

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

Aktualisierung der Zwischenabrechnung:

<#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=10.62.148.10

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

Abrechnungstopp:

<#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- und Sitzungsmanagement

Was ist der PSN-Sitzungscache?

Eine In-Memory-Datenbank, in der alle aktiven Sitzungen eines bestimmten PSN gespeichert werden. Der Sitzungs-Cache ist immer lokal für den Knoten, und es gibt keinen Mechanismus in der ISE, der eine Replikation des vollständigen Sitzungszustands von einem Knoten auf einen anderen durchführen kann.

Für jede aktive Sitzungs-ID speichert PSN alle Attribute, die während der Authentifizierungs-/Autorisierungsphase erfasst wurden, wie interne/externe Benutzergruppen, NAD-Attribute (Network Access Device), Zertifikatattribute usw. Diese Attribute werden von PSN verwendet, um verschiedene Richtlinientypen wie Authentifizierung, Autorisierung, Clientbereitstellung und Status auszuwählen.

Der Sitzungscache wurde vollständig entfernt, wenn die Dienste auf dem Knoten oder Knoten selbst neu gestartet wurden.

Durch die aktuelle Sitzungsverarbeitungslogik wird in zwei Szenarien ein neuer Eintrag im Sitzungscache erstellt. Spätere Details bestehender Sitzungen können aus Accounting-Meldungen aktualisiert werden, die von NADs stammen:

- Die Sitzung wurde auf dem PSN erfolgreich authentifiziert.
- PSN hat ein Accounting-Zwischenupdate für die Sitzung erhalten, das nicht im Sitzungscache vorhanden ist.

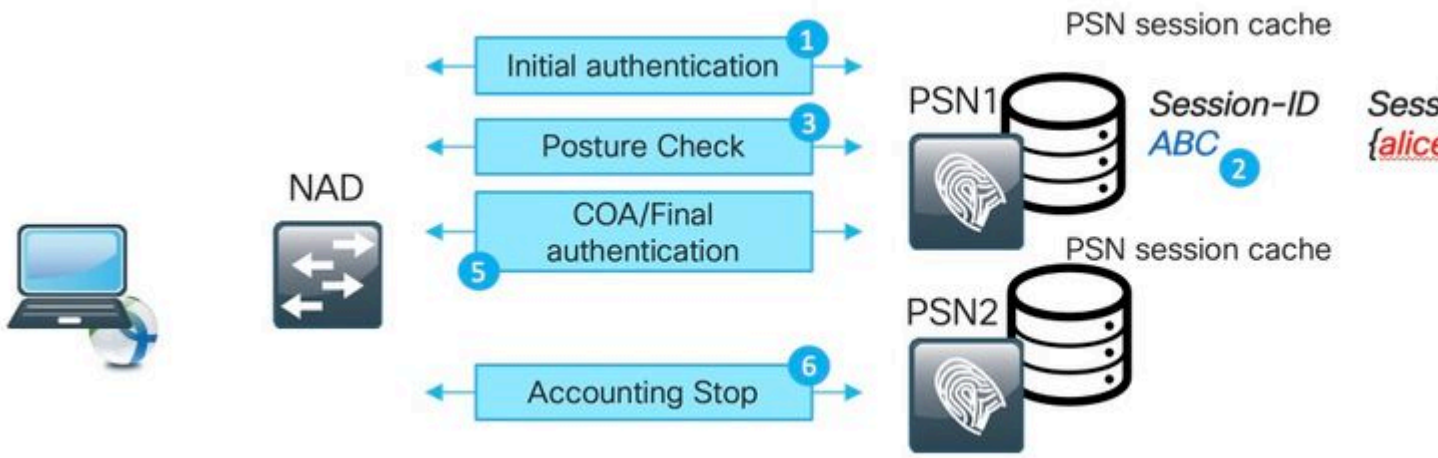
Wenn es um das Entfernen von Sitzungen geht, implementiert PSN diese Logik:

- Der Sitzungscacheeintrag wurde unmittelbar nach der Verarbeitung der Accounting-Stopp-Nachricht entfernt.
- PSN beginnt, die zuletzt verwendeten Sitzungen zu entfernen, wenn ein Knoten **die Grenze** der aktiven Sitzungen erreicht.

Veraltete Sitzung auf PSN

In der ISE-Bereitstellung wurde der Accounting-Stopp für eine vorhandene Sitzung vom PSN verarbeitet, der die eigentliche Authentifizierung nicht durchgeführt hat:

Beispiel der veralteten Sitzung:



1. Die erfolgreiche Authentifizierung erfolgt auf PSN für die Sitzung ABC.

2. PSN erstellt einen Eintrag im Sitzungscache.

3. Statusüberprüfung wird durchgeführt.

4. Sitzung als **konform** markiert.

5. Eine durch Statusänderungen ausgelöste Autorisierungsänderung (COA) führt zur erneuten Authentifizierung des Endpunkts, sodass die nächste Zugriffsebene übernommen wird.

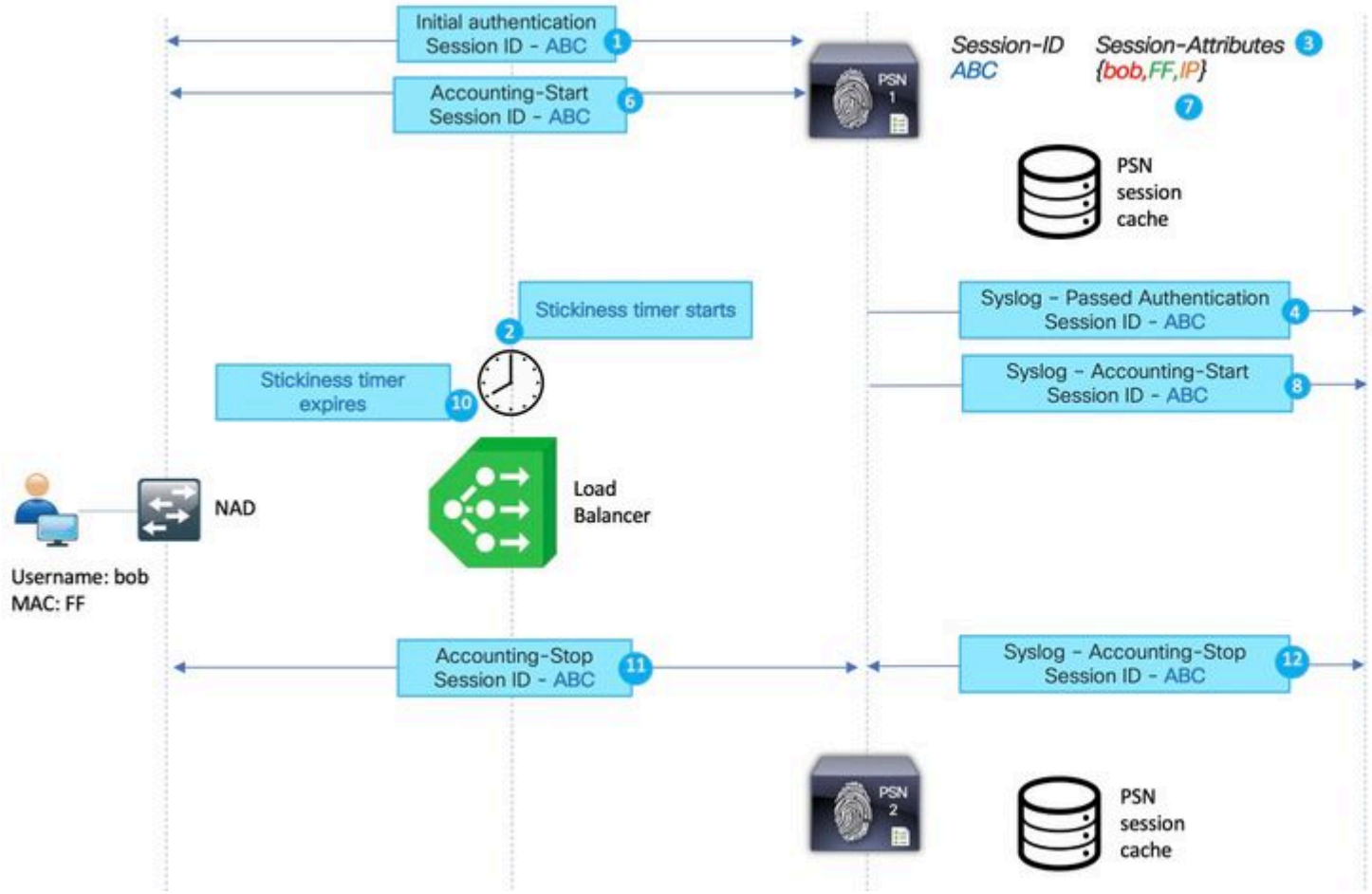
6. Der Abrechnungsstopp für die ABC-Sitzung läuft auf PSN2.

Nach Schritt 6 wird ABC auf dem PSN1 im veralteten Zustand festgehalten, da keine Accounting-Stopp-Meldung auf diesem PSN verarbeitet würde, um es zu entfernen. Die Sitzung wird für einen längeren Zeitraum entfernt, wenn bei der Bereitstellung nicht eine hohe Anzahl von Authentifizierungsversuchen auftreten.

Die veraltete Sitzung wird in folgenden Szenarien im PSN-Sitzungscache angezeigt:

- Der Abrechnungsstopp wurde aufgrund des Ablaufs des Stickiness-Timers auf dem Load Balancer falsch gesetzt.
- Die falsche Konfiguration auf dem NAD ist nicht dieselbe PSN, die für Authentifizierung und Abrechnung konfiguriert wurde.
- Temporäre Verbindungsprobleme auf dem Netzwerkpfad, die einen NAD-Failover auf das nächste PSN verursachen.

Beispiel für eine veraltete Sitzung in einer Load Balancer (LB)-Umgebung:



1. Anfängliche, von PSN 1 durchgeführte Authentifizierung für das Session-ABC.

2. Mit dieser Authentifizierung wird ein Stickiness-Timer für den Load Balancer initiiert.

3. PSN 1 erstellt einen Eintrag für das Session-ABC im lokalen Cache.

4. Syslog-Meldung für übergebene Authentifizierung wird an MNT-Knoten übertragen.

5. Eintrag für Session ABC erstellt in MNT Session Verzeichnis mit dem Status **Authentifiziert**.

6. Abrechnungsstartmeldung für Session ABC landet auf PSN 1.

7. Session-Cache-Eintrag für Session-ABC mit Informationen von Accounting-Start aktualisiert.

8. Syslog-Meldung für Accounting-Start an MNT-Knoten übertragen.

9. Sitzungsstatus auf "**Gestartet**" aktualisiert.

10. Der Stickiness-Timer läuft auf dem Load Balancer ab.

11. Accounting-Stopp für Session-ABC vom Load Balancer an PSN 2 weitergeleitet.

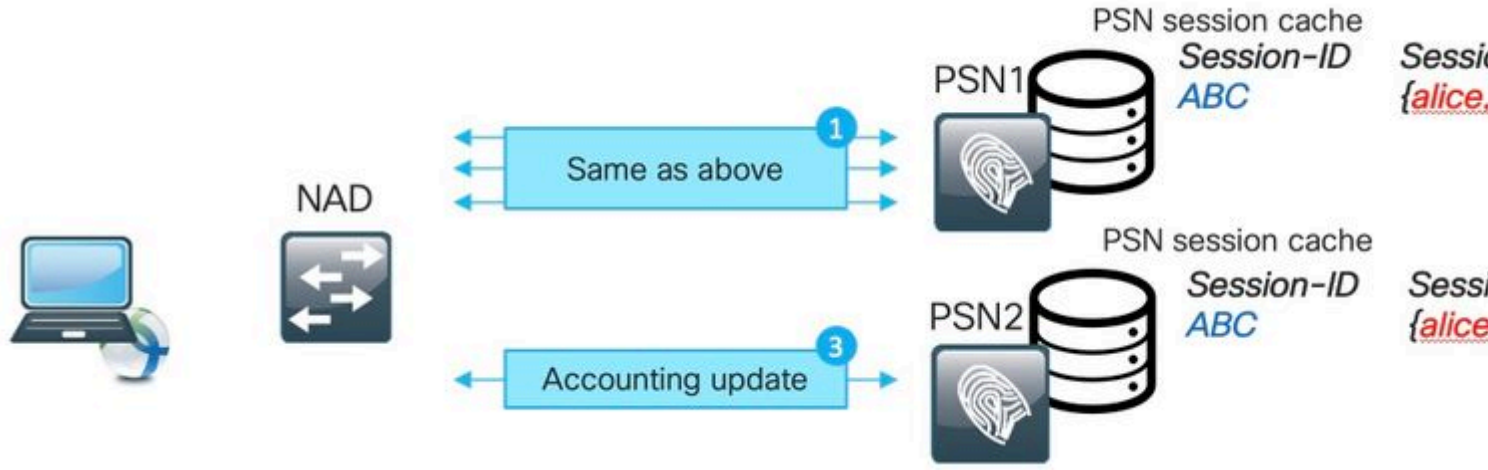
12. Syslog-Meldung für Accounting-Stopp von PSN 2 an MNT weitergeleitet.

13. Sitzung ABC als beendet auf MNT markiert.

Phantom-Sitzung auf dem PSN

Die Phantomsitzung ist ein Szenario, in dem das Accounting-Interim-Update auf das PSN kommt, das keine Authentifizierung für diese spezielle Sitzung durchgeführt hat. In diesem Szenario wird ein neuer Eintrag im PSN-Sitzungscache erstellt. Wenn PSN für diese Sitzung keine Abrechnungsstoppmeldung erhält, wird der Eintrag nur entfernt, wenn PSN die Grenze der aktiven Sitzungen erreicht.

Beispiel einer Phantom-Sitzung:



1. Die gleichen Schritte wie im Beispiel für veraltete Sitzungen werden auf PSN1 für die Sitzung ABC ausgeführt.

2. Sitzung ABC hat im PSN1-Sitzungscache den Status **Compliant**.

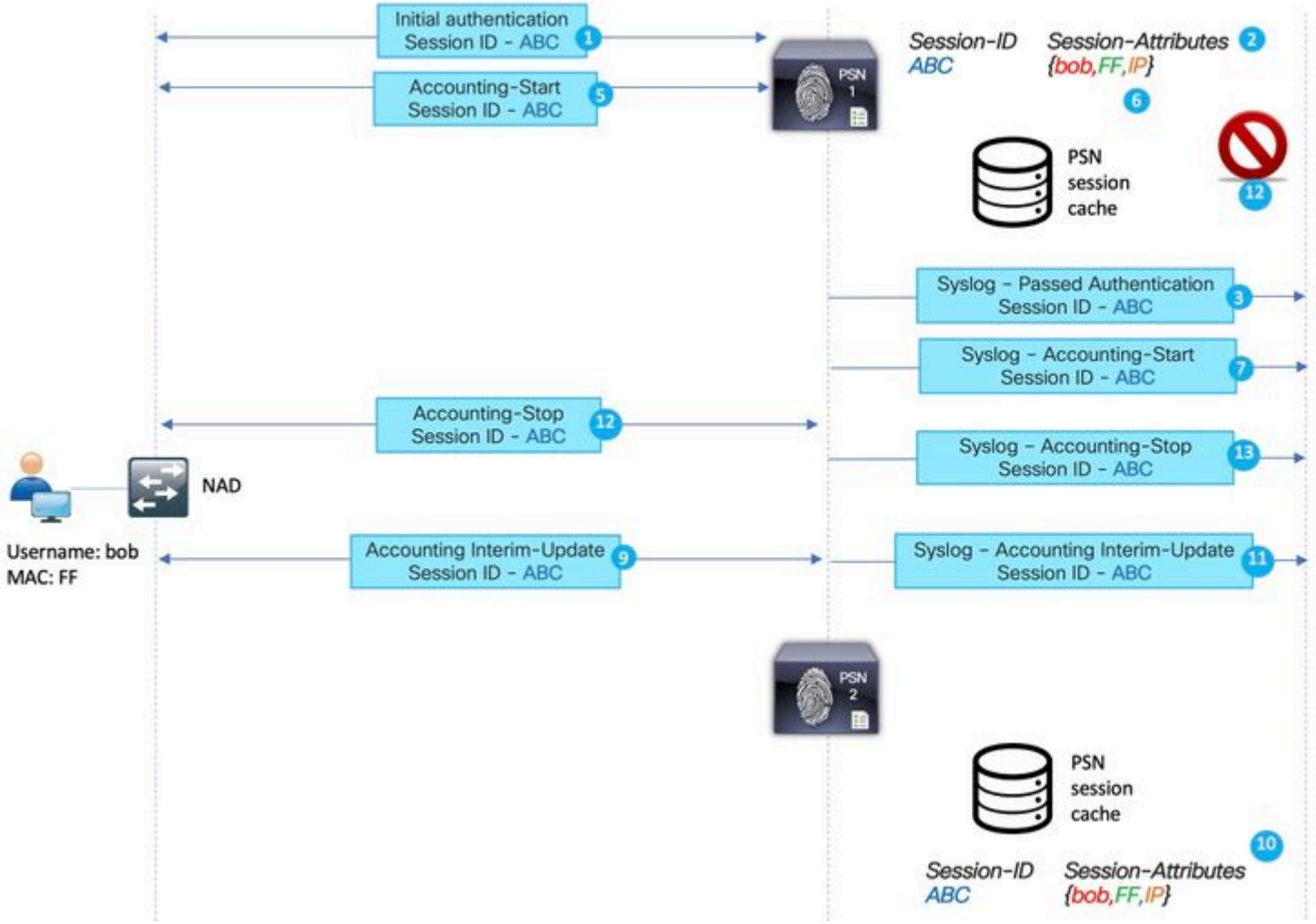
3. Accounting-Zwischenaktualisierung für Sitzung ABC trifft PSN2.

4. Session-Eintrag für Session ABC erstellt auf PSN2. Da der Sitzungseintrag aus der Abrechnungsmeldung erstellt wurde, verfügt er über eine begrenzte Anzahl von Attributen. Beispielsweise ist der Status für Sitzung ABC nicht verfügbar. Auch Funktionen wie Benutzergruppen und andere autorisierungsspezifische Attribute fehlen.

Die Phantom-Sitzung wird in folgenden Szenarien im PSN-Sitzungscache angezeigt:

- Kurzfristige Ausfälle bei der Netzwerkübertragung.
- Fehlverhalten des Netzwerkzugriffsgeräts
- Fehlerhaftes Verhalten oder falsche Konfiguration auf dem Load Balancer.

Beispiel einer Phantom-Sitzung für das Szenario mit temporären Problemen auf dem Netzwerkpfad zu PSN1:



1. Anfängliche, von PSN durchgeführte Authentifizierung für das Session-ABC.

2. PSN1 erstellt einen Eintrag für das Session-ABC im lokalen Cache.

3. Syslog-Meldung für übergebene Authentifizierung wird an MNT-Knoten übertragen.

4. Eintrag für Session ABC in TimesTen DB mit dem Status **Authentifiziert** erstellt.

5. Abrechnungsstartmeldung für Session ABC landet auf PSN 1.

6. Session-Cache-Eintrag für Session-ABC mit Informationen von Accounting-Start aktualisiert.

7. Syslog-Meldung für Accounting-Start an MNT-Knoten übertragen.

8. Sitzungsstatus auf "**Gestartet**" aktualisiert.

9. Interim-Accounting-Update für Session-ABC an PSN2 weitergeleitet.

10. PSN2 erstellt einen Eintrag für die Session ABC im lokalen Cache.

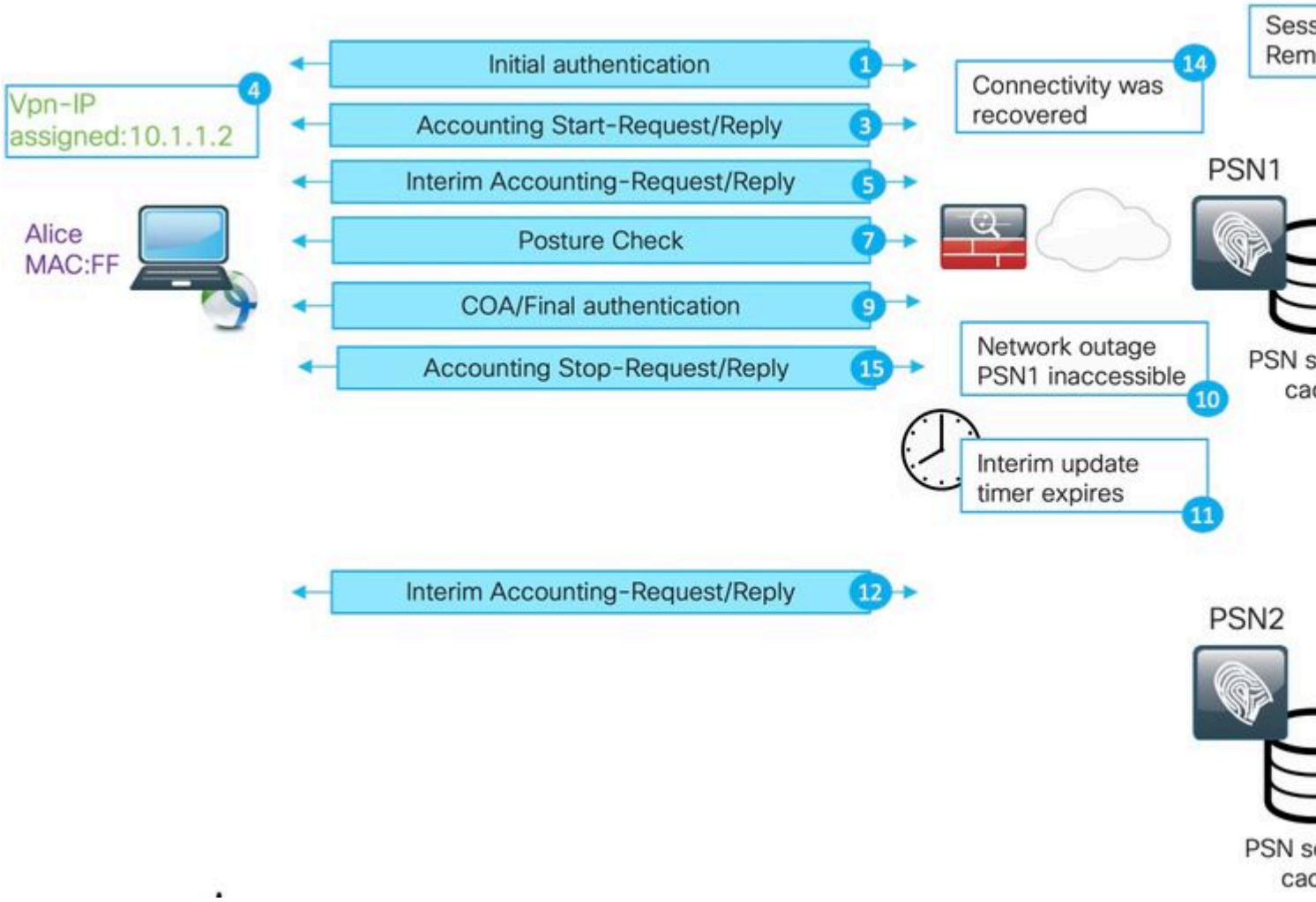
11. Accounting-Stopp für Sitzung ABC an PSN1 weitergeleitet.

12. Eintrag für Session-ABC aus dem Session-Cache von PSN1 entfernt.

13. Syslog-Meldung für Accounting-Stopp von PSN 1 an MNT weitergeleitet.

14. Sitzung ABC als beendet auf MNT markiert.

Das Szenario der Phantom-Sitzung, wie sie für die langlebige VPN-Verbindung erstellt wurde:



1. Anfängliche Authentifizierung auf PSN1.

2. Session-ABC wurde im Session-Cache erstellt.

3. Die Abrechnung startet die vom PSN verarbeitete Nachricht.

4. Die neue IP-Adresse, die dem VPN-Adapter (Virtual Private Network) zugewiesen wurde.

5. Interim Accounting-Update mit IP-Adressinformationen landet auf PSN.

6. Dem Sitzungscache wurden IP-Adressinformationen hinzugefügt.

7. Statusüberprüfung erfolgt mit PSN1.

8. Statusaktualisierung in der Sitzung

9. COA-Push, ausgeführt von der ISE, löst die Zuweisung einer neuen Zugriffsebene aus.

10. Ausfall auf dem Netzwerkpfad, wodurch PSN1 nicht zugänglich ist.

11. Nach Ablauf des vorläufigen Aktualisierungsintervalls erkennt ASA/FTD, dass auf PSN1 nicht zugegriffen werden kann.

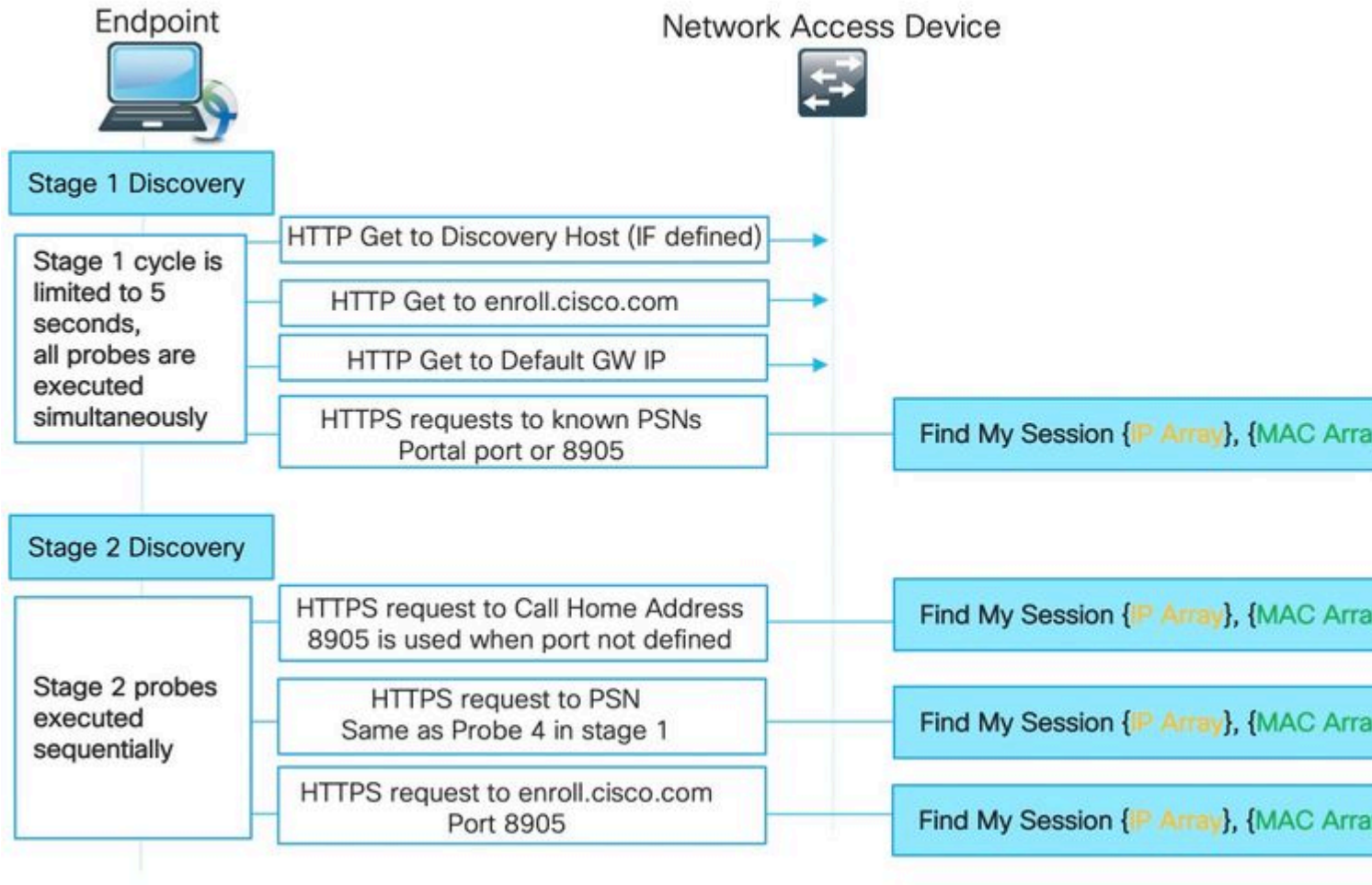
12. Das vorläufige Abrechnungsupdate wird für PSN2 bereitgestellt.

13. Die im PSN2-Sitzungscache erstellte Phantom-Sitzung.

Wenn später PSN1 zugänglich wird (14), werden dort alle nachfolgenden Abrechnungsmeldungen weitergeleitet (15,16), wodurch die Session ABC für eine undefinierte Zeit im PSN2-Session-Cache verbleibt.

Wie veraltete und Phantom-Sitzungen den Prozess der Statusüberprüfung durchbrechen?

Um zu erfahren, wie veraltete Sitzungen und Phantom-Sitzungen den Status unterbrechen, können Sie den Erkennungsprozess des AnyConnect ISE-Statusmoduls überprüfen:



Erkennung in Phase 1:

Während dieser Phase führt das ISE-Statusmodul vier gleichzeitige Probleme aus, um das PSN zu finden, das eine Authentifizierung für den Endpunkt durchgeführt hat.

Zunächst werden 3 Sonden auf der Abbildung umleitungsbasiert (Standard-GW-IP. Discovery Host IP (sofern definiert) und enroll.cisco.com IP): Diese Tests verweisen den Agenten immer auf das richtige PSN, da die Weiterleitungs-URL vom NAD selbst übernommen wird.

Der Prüfpunkt Nummer 4 wird an alle primären Server in der Datei **ConnectionData.xml** gesendet. Diese Datei, die nach dem ersten erfolgreichen Statusversuch und dem späteren Dateiinhalt erstellt wurde, kann aktualisiert werden, falls der Client zwischen PSNs migriert. Auf Windows-Systemen lautet der Dateispeicherort: **C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.**

Da alle Phase-1-Tests gleichzeitig ausgeführt werden, wird das Ergebnis von Probe 4 nur verwendet, wenn alle anderen drei Tests fehlschlugen oder das ISE-Statusmodul nicht in der Lage war, innerhalb von 5 Sekunden eine korrekte Kommunikation mit dem in der Umleitungs-URL zurückgegebenen PSN herzustellen.

Wenn Probe 4 auf dem PSN landet, enthält es eine Liste der aktiven IP- und MAC-Adressen, die auf dem Endpunkt erkannt werden. PSN verwendet diese Daten, um eine Sitzung für diesen Endpunkt im lokalen Cache zu suchen. Wenn PSN eine veraltete oder Phantom-Sitzung für den Endpunkt hat, kann dies zu einem falschen Statusstatus führen, der später auf der Clientseite angezeigt wird.

Wenn ein Agent mehrere Antworten für Probe 4 erhält (**ConnectionData.xml** kann mehr als ein primäres PSN enthalten), wird immer die schnellste Antwort verwendet.

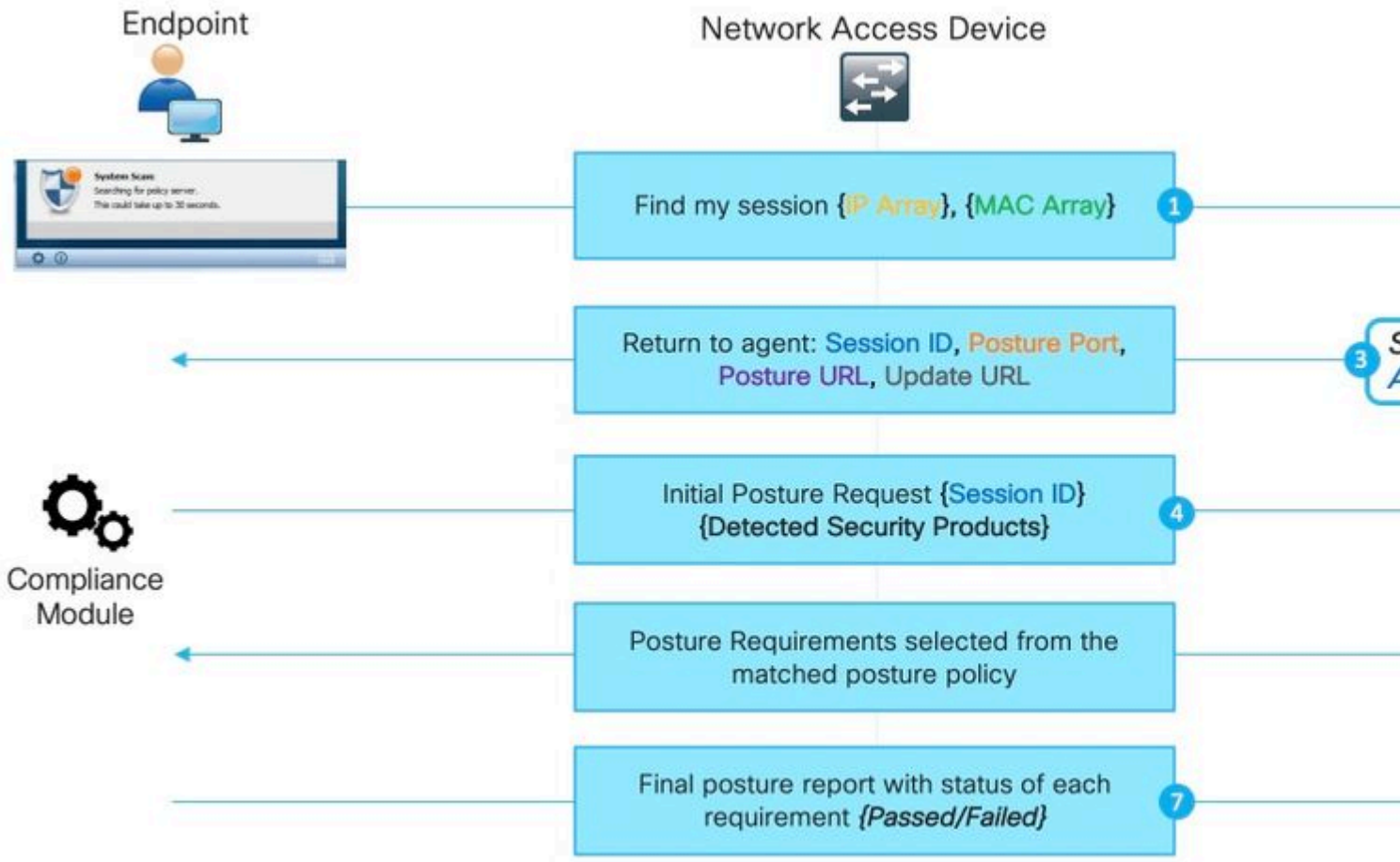
Erkennung in Phase 2:

Alle Erkennungssonden der Stufe 2 sind umleitungslos, d. h., jeder Test löst eine Sitzungssuche für das Ziel-PSN aus. Wenn PSN die Sitzung nicht im lokalen Sitzungscache findet, muss es eine MNT-Suche (nur auf Basis der MAC-Adresse) durchführen, um einen Sitzungsbesitzer zu finden und den Besitzernamen an den Agenten zurückzugeben.

Da alle Tests eine Sitzungssuche auslösen, kann die Erkennung in Stufe 2 durch veraltete oder Phantom-Sitzungen noch stärker von Problemen betroffen sein.

Wenn PSN Phase 2 erreicht, erstellt die im Sitzungscache vorhandene Erkennungssonde einen veralteten oder Phantom-Eintrag für denselben Endpunkt. Dies führt dazu, dass der Endbenutzer den falschen Status erhält.

Das Beispiel zeigt den Status, wenn PSN eine veraltete Sitzung oder eine Phantom-Sitzung hält:



Hinweis: Beachten Sie, dass dieses Problem nur auftreten kann, wenn alle umleitungsbasierten Erkennungsüberprüfungen fehlschlagen oder wenn ein Status ohne Umleitung implementiert ist.

---

1. Alle vom ISE-Statusmodul herausgegebenen **Sitzungssonden finden**

2. PSN führt eine Sitzungssuche im Sitzungscache durch. Wenn die Sitzung gefunden werden soll, tritt ein veraltetes oder Phantom-Sitzungsproblem auf.

3. PSN führt die Richtlinienauswahl für die Clientbereitstellung aus. Bei einer Phantom-Sitzung, bei der es an Authentifizierungs-/Autorisierungsattributen mangelt und alle vom Kunden konfigurierten Richtlinien sehr spezifisch sind (Richtlinien werden beispielsweise für bestimmte Active Directory-Gruppen erstellt), kann PSN keine richtige Richtlinie für die Client-Bereitstellung zuweisen. Dies kann sich in der Fehlermeldung "Bypassing AnyConnect scan your network is configured to use Cisco NAC Agent" (Scannen mit AnyConnect umgehen ist für die Verwendung von Cisco NAC Agent konfiguriert) zeigen.

- Wenn die Richtlinien für die Client-Bereitstellung allgemein sind (die in der Phantom-Sitzung verfügbaren Attribute reichen aus, um die Richtlinien mit der AnyConnect-Konfiguration abzugleichen), antwortet PSN mit den für die Fortsetzung des Bewertungsprozesses erforderlichen Details.
- Auch in diesem Schritt, wenn wir mit veralteten Sitzungen PSN-Antworten sofort mit Status **Compliant** behandeln können und nicht alle nächsten Schritte durchgeführt werden. PSN sendet kein COA, da die Sitzung seiner Meinung nach bereits konform ist. In Radius Live-Protokollen wird kein Sitzungsereignis mit dem Status **Compliant** angezeigt.

4. Im Szenario mit einer Phantom-Sitzung wird das ISE-Statusmodul mit der Anforderung für den anfänglichen Status fortgesetzt. Diese Anfrage enthält Informationen zu allen Sicherheits- und Patch-Verwaltungsprodukten, die auf dem Endpunkt erkannt wurden.

5. PSN verwendet Informationen aus den Anforderungs- und Sitzungsattributen, um die richtige Statusrichtlinie abzugleichen. Da die Phantom-Sitzung zu diesem Zeitpunkt über keine Attribute verfügt, gibt es keine übereinstimmende Richtlinie. In diesem Fall antwortet PSN auf den Endpunkt, dass er konform ist, da es sich um ein Standard-ISE-Verhalten handelt, wenn die Statusrichtlinie nicht übereinstimmt.

> **Hinweis**: Wenn es eine allgemeine Richtlinie gibt, die aus Attributen von Phantom-Sitzungen ausgewählt werden kann, fahren wir mit Schritt 6 fort.

---

6. PSN gibt die ausgewählten Statusrichtlinien an den Agenten zurück.

> **Hinweis**: Wenn keine Richtlinie ausgewählt werden kann, gibt PSN den Status "Konformität" zurück.

---

7. Der Agent gibt für jede Richtlinie/Anforderung den Status "Bestanden" oder "Fehlgeschlagen" zurück.

8. Die Berichtsauswertung erfolgt zur ISE und die Änderung des Sitzungsstatus ist **konform.**

> **Hinweis:** Bei Statusproblemen, die durch die Phantom-Sitzung verursacht werden, kann der ISE-Administrator möglicherweise einige fehlerhafte Status-COAs feststellen, da in diesem Fall COA-Anforderungen von den falschen PSNs und für falsche Sitzungs-IDs ausgeführt werden.

Der Erkennungsprozess wird bei einem neuen Authentifizierungsversuch nicht gestartet.

ISE-Statusmodul zur Überwachung einer begrenzten Anzahl von Ereignissen auf dem Endgerät, um einen Erkennungsprozess auszulösen Liste der Ereignisse, die die Erkennung auslösen:

- Erstinstallation des ISE-Statusmoduls.
- Benutzeranmeldung.
- Energieereignisse.
- Änderung des Schnittstellenstatus.
- Das Betriebssystem wird nach dem Energiesparmodus fortgesetzt.
- Ändern des Standard-Gateways (DG).
- Statusüberprüfung (PRA) fehlgeschlagen, siehe Cisco Bug-ID CSCvo69557

Neue 802.1x-Authentifizierung, PC-Entsperrung, IP-Adressänderung werden vom ISE-Statusmodul nicht erkannt.

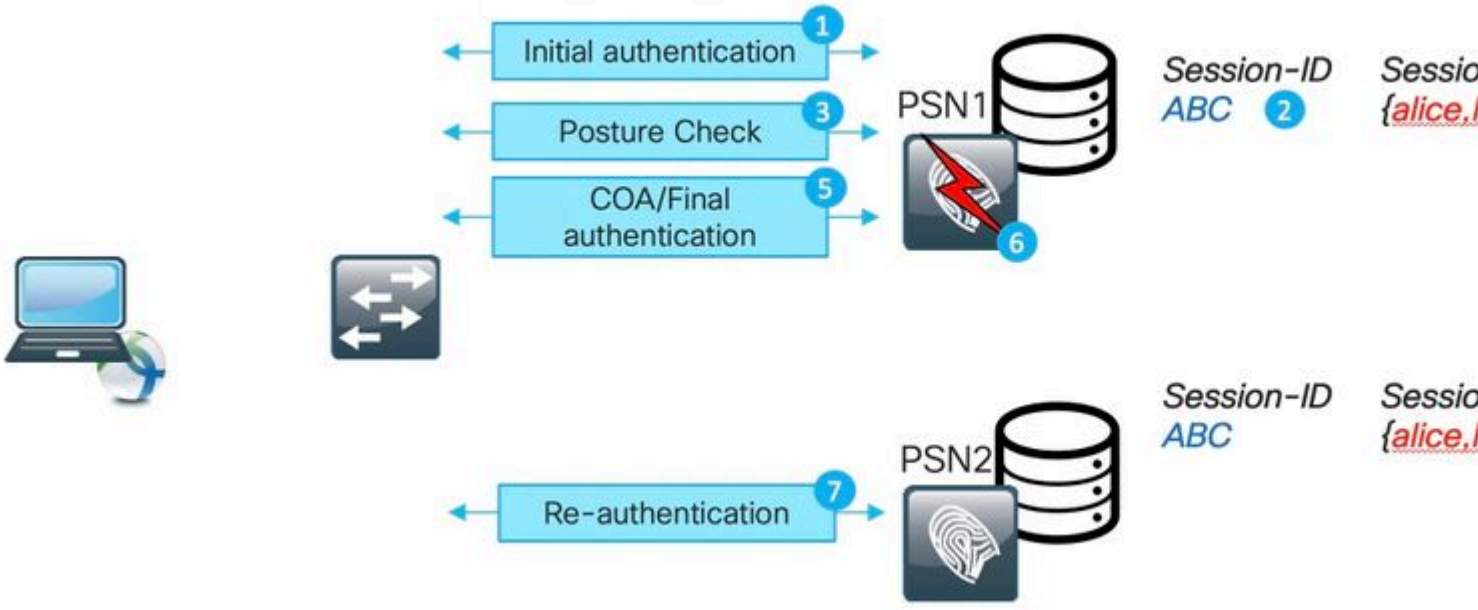
Das ISE-Statusmodul kann in den folgenden Szenarien keinen neuen Authentifizierungs- oder Neuauthentifizierungsversuch erkennen:

- Die Neuauthentifizierung trifft auf unterschiedliche PSN zu (entweder aufgrund von LB-Entscheidungen oder Problemen mit dem ursprünglichen PSN).
- NAD generiert bei der Neuauthentifizierung eine neue Sitzungs-ID.

Neuauthentifizierung auf anderem PSN

Beispiel für eine erneute Authentifizierung auf einem anderen PSN, die durch den Ausfall des

ursprünglichen PSN verursacht wurde. Das Szenario mit dem Load Balancer sieht sehr ähnlich aus. Im Fall von LB wird die erneute Authentifizierung aufgrund des Ablaufs des Stickiness-Timers an die verschiedenen PSNs weitergeleitet.



1. Anfängliche Authentifizierung auf PSN1.

2. Sitzung ABC wurde im PSN1-Sitzungscache erstellt.

3. Statusüberprüfung mit PSN1 durchgeführt.

4. Der Status des Sitzungs-ABS wird auf "**Konformität" gesetzt.**

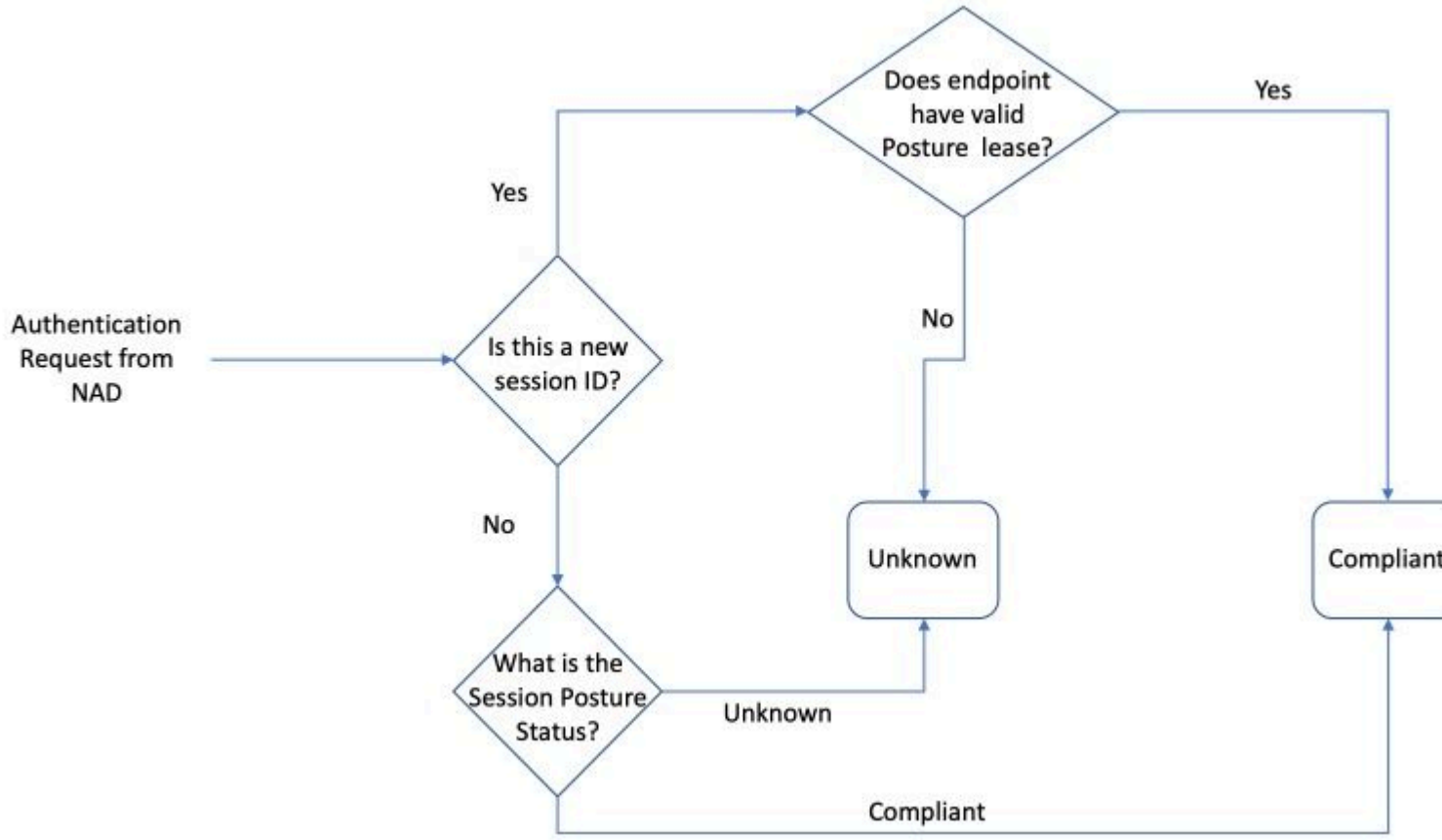
5. Ein durch Statusänderungen ausgelöster COA führt zur erneuten Authentifizierung des Endpunkts, sodass die nächste Zugriffsebene übernommen wird.

6. PSN1 ist nicht mehr verfügbar.

7. Erneute Authentifizierung für Sitzung ABC trifft PSN2.

8. Da es sich um eine neue Sitzung für den PSN2-Statusstatus der Sitzung handelt, wird sie zu **Ausstehend.**

Anfänglicher Status, der der Sitzung von PSN zugewiesen wurde:



> **Hinweis**: State-Machine beschreibt nur eine erste Auswahl des Statusstatus. Jede Sitzung, die anfänglich als "Unbekannt" markiert wurde, kann später auf Grundlage der vom ISE-Statusmodul erhaltenen Berichtsbewertung als "Compliance" oder "Non-Compliant" eingestuft werden.

NAD generiert neue Sitzungs-ID bei der Neuauthentifizierung

Dies könnte in den beiden gängigsten Szenarien geschehen:

- Die erneute Authentifizierung ist auf der ISE-Seite falsch konfiguriert. Die Lösung dieses Problems wird weiter unten in diesem Dokument behandelt.
- Fehlverhalten auf NAD-Seite - normalerweise behält NAD während des erneuten Authentifizierungsversuchs die gleiche Sitzungs-ID bei. Falls Sie feststellen konnten, dass NAD bei der erneuten Authentifizierung eine Sitzungs-ID geändert hat, handelt es sich hierbei um ein potenziell fehlerhaftes Verhalten, das im NAD selbst untersucht werden muss.

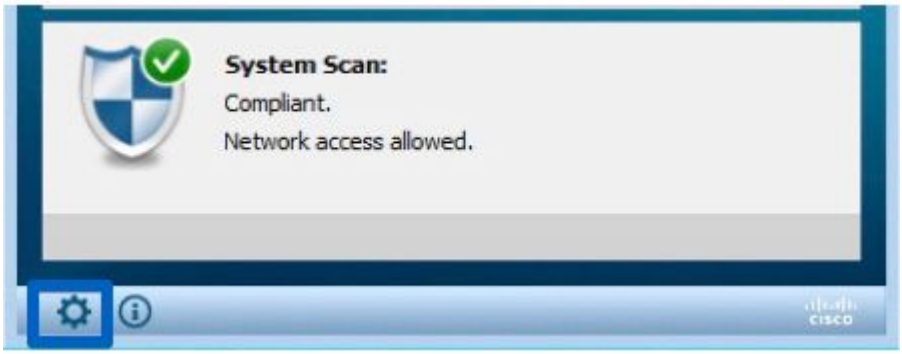
Die neue Sitzungs-ID kann auch in anderen Szenarien generiert werden. In einigen Fällen kann beispielsweise Wireless-Roaming eine Ursache dafür sein. Die Hauptsache hierbei ist, dass ISE PSN eine neue Sitzung immer in den Status "**Ausstehend" versetzt,** sofern der Status-Lease nicht konfiguriert ist. Der Leasingvertrag für Status wird weiter unten in diesem Dokument erläutert.

Schnelle Identifizierung, wann das Problem durch die veraltete/Phantom-Sitzung verursacht wurde

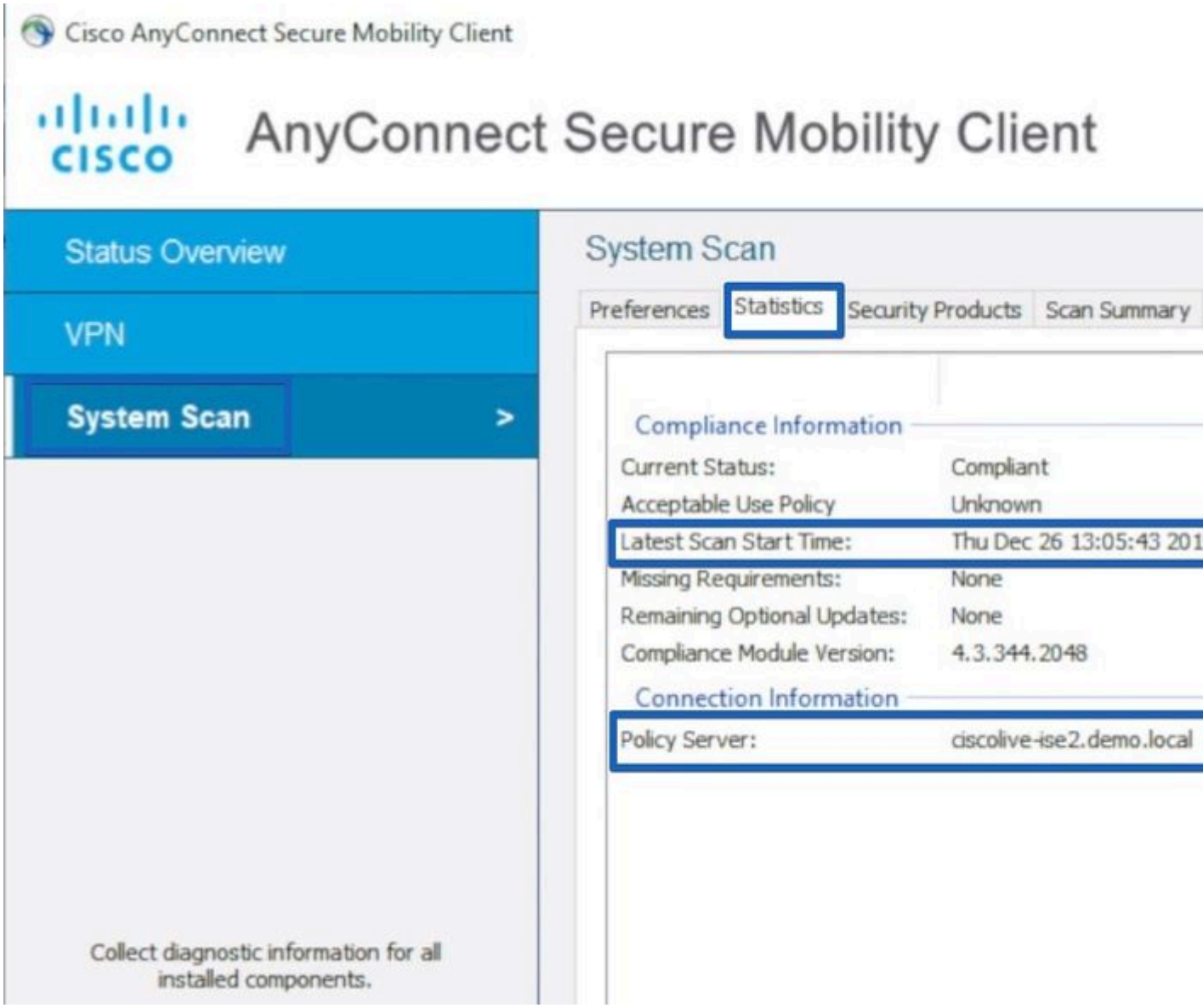
Um festzustellen, ob AnyConnect die Compliance zeigt, während sich der Umleitungsstatus in der veralteten/Phantom-Sitzung befindet, müssen wir Zugriff auf den Endpunkt erhalten, während dieser sich im problematischen Zustand befindet.

1. Systemscan-Details untersuchen:

    1. Klicken Sie auf das Zahnrad-Symbol in der AnyConnect-Benutzeroberfläche.



    2. Navigieren Sie im neuen Fenster zur Registerkarte "Systemscan" und zur Unterregisterkarte "Statistics".



    Beachten Sie dabei zwei Aspekte:

- Latest Scan Start Time (Neueste Scan-Startzeit): Der Zeitstempel hier muss nahe der Zeit liegen, zu der das Problem erkannt wurde.
- Policy Server: In diesem Feld wurde der Name des Policy Servers angegeben, der eine Statusüberprüfung für den Endpunkt durchgeführt hat. Der FQDN von hier muss mit dem FQDN von Redirect-URL (für Redirect Base Posture) oder mit dem PSN-Namen vom letzten Authentifizierungsversuch (für Redirect-less Posture) verglichen werden.

2. Vergleichen Sie den FQDN des Policy Servers aus der Systemscanstatistik mit dem Knotennamen, der die Authentifizierung für den Endpunkt durchgeführt hat:

Im vorliegenden Beispiel stimmt der Name nicht überein. PSN mit dem Namen ciscolive-ise2 enthält eine veraltete oder Phantom-Sitzung für diesen Endpunkt.

Die Demo zeigt die Aufzeichnung der Schritte zur Problemermittlung:

Erweiterte Fehlerbehebung bei veralteten/Phantom-Sitzungen

Im vorherigen Beispiel wird das Problem einer veralteten oder Phantom-Sitzung vom Problem des Erkennungsvorgangs unterschieden, der nicht gestartet wurde. Gleichzeitig müssen wir die eigentliche Sitzung identifizieren, die das Problem ausgelöst hat, um besser verstehen zu können, wie es zu einem veralteten oder Phantom-Sitzungsproblem wird.

Während in einigen Szenarien veraltete und Phantom-Sitzungen nicht vermieden werden können. Wir müssen sicherstellen, dass in der Umgebung keine veralteten Sitzungen erstellt werden, da einige der Best Practices nicht implementiert wurden.

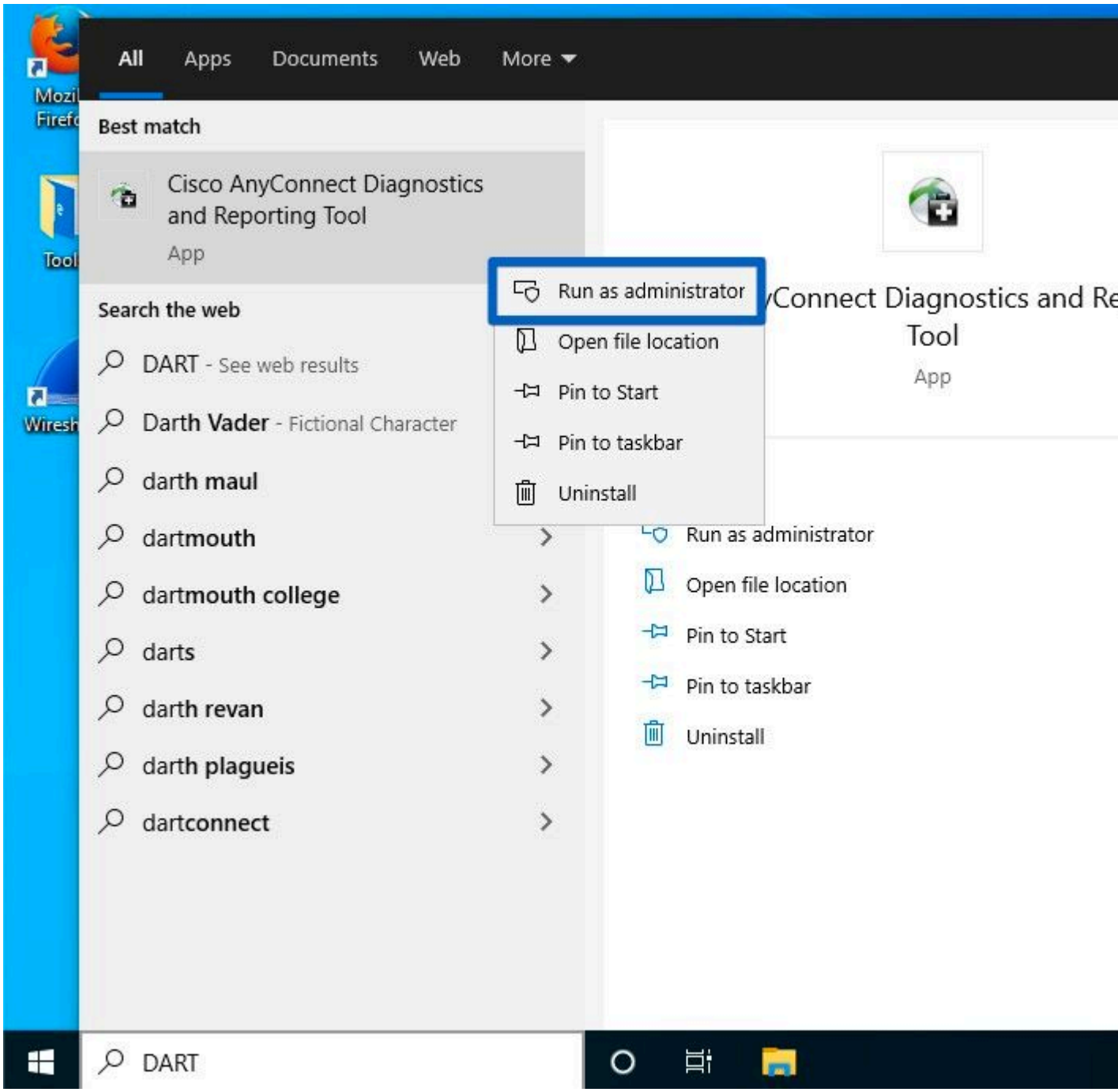
DART-Paketsammlung

Analyse eines DART-Pakets vom Endgerät, das das Problem reproduziert

- Führen Sie nur wichtige Protokolle im DART. Es wird empfohlen, die Protokolle zu löschen, bevor das Problem reproduziert wird.

Um dies zu erreichen, muss das DART-Paketdienstprogramm als Administrator starten und die Protokollbereinigung durchführen.

1. Navigieren Sie unter Windows zu Start, und beginnen Sie mit der Eingabe von DART, klicken Sie mit der rechten Maustaste, und wählen Sie - **Als Administrator ausführen.**



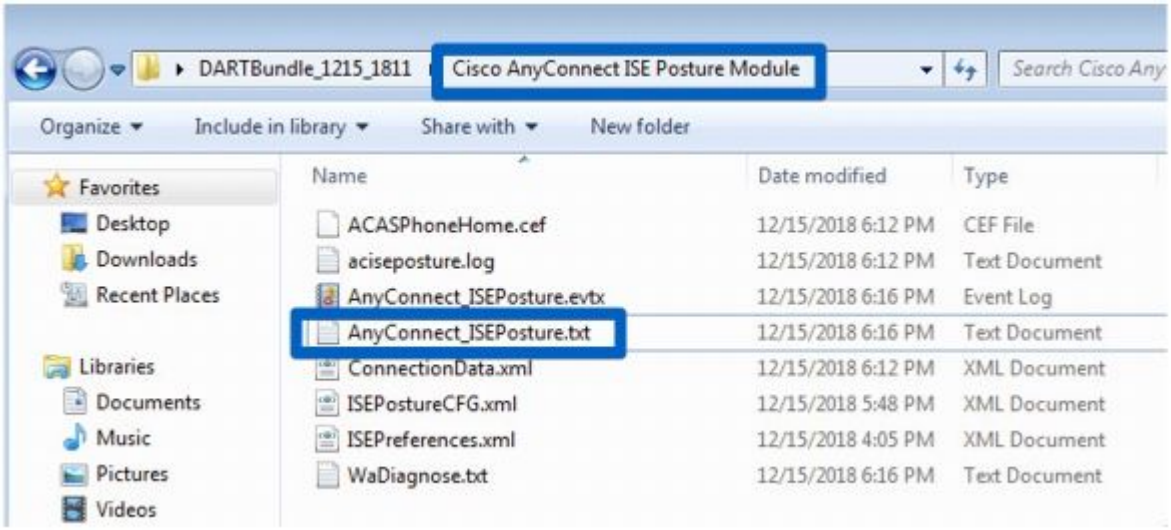
2. Drücken Sie im ersten Bildschirm des Assistenten auf Weiter.

3. Drücken Sie im nächsten Assistenten auf Alle Protokolle löschen.

4. Nachdem das Problem reproduziert wurde, kann DART von hier erfasst werden. Drücken Sie **Weiter**.

DART-Paketanalyse

Nachdem das DART-Paket gesammelt wurde, müssen wir die Archivierung aufheben und uns auf die Datei **AnyConnect_ISEPosture.txt** konzentrieren, die sich im Ordner **Cisco AnyConnect ISE Posture Module** befindet. Diese Datei enthält alle erkennungsbezogenen Ereignisse.



1. Starten Sie die Fehlerbehebung, und identifizieren Sie alle Momente des Neustarts der Erkennung. Die zu suchenden Schlüsselwörter sind "**Neustarten der Erkennung"** oder "HTTP-Erkennung". Navigieren Sie hier zu der Zeile mit dem Neustart der Erkennung, der im problematischen Moment stattfand:

```
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. Ein paar Zeilen nach dem Neustart der Erkennung sehen Sie eine Zeile, die - Probing no MNT stage targets enthält. Dies ist ein Indikator für den Erkennungsstart in Phase 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
```

Es wird empfohlen, alle umleitungsbasierten Tests mit derselben Farbe zu markieren, während zuvor verbundene PSNs aus **ConnectionData.xml (**Auth-Status-Ziele) in verschiedenen Farben hervorgehoben werden müssen, da PSN-FQDNs normalerweise sehr ähnlich sind und der Unterschied schwer zu erkennen ist.

3.Lesen Sie die Log-Dateien, um ein Ergebnis für jede einzelne Probe zu sehen. Wie bereits gesagt wurde, müssen alle auf der Umleitung basierenden Tests fehlschlagen, wenn das Problem durch eine veraltete/Phantom-Sitzung verursacht wird. Dies ist ein Beispiel dafür, wie die fehlgeschlagene Überprüfung aussieht:

```
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. Irgendwo in der Datei nach dem Neustart der Erkennung für Stufe 1 oder Stufe 2 wird eine erfolgreiche Antwort von einem oder mehreren PSNs angezeigt:

```
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. Ein paar Zeilen später gibt es eine Zeile mit dem Schlüsselwort **MSG_NS_SWISS_NEW_SESSION.** Diese Zeile enthält eine tatsächliche Sitzungs-ID, die von PSN als Ergebnis der Sitzungssuche ausgewählt wurde. Verwenden Sie diese Sitzungs-ID für weitere Untersuchungen der ISE, um herauszufinden, wie diese Sitzung veraltet/Phantom wird:

```
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
```

Untersuchung zu ISE-Protokollen

Im guest.log mit aktivierter **clientwebapp**-Komponente in DEBUG ist der PSN zu sehen, der mit der Stale/Phantom-Sitzung antwortet.

PSN erhält eine Anfrage vom ISE-Statusagenten. Sie können sehen, dass es sich um eine Anforderung von AnyConnect aufgrund des User-Agent-Werts handelt:

<#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

Die Anforderung enthält Arrays aus IP- und MAC-Adressen. In diesem Beispiel enthält jedes Array nur einen Wert. Das Protokoll zeigt außerdem an, dass die Sitzungs-ID der Anforderung NULL ist. Dies bedeutet, dass es sich um eine Anforderung des nicht umleitungsbasierten Tests handelt.

Später können Sie sehen, wie Werte aus Arrays zum Auffinden einer Sitzungs-ID verwendet werden:

<#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

Nach der Zeile mit den Schlüsselwörtern **Gesendet http-Antwort** können Sie den Inhalt der tatsächlichen Antwort sehen:

<#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

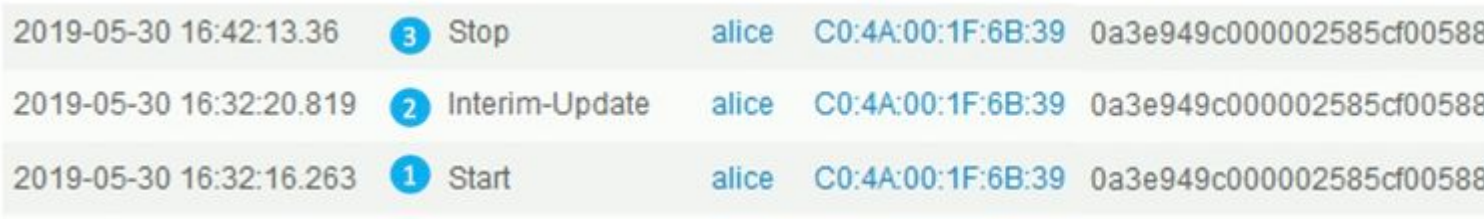
```
cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-AC_PKG_PORT value is 8443

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
```

Untersuchung zu ISE-Berichten

Nachdem Sie die ID der veralteten/Phantom-Sitzung kennen, können Sie den Radius-Accounting-Bericht untersuchen, um ein besseres Verständnis darüber zu erhalten, was diese Sitzung veraltet/Phantom wurde:

- Navigieren Sie zu Operations > Reports > Endpoints and Users > Radius Accounting-Bericht, und führen Sie diesen Bericht 7 Tage lang aus. Benutzer eine Endpunkt-ID als Filterschlüssel.

Beispiel eines Berichts, der zeigt, wie veraltete Sitzungen auf ciscolive-ise2 zurückbleiben:



1. Der Accounting-Start für die Sitzung erfolgte über das PSN ciscolive-ise2
2. Die Zwischenaktualisierung für die Sitzung wurde auf demselben PSN verarbeitet.
3. Die Abrechnungsstoppmeldung für die problematische Sitzungs-ID wurde an verschiedene PSN gesendet (ciscolive-ise1).

Eine schnelle Methode zur Identifizierung, wann das Problem durch das Fehlen eines Discovery-Neustarts verursacht wurde

Hier gilt dieselbe Logik wie für die vorherige Ausgabe. Der einzige Unterschied besteht darin, dass Sie sich auf die letzte Startzeit des Scans konzentrieren müssen. Bei dieser Art von Problem liegt der Zeitstempel des letzten Scans irgendwo in der Vergangenheit.

Wenn der Endbenutzer ein Problem erkennt, wird normalerweise ein Scan angezeigt, der vor einiger Zeit durchgeführt wurde. Während der ISE Radius Live-Protokolle werden die letzten Authentifizierungsversuche vom problematischen Endpunkt festgestellt.

Die Demo zeigt die Aufzeichnung der Schritte zur Problemermittlung:

Erweiterte Fehlerbehebung Fehlende Erkennung Neustart

Der Ansatz hier ähnelt dem Abschnitt "Erweiterte Fehlerbehebung bei veralteten/Phantom-Sitzungen". Das wichtigste Element der Fehlerbehebung ist die Untersuchung des DART-Pakets. Innerhalb des DART-Pakets können Sie nach Erkennungsneustarts suchen, wie sie für das vorherige Problem gezeigt wurden, und bestätigen, dass zum Zeitpunkt der Problemmeldung kein Erkennungsneustart stattgefunden hat.

Auf der ISE-Seite sollten Sie sich auf den Radius Live Logs/Radius-Authentifizierungsbericht konzentrieren, um sicherzustellen, dass entweder ein Failover zwischen PSNs stattgefunden hat oder dass von NAD eine neue Sitzungs-ID generiert wurde.

Lösung

Klassischer Ansatz - Vermeidung von Problemen

In der Vergangenheit gab es keine Funktion für die ISE, die die in diesem Dokument beschriebenen Probleme lösen konnte. Die einzige Möglichkeit bestand daher darin, sich auf die Best Practices zu verlassen, die auf dem Netzwerk und der ISE-Seite implementiert werden, um Risiken zu minimieren.

Best Practices zur Minimierung veralteter oder Phantom-Sitzungen bei der ISE-Bereitstellung

Implementieren Sie, wenn möglich, stets einen auf Umleitung basierenden Status.

Ein gängiges Gegenargument zu dieser Empfehlung ist ein schlechtes Anwendererlebnis, da Popup-Fenster im Betriebssystem oder Browser eine Umleitung anzeigen, während das AnyConnect ISE-Statusmodul im Hintergrund einen Bewertungsprozess durchführt.

Als Lösung hierfür ist es möglich, NUR ISE Posture-Modul-Erkennungssonden umzuleiten und selektiv den gesamten anderen Datenverkehr zuzulassen.

Das Beispiel zeigt eine Umleitungszugriffskontrollliste, die nur zum Umleiten von HTTP-Anforderungen an den Discovery Host (in diesem Beispiel 10.1.1.1) und an enroll.cisco.com (172.16.1.80) entwickelt wurde:

```
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
```

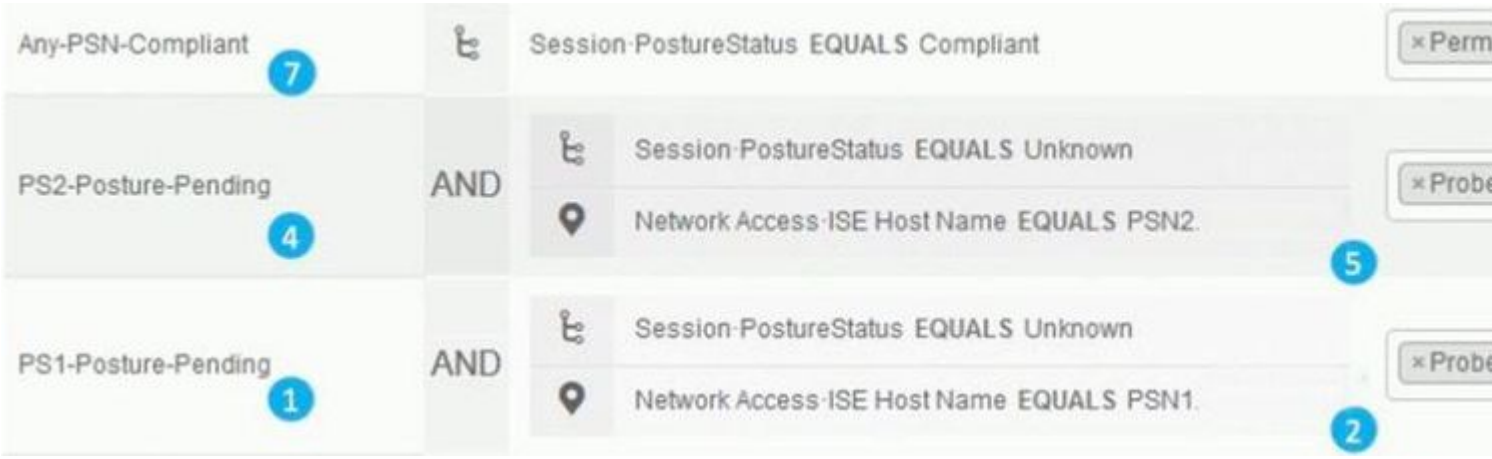
Um ein akzeptables Maß an Sicherheit zu gewährleisten, kann eine solche Umleitungs-ACL mit einer von der ISE zugewiesenen DACL kombiniert werden.

Ausstehend - Ermöglicht Verbindungen nur mit PSN, wenn das Endgerät authentifiziert wurde

Dieser Ansatz eignet sich für Umgebungen, in denen die URL-Umleitung nicht unterstützt wird (z. B. Implementierungen mit NADs von Drittanbietern).

Als Lösung müssen Sie mehrere **PosturePending**-Autorisierungsrichtlinien (eine pro PSN) implementieren. Jede Richtlinie muss als eine der Bedingungen den Namen des PSN enthalten, bei dem die Authentifizierung erfolgt ist. Im Autorisierungsprofil, das jeder Richtlinie zugewiesen ist, muss der Zugriff auf alle PSNs mit Ausnahme des Knotens blockiert werden, an dem die Authentifizierung erfolgt ist.

Erstellen von Autorisierungsrichtlinien für die Bereitstellung von 2 Knoten:



â€ƒ

1. Status **Ausstehende** Richtlinie für PSN1.

2. Der in der Richtlinie als Bedingung verwendete Name PSN1.

3. Autorisierungsprofil mit ACL, das den Zugriff auf alle PSNs außer PSN1 blockiert.

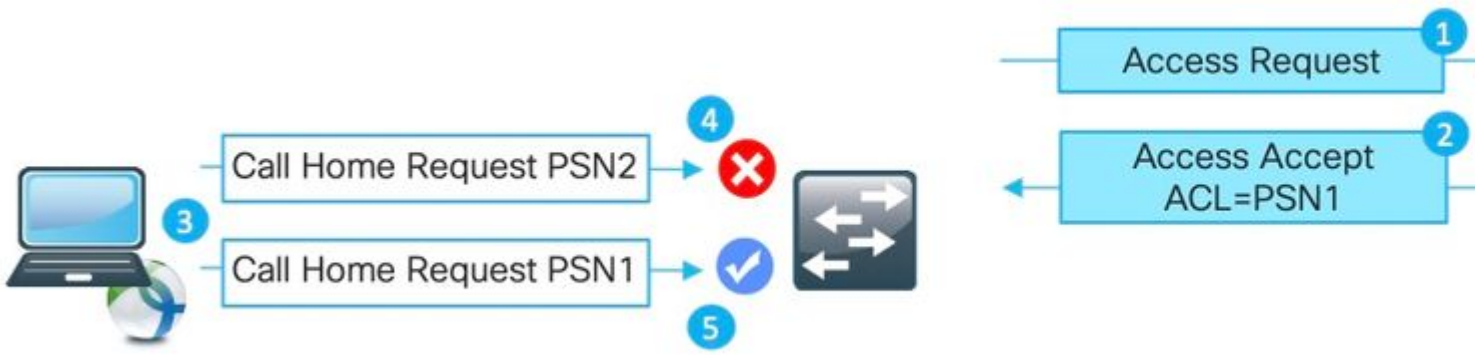
4. Status **Ausstehende** Richtlinie für PSN2.

5. Der in der Richtlinie als Bedingung verwendete PSN2-Name.

6. Autorisierungsprofil mit ACL, das den Zugriff auf alle PSNs außer PSN2 blockiert.

7. Integritätsrichtlinie "Konforme" Autorisierung.

Die Abbildung erklärt, wie dieser Ansatz funktioniert:



1. Die Authentifizierung trifft auf PSN1.

2. Als Ergebnis der konfigurierten Autorisierungsrichtlinien weist PSN1 ein Autorisierungsprofil zu, das den Zugriff auf alle anderen Knoten mit Ausnahme von PSN1 blockiert.

3. Das AnyConnect ISE-Statusmodul startet den Erkennungsprozess neu.

4. Anfrage an PSN2, die vom NAD wie von einer zuvor zugewiesenen ACL blockiert wurde.

5. Der Test für PSN1 ist durch die auf NAD zugewiesene ACL zulässig.

Load Balancer - Best Practices

- Stickiness auf LB für Authentifizierung und Abrechnung mit Calling-Station-ID als Stickiness-Schlüssel aktiviert. Weitere Informationen zu LB Best Practices für ISE finden Sie hier.
- Verwenden Sie einen Verklebungszeitgeber, der länger als ein durchschnittlicher Arbeitstag ist, um den Moment abzudecken, in dem der PC in den Schlaf geht (z. B. 10 statt 8 Stunden).
- Falls eine erneute Authentifizierung implementiert ist, verwenden Sie einen etwas niedrigeren Timer für die erneute Authentifizierung als den Stickiness-Timer (z. B. 8 Stunden, wenn Stickiness für 10 Stunden konfiguriert ist). Dadurch wird sichergestellt, dass das Stickiness-Intervall durch eine erneute Authentifizierung verlängert wird.

Statusüberprüfung beim VPN-Anwendungsfall

- Stellt sicher, dass das Accounting-Interim-Aktualisierungsintervall höher oder gleich dem vpn-session-timeout ist. Dadurch wird vermieden, dass bei langlebigen VPN-Sitzungen die Abrechnung zwischen den PSNs hin und her schwankt.

Dieses Beispiel zeigt das Interim Accounting-Aktualisierungsintervall, das für 20 Stunden konfiguriert wurde. Das anfängliche Zwischenupdate, das die dem Endpunkt zugewiesene IP-Adresse enthält, wird dadurch nicht verhindert.

```
aaa-server ISE protocol radius

 interim-accounting-update periodic 20

group-policy SSL-VPN attributes

 vpn-idle-timeout 1200

 vpn-session-timeout 1200
```

Best Practices können implementiert werden, um die Auswirkungen eines fehlenden ISE-Statusmodul-Erkennungsneustarts zu minimieren

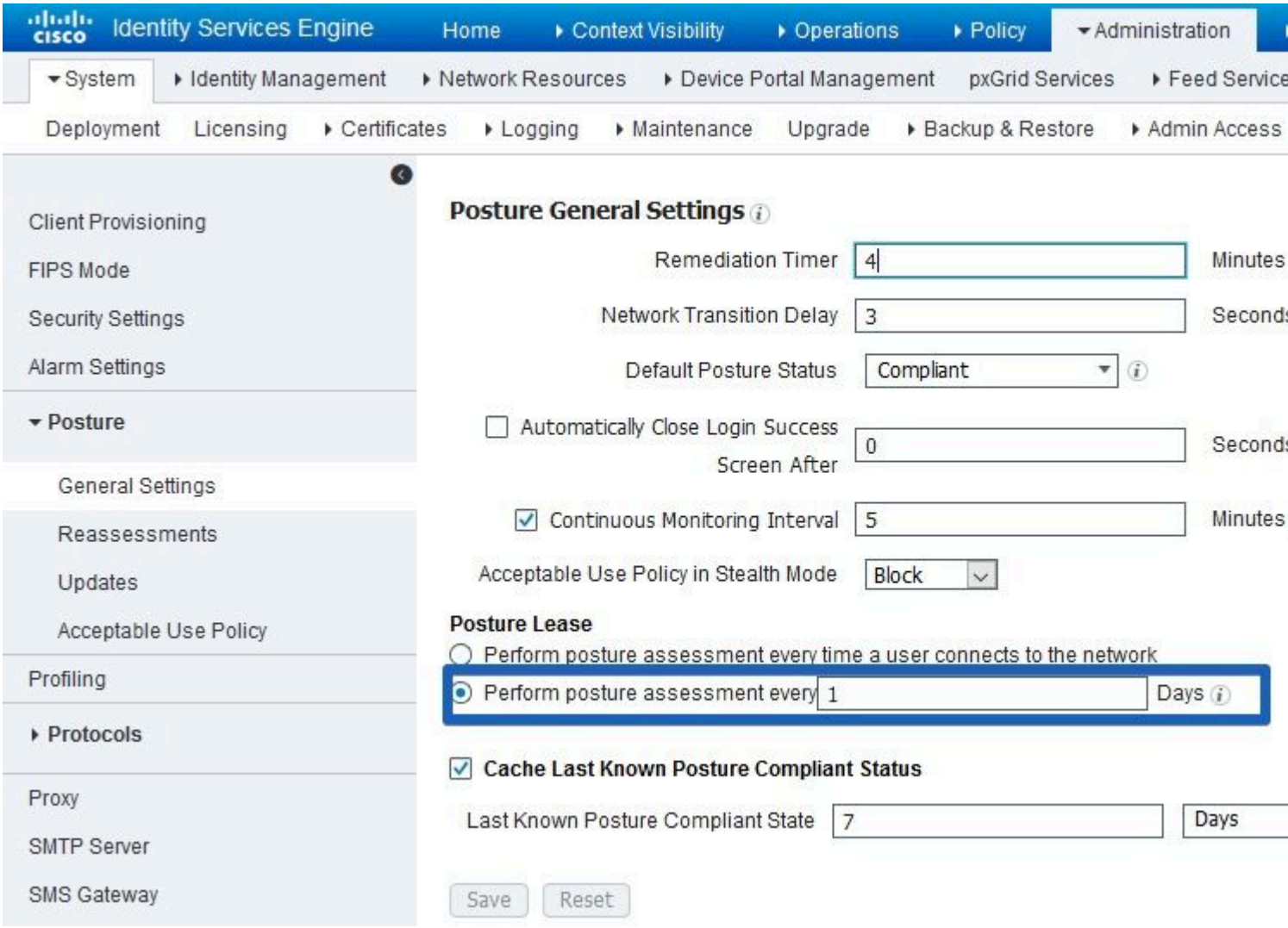
Statusleasing aktivieren

Dies ist eine Funktion auf der ISE, die einen Endpunkt für einen definierten Zeitraum (1-365 Tage) als konform markiert. Der Status-Leasingwert ist ein Endgeräteattribut, d. h., er wird in der ISE DB gespeichert. Alle Endpunkteigenschaften, die Statusleasing umfassen, werden über alle Knoten in der ISE-Bereitstellung repliziert.

Wenn PSN eine neue Sitzung für den Endgerätestatus erhält, kann die Sitzung sofort als **konform** markiert werden.

Für diese Entscheidung verwendet PSN drei Werte. Diese Werte sind:

- Für Statusleasing in ISE-Einstellungen definierte Anzahl von Tagen: **Navigieren Sie zu Administration > System > Posture > General Settings**:



- Wert des PostureExpiry-Attributs - Dies ist ein tatsächliches Endpunktattribut, das einen Epoch-Zeitstempel enthält. PostureExpiry-Wert wird anfänglich beim ersten erfolgreichen Statusversuch für Endpunkt aufgefüllt, nachdem der ISE-Administrator das Statusleasing aktiviert hat. Später wurde dieser Wert beim nächsten erfolgreichen Statusversuch aktualisiert, der nach Ablauf des Leasingvertrags stattfindet.

Sie können ein PostureExpiry-Ereignis in Context Visibility > Endpoints (Kontextsichtbarkeit > Endpunkte) sehen, während einer der angezeigten Endpunkte geöffnet wird:

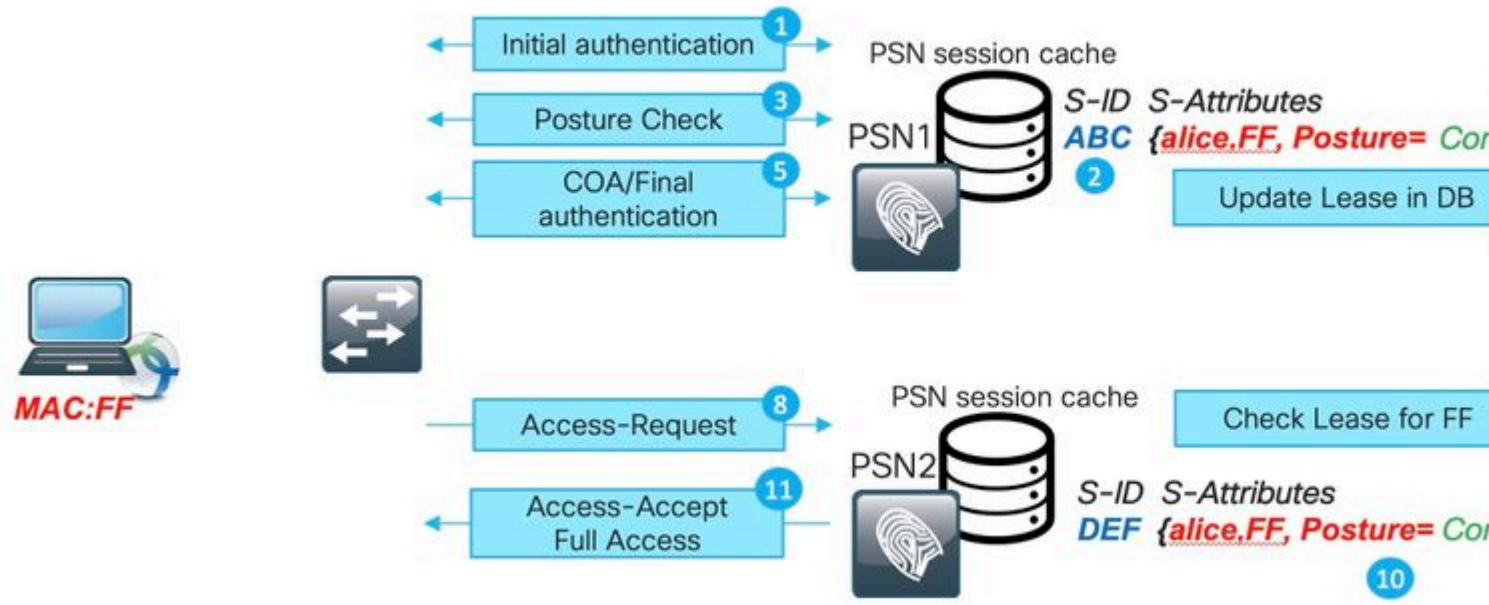
PostureExpiry	1586332942236
PostureOS	Windows 10 Professional 64-bit

Dieser Wert kann z.B. hier in den menschenlesbaren Zeitstempel konvertiert werden - https://www.epochconverter.com/

- PSN-Systemzeit zum Zeitpunkt der neuen Authentifizierung

Wenn die Authentifizierung für einen Endpunkt mit Statusleasing auf PSN trifft, werden mithilfe von PostureExpiry und dem Systemdatum eine Anzahl von Tagen abgerufen, die seit der letzten erfolgreichen Statusüberprüfung vergangen sind. Wenn der Ergebniswert innerhalb eines Leaseintervalls liegt, das in den Einstellungen definiert wurde, erhält die Sitzung den Status **Konformität**. Wenn der Ergebniswert höher ist als der Lease-Wert, erhält die Sitzung den Status **Unbekannt**. Dadurch wird der Status erneut ausgeführt, und es kann ein neuer PostureExpiry-Wert gespeichert werden.

In der Abbildung wird der Prozess bei einem Failover erläutert:



1. Die Erstauthentifizierung erfolgt mit PSN1.

2. Session-ABC wurde im Session-Cache erstellt.

3. Statusüberprüfung wird durchgeführt.

4. Änderung des Sitzungsstatus in "**Compliant**"

5. Ein durch Statusänderungen ausgelöster COA führt zur erneuten Authentifizierung des Endpunkts, sodass die nächste Zugriffsebene übernommen wird.

6. PostureExpiry-Wert im Endpunkt gespeichert.

7. Endpunktdaten werden in der gesamten Bereitstellung repliziert.

8. Nächste Authentifizierung trifft auf PSN2 zu.

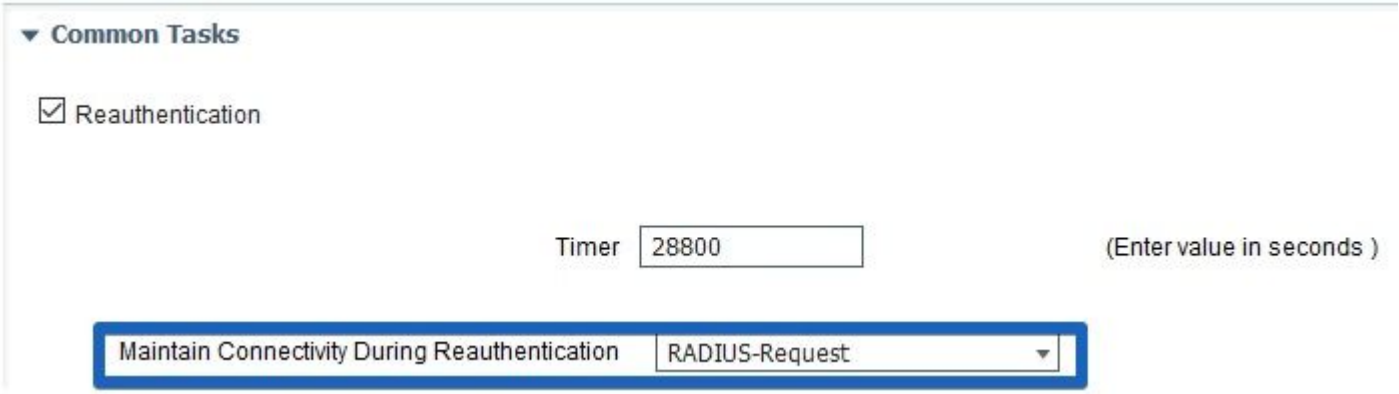
9. PSN2 überprüft, ob sich der Endpunkt innerhalb eines gültigen Leasing-Zeitraums befindet.

11. Sitzung wurde dem Sitzungscache als **konform** hinzugefügt.

12. Aufgrund des gültigen Leasingvertrags wurde die Sitzung mit dem Status "**Konformität"** erstellt.

Implementierung der erneuten Authentifizierung

Push-Timer für die Neuauthentifizierung von ISE immer mit ausgewählter **RADIUS-Anforderung** unter **Verbindung aufrechterhalten während der Neuauthentifizierung** Mit dieser Einstellung wird sichergestellt, dass NAD bei der erneuten Authentifizierung dieselbe Sitzungs-ID beibehält.



.

Umgebungen mit Load Balancern

Es können dieselben Best Practices implementiert werden, die im Abschnitt über veraltete/Phantom-Sitzungen erläutert wurden.

Verschiedene Subnetze können für ausstehende und konforme Zustände verwendet werden

Wenn das Netzwerkdesign die Möglichkeit bietet, verschiedene Subnetze mit dem Status **Ausstehend** und **Konformität** zu verwenden, ist durch diesen Ansatz gewährleistet, dass jede Statusänderung zu einer Änderung des Standard-Gateways führt.

Statusüberprüfung Im gleichen Intervall wie bei einem Timer zur erneuten Authentifizierung verwendet

Die Statusüberprüfung kann aktiviert werden, wobei das Intervall dem Neuauthentifizierungs-Timer entspricht. In einem solchen Fall, wenn das ursprüngliche PSN nicht mehr verfügbar ist, startet der PRA-Fehler den Erkennungsprozess neu.

Moderner Ansatz - Statusfreigabe

Als Teil einer implementierten Verbesserung, die in Cisco Bug-ID CSCvi35647 Patch 6 für ISE 2.6 beschrieben wurde, erhielt eine neue Funktion, die die Freigabe des Sitzungsstatus für alle Knoten in der ISE-Bereitstellung implementiert. Diese Erweiterung ist Bestandteil zukünftiger Versionen: ISE 2.7 Patches 2 und ISE 3.0.

Diese neue Funktion basiert auf dem LSD-Mechanismus (Light Session Directory), der in ISE 2.6 eingeführt wurde. In den neueren Versionen wurde diese Funktion in LDD (Light Data Distribution) Radius Session Directory umbenannt. Light Data Distribution ist standardmäßig aktiviert und ermöglicht die gemeinsame Nutzung eines begrenzten Sitzungskontexts zwischen ISE-Knoten. Es gibt keine vollständige

Replikation des Sitzungskontexts zwischen PSNs, sondern nur eine begrenzte Anzahl von für jede Sitzung freigegebenen Attributen.

Die Grundidee hinter Light Session Directory besteht darin, die Notwendigkeit zu beseitigen, Ressourcen teure API-Aufrufe an MNT auszuführen, wenn einer der Knoten in der Bereitstellung herausfinden muss, wer der aktuelle Sitzungsbesitzer ist. Meist ist eine Owner-Suche erforderlich, wenn der COA-Fluss beginnt. Mit LDD kann jeder PSN einen tatsächlichen Besitzer der Sitzung aus dem lokalen Radius Session Directory-Cache finden.

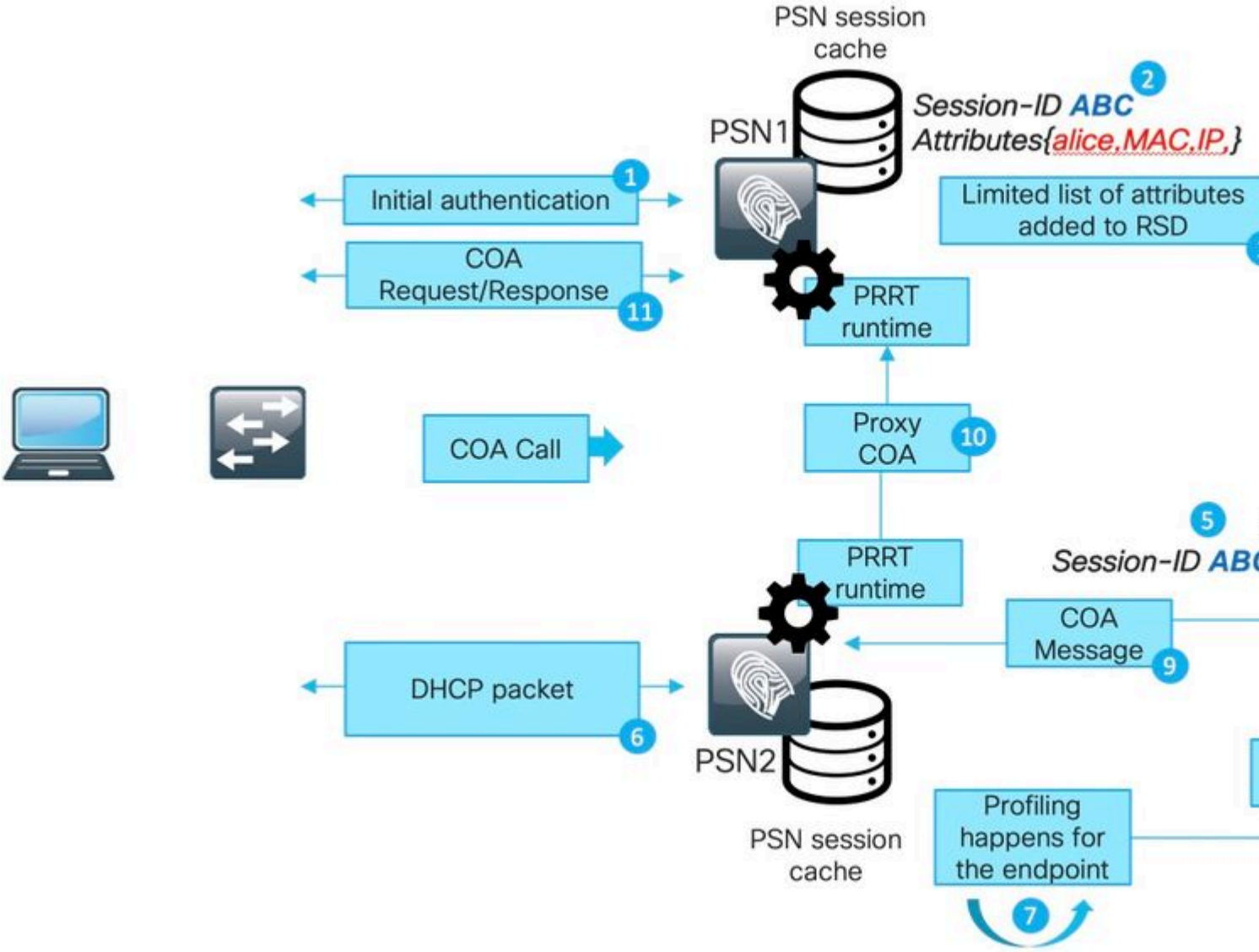
Architektur für die leichte Datenverteilung

Diese Funktion umfasst folgende Elemente:

- Radius Session Directory (RSD)-Cache: Dieser Cache befindet sich auf jedem ISE-Knoten und speichert alle aktiven Sitzungen in der ISE-Bereitstellung. Jede Sitzung hat eine begrenzte Anzahl von Attributen im Cache. Beispiele für die im Radius-Sitzungsverzeichnis gespeicherten Attribute für jede Sitzung:
    - Sitzungs-ID.
    - Endpunkt-MAC
    - CallingStationID
    - Endpunkt-IP.
    - PSN-IP - PSN, bei dem die Authentifizierung erfolgt ist.
    - PSN-FQDN - identisch mit oben.
    - NAS-IP-Adresse.
    - NAS-IPv6-Adresse
    - Status - Authentifiziert, gestartet, gestoppt.
- RabbitMQ exchange - Es wird ein Exchange gebildet, in dem Publisher, zugehörige Queue und Consumer auf jedem Knoten in der ISE-Bereitstellung dargestellt werden. Dadurch wird sichergestellt, dass sich die vollständig vermaschte Topologie zwischen allen ISE-Knoten bildet.
- Publisher - Das Radius-Sitzungsverzeichnis stellt hier einen Publisher dar. Wenn eine neue erfolgreiche Authentifizierung, die von PSN verarbeitet wird, im PSN-Sitzungscache erstellt wird, wird eine neue Sitzung erstellt. Für diese Sitzung wird ein begrenzter Satz von Attributen in das Radius-Sitzungsverzeichnis eingefügt.
- Consumer - auf allen anderen Knoten stellt Radius Session Directory einen Consumer dar.

Hinweis: Die allgemeine Terminologie und Architektur von RabbitMQ ist nicht Bestandteil dieses Dokuments.

Die Abbildung erklärt, wie der COA-Fluss mit dem RSD-Cache funktioniert:



1. Die Erstauthentifizierung erfolgt mit PSN1.

2. Session-ABC wurde im Session-Cache erstellt.

3. Erforderliche Attribute werden in RSD gespeichert.

4. Über RabbitMQ gemeinsam genutzte Sitzung mit allen anderen ISE-Knoten.

5. Sitzung wird im RSD-Cache auf allen ISE-Knoten erstellt.

6. Neue Profildaten werden auf PSN2 empfangen.

7. Endpunkt wird neu profiliert und im Fall der Änderung, die COA-Ausführung erfordert PSN2 fährt mit dem nächsten Schritt fort.

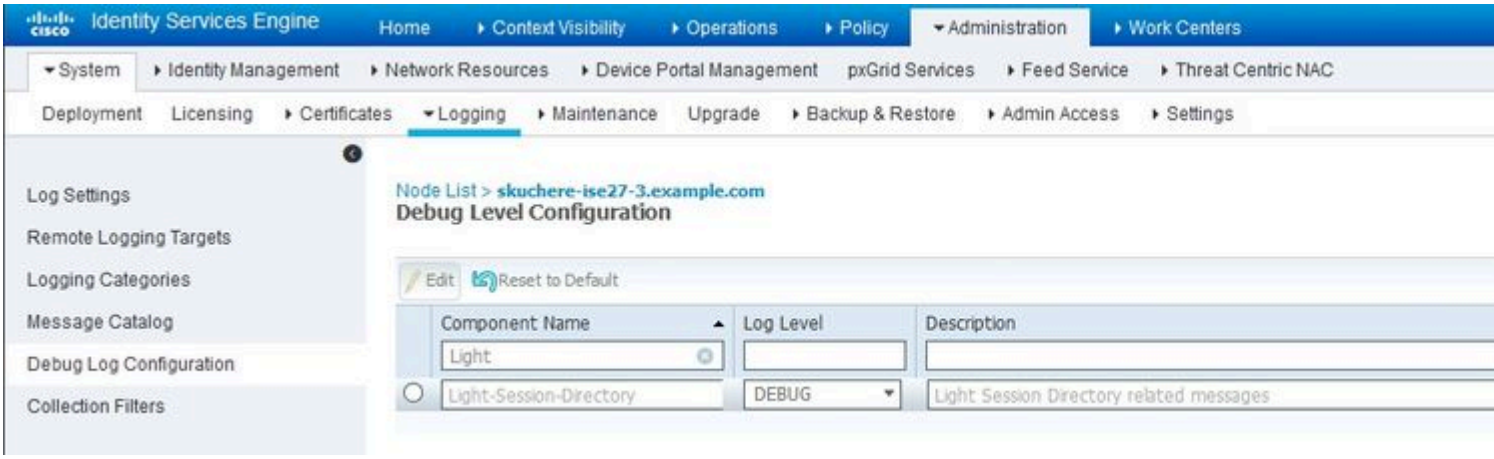
8. Ein interner API-Aufruf, der an den RSD-Cache übermittelt wurde, um COA auszuführen.

9. Daten aus dem RSD-Cache, die zur Vorbereitung einer Proxy-COA-Nachricht verwendet werden (ein COA, der von einem ISE-Knoten zu einem anderen wechselt, enthält alle Details, die der Zielknoten zur Ausgabe einer CAO-Anforderung an NAD verwenden kann). COA-Nachricht zuerst intern an PRRT Runtime (tatsächlicher AAA-Server innerhalb der ISE) übertragen.

10. PSN2 sendet eine COA-Nachricht an PSN1.

11. PSN1 sendet eine COA-Nachricht an NAD.

Um eine Fehlerbehebung für die Kommunikation über LDD auf der ISE durchzuführen, können Sie die **Light Session Director**-Komponente in DEBUG aktivieren:



Beispiel einer Debug-Meldung aus der Datei lsd.log für die Erstellung und Veröffentlichung von Sitzungen im ursprünglichen 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
```

Auf allen anderen ISE-Knoten wird angezeigt, wie eine Sitzung genutzt wurde:

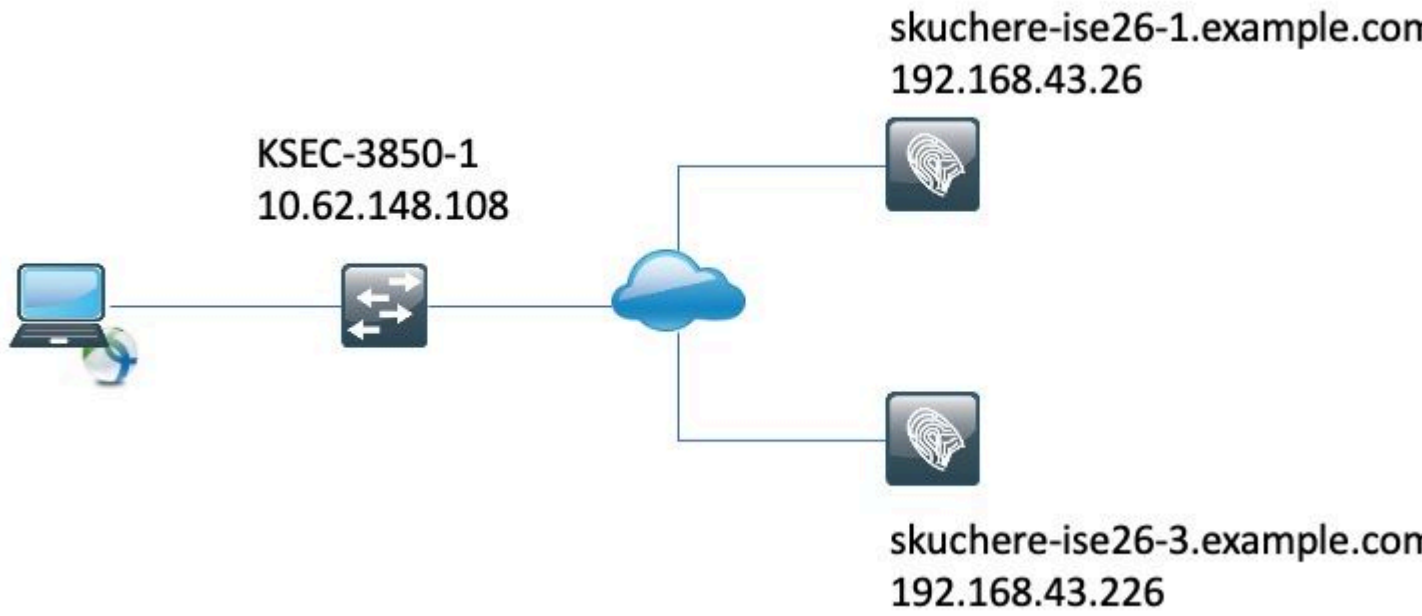
```
[pool-35-thread-38][] cisco.cpm.lsd.service.SessionConsumer -:::::- Consumer is processing : sessionID:[0
```

Statusfreigabe über RSD

Die Statusfreigabe zwischen den Knoten löst das Problem, das das Symptom "AnyConnect ISE-Statusmodul zeigt Konformität an, während der Sitzungsstatus auf ISE aussteht" aufweist, wenn die Ursache entweder "Stale/Phantom Session" oder "Re-authentication" auf verschiedenen PSN mit einer ursprünglichen Sitzungs-ID ist, die keinen Neustart der Erkennung ausgelöst hat. Sobald die Sitzung "Compliant" wird, werden diese Informationen in die RSD-Sitzung eingefügt, die später von jedem PSN in der Bereitstellung verwendet werden kann.

Es gibt noch einige andere Eckfälle, die die beschriebene Funktion nicht lösen kann. Beispiel: NAD führt eine erneute Authentifizierung auf demselben PSN mit einer anderen Sitzungs-ID durch. Solche Szenarien können mit den in diesem Dokument beschriebenen Best Practices behandelt werden.

Die Abbildung zeigt die Topologie, die für einen Test der Statusfreigabe verwendet wird:



Statusfreigabe über RSD - veraltete/Phantom-Sitzung

Um eine veraltete Sitzung zu erstellen, wurde die Authentifizierung zuerst auf dem skuchere-ise26-1 durchgeführt, und später wurde NAD neu konfiguriert, um die Abrechnung an skuchere-ise26-3 zu senden. Nachdem eine Accounting-Nachricht an das falsche PSN weitergeleitet wurde, wurde NAD erneut konfiguriert, um das Accounting zurück an skuchere-ise26-1 zu senden.

Die Abbildung zeigt einen Abrechnungsbericht, der das Vorhandensein der Phantom-Sitzung auf skuchere-ise26-3 belegt:

	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. Accounting-Start Nachrichten verarbeitet von skuchere-ise26-1.

2. Interim Accounting-Update für dieselbe Session, die von skuchere-ise26-3 verarbeitet wird.

3. Die Sitzung endet später auf skuchere-ise26-1.

Nach einiger Zeit stellt der Endpunkt wieder eine Verbindung mit dem Netzwerk her, aber die Umleitung funktioniert nicht mehr. Im guest.log von PSN - skuchere-ise26-3 können Sie diese Protokollmeldungen sehen, wenn die **Client-webapp**-Komponente in DEBUG aktiviert ist:

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

Wenn PSN feststellt, dass eine veraltete/Phantom-Sitzung für den Endpunkt vorhanden ist, antwortet es nicht auf das ISE-Statusmodul. Dies ermöglicht es uns, die richtige Antwort vom PSN zu erhalten, wenn die letzte Authentifizierung erfolgt ist.

Als Lösung für das Problem veralteter/Phantom-Sitzungen wird bei der Suche nach der Sitzung jetzt das Vorhandensein einer neuen Sitzung für den Endpunkt im RSD überprüft. Wenn RSD eine Sitzungs-ID enthält, die sich von der PSN-ID im lokalen Sitzungscache unterscheidet, wird davon ausgegangen, dass die im Sitzungscache präsentierte Sitzung veraltet ist.

Statusfreigabe über RSD - Failover zwischen PSNs

Um dieses Szenario zu reproduzieren, wurde in dem Autorisierungsprofil, das dem Endpunkt im kompatiblen Zustand zugewiesen ist, ein kurzer Neuauthentifizierungs-Timer aktiviert. Später wurde NAD neu konfiguriert, um die Authentifizierung und Abrechnung an ein anderes PSN (skuchere-ise26-3) zu senden. Nach Ablauf des Zeitgebers für die Neuauthentifizierung wurde dieselbe Sitzung auf dem anderen PSN nicht authentifiziert.

Die Abbildung zeigt einen Authentifizierungsbericht, der Failover für die normale Sitzung von skuchere-ise26-1 zu skuchere-ise26-3 anzeigt:

1. Authentifizierung erfolgt auf skuchere-ise26-1, Autorisierungsprofil mit Umleitung wird zugewiesen.

2. COA nach erfolgreicher Haltungsbeurteilung.

3. Die nächste Authentifizierung bei der Zuweisung eines Autorisierungsprofils für den kompatiblen Status.

4. Die Authentifizierung trifft auf verschiedene PSN zu, erhält aber weiterhin ein Autorisierungsprofil für den kompatiblen Zustand.

Die Sitzung erhält nach einem Failover in ise-psc.log den Compliance-Status auf dem neuen PSN, wenn **epm-pip** und **nsf-session** Komponenten in DEBUG aktiviert sind:

<#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

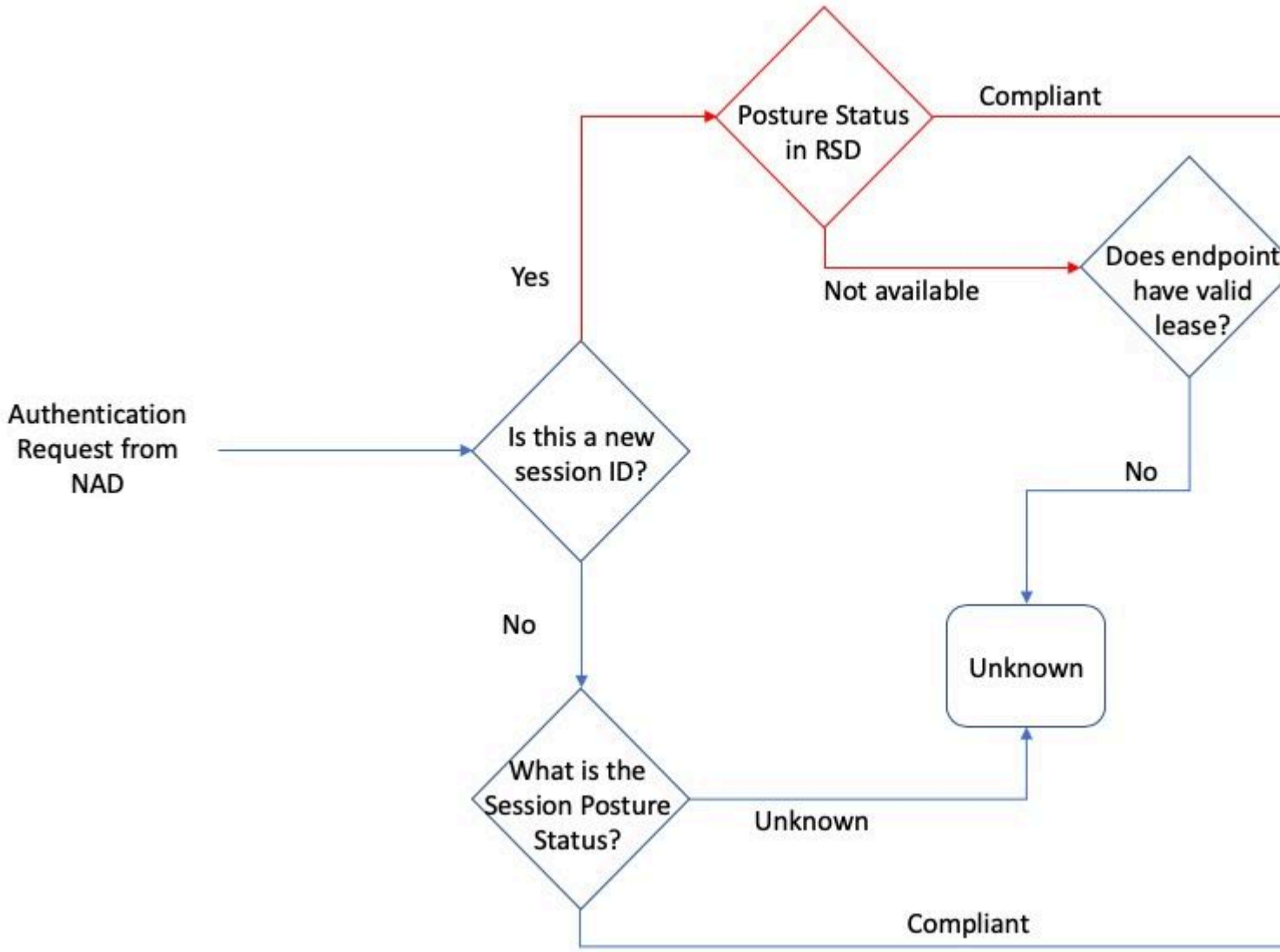
```
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution cont
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP com
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::-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

Das ursprüngliche Problem wurde durch die Hinzufügung zusätzlicher Logik in den Statusauswahlprozess gelöst. Die Abbildung zeigt, was geändert wurde (Änderungen rot hervorgehoben):



Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.