Dépannage de la gestion et de la position des sessions ISE

Table des matières

- Aperçu
- Introduction
- Informations générales
- Problème
  - Expérience utilisateur final
  - Expérience administrateur ISE
  - Scénarios problématiques courants
  - Problème de session obsolète/fantôme
    - Logique de gestion de session ISE
    - MNT et gestion de session
    - PSN et gestion de session
    - Session obsolète sur PSN
    - Session fantôme sur le PSN
    - Comment une session obsolète et une session fantôme rompent le processus de positionnement
  - Le processus de découverte ne démarre pas lors d'une nouvelle tentative d'authentification
    - Réauthentification sur un PSN différent
    - NAD génère un nouvel ID de session lors de la réauthentification
  - Méthodes rapides pour identifier le moment où un problème a été causé par une session obsolète/fantôme
  - Dépannage avancé des sessions obsolètes/fantômes
    - Collection d'offres groupées DART
    - Analyse du bundle DART
    - Enquête sur les journaux ISE
    - Enquête sur les rapports ISE
  - Comment identifier le moment où un problème a été causé par l'absence d'un redémarrage de détection
  - Dépannage avancé de l'absence de redémarrage de la détection
- Solution
  - Approche classique - Évitement des problèmes
    - Meilleures pratiques permettant de réduire le nombre de sessions obsolètes ou fantômes dans le déploiement ISE
    - Cas d'utilisation de Posture Over VPN
    - Les Méthodes Recommandées peuvent être mises en oeuvre pour minimiser l'impact de l'absence de redémarrage du module de détection de position ISE
    - Implémentation de réauthentification
    - Environnements avec équilibreurs de charge
  - Approche moderne - Partage d'état de posture
    - Architecture de distribution de données légères
    - Partage d'état de posture sur RSD
    - Partage d'état de position sur RSD - Session obsolète/fantôme
    - Partage d'état de position sur RSD - Basculement entre PSN

Introduction

Ce document décrit le problème courant des services de posture Identity Service Engine (ISE), tel que « AnyConnect ISE posture module shows compliance... »

Informations générales

Ce document décrit le problème courant des services de posture ISE (Identity Service Engine) : "Le module de posture ISE AnyConnect affiche conforme alors que l'état de session sur ISE est en attente."

Bien que les symptômes soient toujours les mêmes, il existe plusieurs causes profondes à ce problème. Souvent, le dépannage d'un problème comme celui-ci prend énormément de temps, ce qui a de graves conséquences.

Ce document explique :

- Scénarios problématiques courants.
- Algorithmes d’identification rapide des problèmes.
- Solutions classiques aux scénarios problématiques courants.
- Partage d'état de position sur le répertoire de session Radius.
- Manifestation du problème du point de vue des utilisateurs finaux et des administrateurs ISE.
- Théorie sous-jacente aux opérations ISE, AnyConnect et réseau qui déclenche le problème.

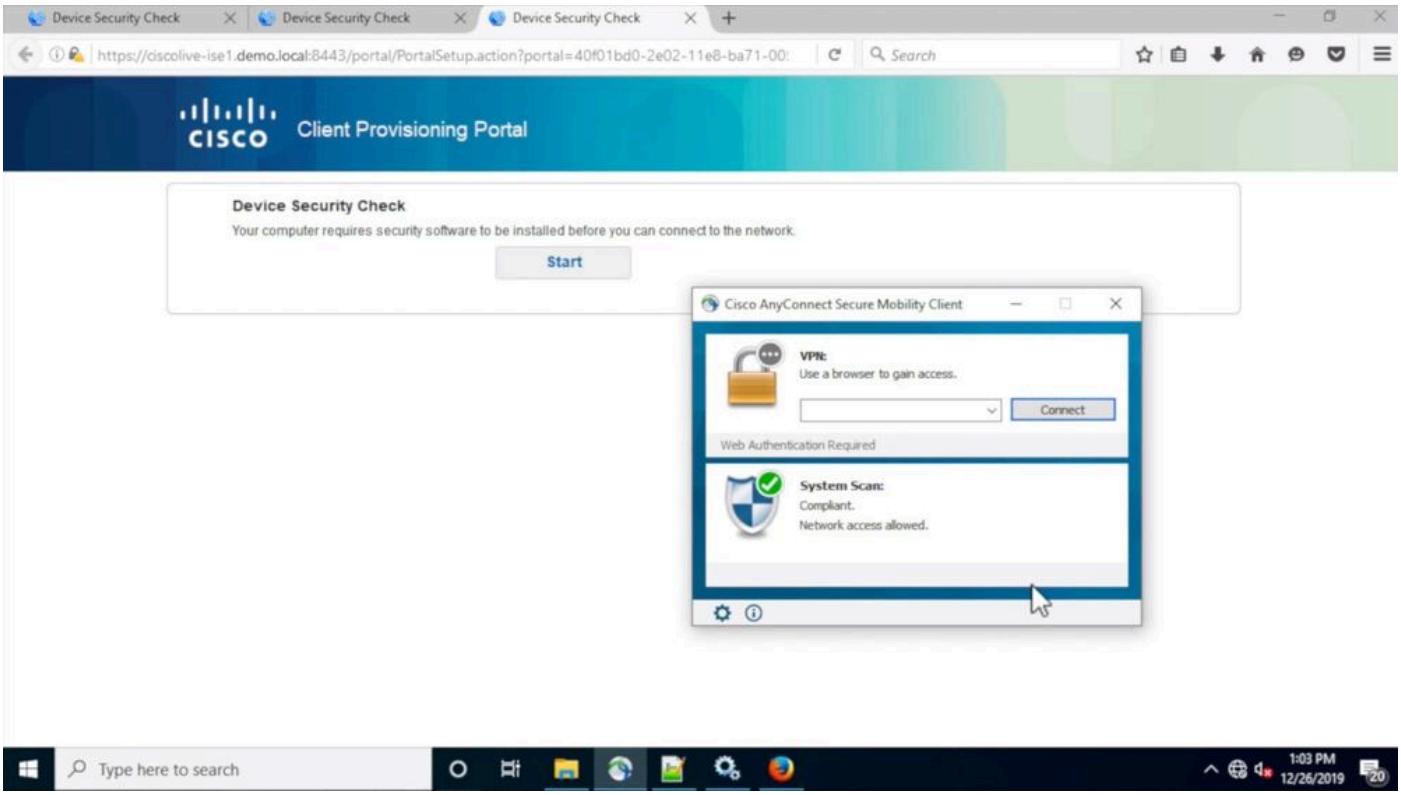
Pour une meilleure explication des concepts décrits plus loin, référez-vous à Comparaison de style de posture ISE pour Pre et Post 2.2

Problème

Expérience utilisateur final

Ce problème se manifeste normalement en l'absence d'accès réseau ou de redirection constante vers le portail de mise à disposition du client ISE dans le navigateur, tandis que, dans le même temps, le module de posture ISE AnyConnect affiche l'état de posture comme Conforme.

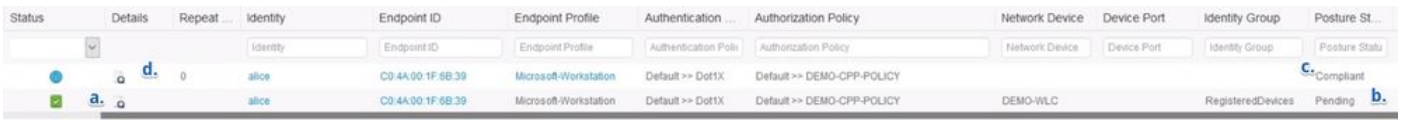
Expérience utilisateur type :



Expérience administrateur ISE

Lors du triage initial de ce problème, un administrateur ISE commence une enquête sur les journaux Radius Live pour s'assurer qu'une authentification atteint ISE. Le premier symptôme découvert à cette étape indique une non-correspondance dans un état de posture entre le point d'extrémité et ISE dans les journaux actifs. Ou, l'authentification Radius signale la dernière authentification réussie pour le point de terminaison affiche l'état de la position en attente.

Expérience d'administration ISE type :



- Dernière authentification réussie pour l'identité : Alice.
- L'état de la position de la session est En attente.
- Dernier événement de session pour l'identité : Alice.

- L'événement de session affiche l'état de posture comme Conforme.

Remarque : Dans l'exemple, C et D ne sont pas toujours présentés dans les journaux en direct lorsque le problème décrit se manifeste. Un événement de session avec l'état de position Conforme est plus courant pour les scénarios provoqués par les sessions obsolètes ou fantômes (décrites plus loin dans ce document).

Scénarios problématiques courants

Ce problème se manifeste normalement dans deux scénarios problématiques et chacun d'entre eux a plusieurs causes profondes. Les scénarios :

- Le module de posture ISE AnyConnect a été mal informé par le noeud de service de stratégie (PSN) pendant le processus de posture, ce qui a entraîné l'affichage du mauvais état de posture. Dans ce cas, le TAC fonctionne normalement avec une session obsolète ou fantôme dans le cache de session PSN.

- AnyConnect ISE affiche l'état de posture du cycle de détection précédent, car l'authentification actuelle n'a pas déclenché de processus de détection.

Le module de posture ISE d'AnyConnect comporte un nombre limité d'événements qui déclenchent le processus de détection. Il est possible qu'aucun de ces événements n'ait été détecté lors de l'authentification ou de la nouvelle authentification.

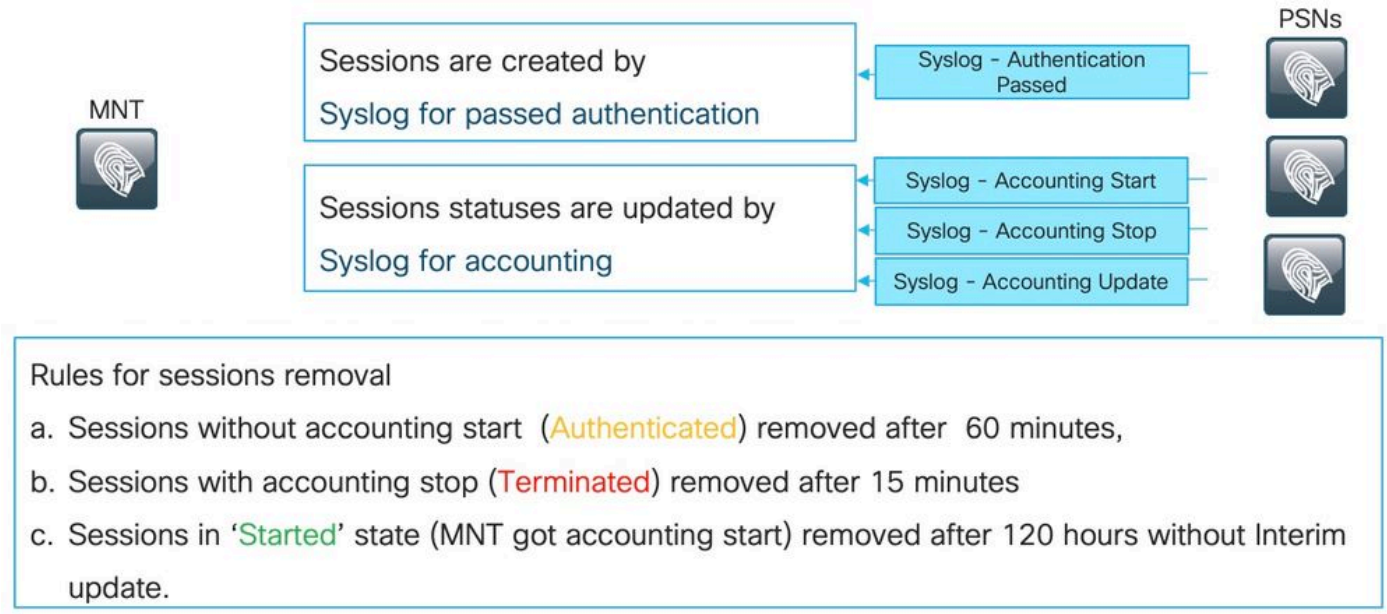
Problème de session obsolète/fantôme

Pour mieux comprendre le problème, étudiez la logique de gestion des sessions ISE et le processus de détection AnyConnect requis.

Logique de gestion de session ISE

Dans le déploiement ISE, deux personnes sont responsables du processus de gestion des sessions : PSN et noeud de surveillance (MNT). Pour dépanner et identifier correctement le problème, il est essentiel de comprendre la théorie de la gestion des sessions sur les deux personnes.

MNT et gestion de session



Comme expliqué dans cette image, le noeud MNT crée des saisons en fonction des messages Syslog d'authentification passés qui proviennent des PSN. L'état de la session peut être mis à jour ultérieurement par le Syslog pour la comptabilisation.

La suppression de session sur MNT se produit dans trois scénarios :

1. Les sessions sans comptabilité commencent à être supprimées environ 60 minutes après leur création. Une tâche cron est exécutée toutes les 5 minutes pour vérifier l'état de la session et la nettoyer.

2. La session terminée a été supprimée environ 15 minutes après que l'arrêt de la comptabilité a été traité par la même tâche cron.

3. Le même cron à chaque exécution supprime les sessions à l'état « Démarré » pendant plus de 5 jours (120 heures). Un état démarré signifie que le noeud MNT a traité l'authentification et la comptabilité pour démarrer la session Syslog.

Remarque : Il s'agit des minuteurs de nettoyage MnT normaux, et non des délais de suppression d'horloge murale garantis. La suppression peut être retardée si :

- SessionPurgeJob ne s'exécute pas correctement.
- MnT est sous pression de ressources ou de bases de données.
- Le paramètre Accounting-Stop ne peut pas être mis en corrélation avec la session existante.

Exemples de messages Syslog de PSN :

Les messages sont consignés dans le fichier prt-server.log lorsque le composant runtime-aaa est activé dans DEBUG. Les parties en gras peuvent être utilisées pour construire des expressions régulières de recherche.

Authentification réussie :

<#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

Début de la comptabilisation :

<#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-Tim

---

Mise à jour comptable provisoire :

<#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=Defa

---

Arrêt de la comptabilisation :

<#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=10.62.148.1

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

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

0A3E946C00000073559C0123

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

---

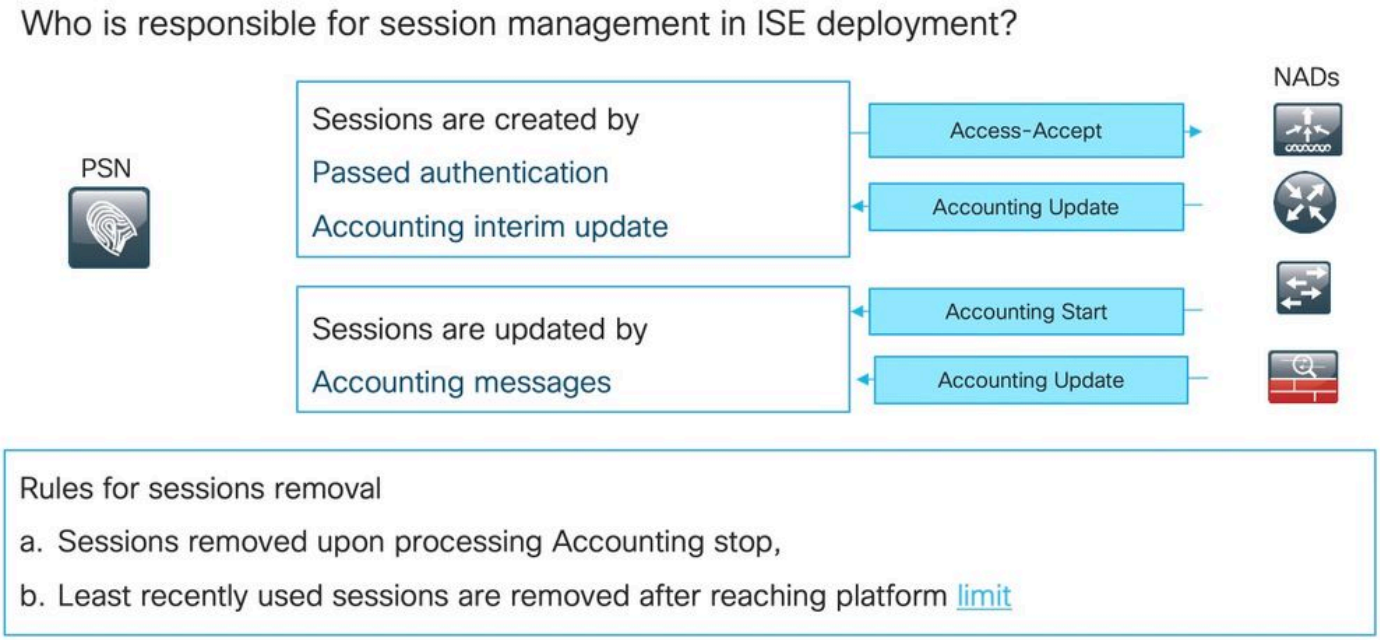
PSN et gestion de session

Le cache de session PSN est une base de données en mémoire qui stocke toutes les sessions actives d'un PSN spécifique. Le cache de session est toujours local au noeud. ISE ne dispose d'aucun mécanisme permettant d'effectuer la réplication des états de session FULL d'un noeud à un autre.

Pour chaque ID de session active, PSN stocke tous les attributs collectés pendant la phase d'authentification/autorisation (par exemple, les groupes d'utilisateurs internes/externes, les attributs NAD (Network Access Device), les attributs de certificat, etc.). Ces attributs sont utilisés par PSN pour sélectionner différents types de stratégie tels que l'authentification, l'autorisation,

l'approvisionnement client et la position.

Le cache de session est complètement supprimé lorsque le noeud (ou les services sur le noeud) sont redémarrés.



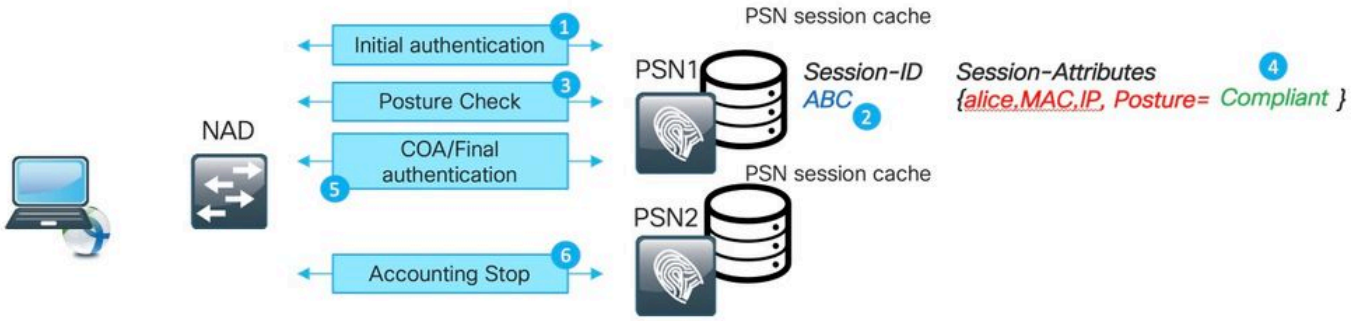
La logique de traitement de session actuelle crée une nouvelle entrée dans le cache de session dans deux scénarios. Les détails ultérieurs des sessions existantes peuvent être mis à jour à partir des messages de comptabilité, qui proviennent des NAD.

- La session a été authentifiée sur le PSN.
- PSN a une mise à jour intermédiaire de comptabilité pour la session qui n'existe pas dans le cache de session. Avec la suppression de session, PSN implémente cette logique :
  - L'entrée du cache de session est supprimée immédiatement après le traitement du message d'arrêt de la gestion.
  - PSN commence à supprimer les dernières sessions utilisées lorsqu'un noeud atteint la limite des sessions actives.

Session obsolète sur PSN

Dans le déploiement ISE, l'arrêt de la gestion des comptes pour une session existante a été traité par le PSN qui n'a pas effectué l'authentification réelle :

Exemple de session obsolète :



---

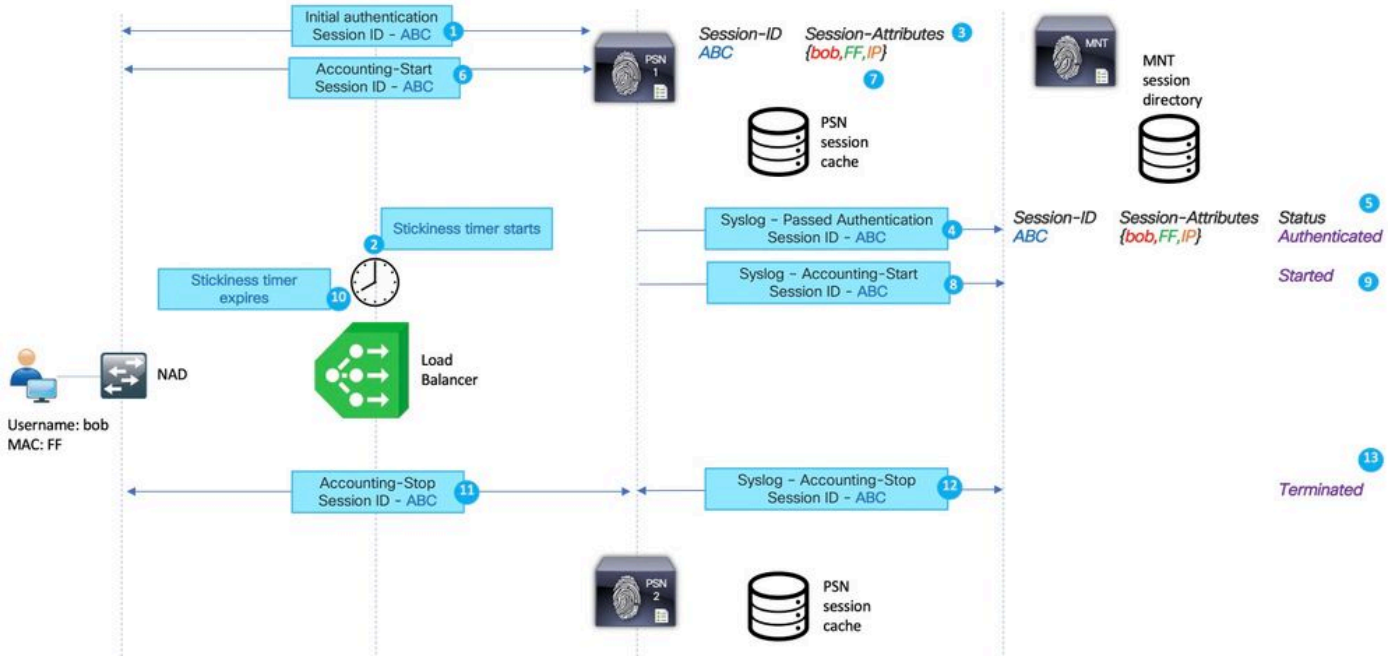
1. L'authentification a réussi sur PSN pour la session ABC.
2. PSN crée une entrée dans le cache de session.
3. Évaluation de la posture.
4. La session est marquée comme conforme.
5. Le changement d'autorisation (COA) est déclenché par le changement d'état de la position, ce qui entraîne une nouvelle authentification du terminal pour appliquer le niveau d'accès suivant.
6. La comptabilisation s'arrête pour la session ABC vers PSN2.

Par la suite, ABC est bloqué dans un état d'obsolescence sur PSN1, car aucun message d'arrêt de comptabilité n'est traité sur ce PSN pour le supprimer. La session est supprimée si le déploiement ne fait pas l'objet d'un nombre élevé de tentatives d'authentification.

La session obsolète apparaît dans le cache de session PSN dans les scénarios suivants :

- L'arrêt de la gestion des comptes a été envoyé au mauvais PSN en raison de l'expiration du minuteur de rémanence sur l'équilibreur de charge.
- La configuration incorrecte sur le NAD n'est pas le même PSN configuré pour l'authentification et la gestion des comptes.
- Des problèmes de connectivité temporaires sur le chemin réseau ont provoqué le basculement NAD vers le PSN suivant.

Exemple de session obsolète dans l'environnement d'équilibrage de charge :



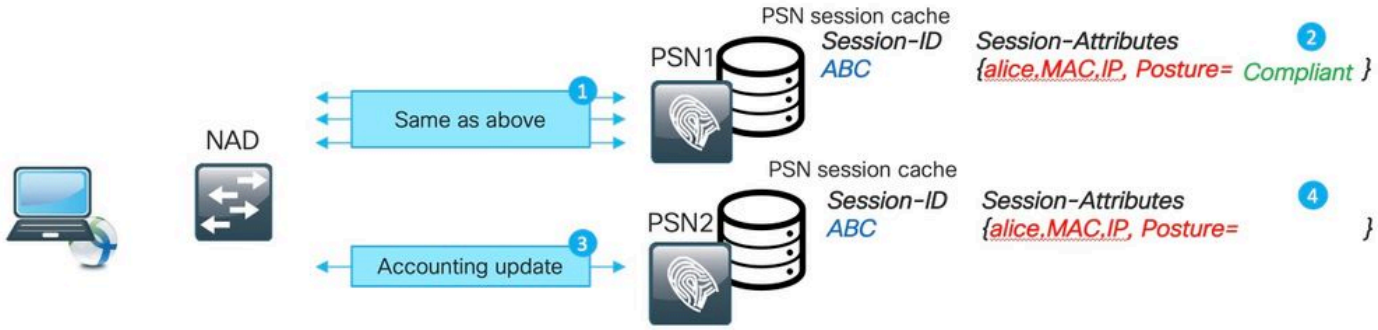
---

1. L'authentification initiale pour la session ABC est effectuée par PSN1. Cette authentification initie un compteur d'adhésion sur l'équilibreur de charge.
2. PSN1 crée une entrée pour la session ABC dans le cache local.
3. Le message Syslog pour l'authentification passée est transféré au noeud MNT.
4. L'entrée pour la session ABC est créée dans le répertoire de session MNT avec l'état Authenticated.
5. Le message de début de comptabilisation pour la session ABC se pose sur PSN1.
6. L'entrée du cache de session pour la session ABC est mise à jour avec les informations de Accounting-Start.
7. Le message Syslog pour Accounting-Start est transféré au noeud MNT.
8. L'état de la session est mis à jour à Démarré.
9. Expiration du minuteur de rémanence sur l'équilibreur de charge.
10. Accounting-Stop pour la session ABC est transféré par l'équilibreur de charge vers PSN2.
11. Le message Syslog pour Accounting-Stop est transmis par PSN2 à MNT.
12. La session ABC est marquée comme terminée sur MNT.

Session fantôme sur le PSN

La session fantôme est un scénario dans lequel la mise à jour provisoire de comptabilité arrive sur le PSN et n'a pas effectué d'authentification pour cette session. Dans ce scénario, une nouvelle entrée est créée dans le cache de session PSN. Si PSN ne reçoit pas de message d'arrêt de comptabilisation pour cette session, l'entrée n'est pas supprimée sauf si PSN atteint la limite des sessions actives.

Exemple de session fantôme :



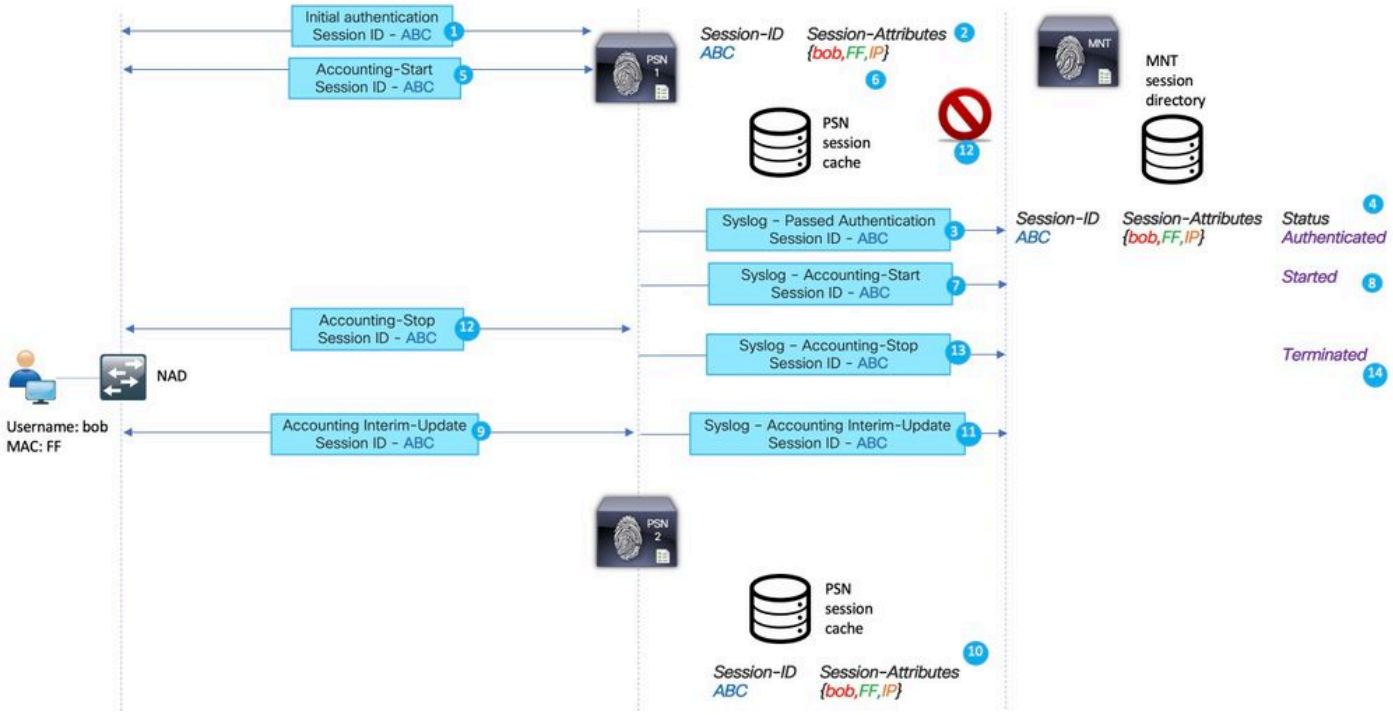
---

1. Les mêmes étapes décrites dans l'exemple de session obsolète se produisent sur PSN1 pour la session ABC.
2. L'état de la session ABC est Conforme dans le cache de session PSN1.
3. Une mise à jour intermédiaire comptable pour la session ABC frappe PSN2.
4. Une entrée de session pour ABC est créée sur PSN2. Comme l'entrée de session est créée à partir du message de comptabilité, elle possède un nombre limité d'attributs. Par exemple, l'état de la position n'est pas disponible pour la session ABC, et les groupes d'utilisateurs ou d'autres attributs spécifiques à l'autorisation sont également absents.

La session fantôme apparaît dans le cache de session PSN dans les scénarios suivants :

- Interruption à court terme du transit réseau.
- Défaut de fonctionnement du périphérique d'accès réseau.
- Mauvais comportement ou configuration incorrecte sur l'équilibreur de charge.

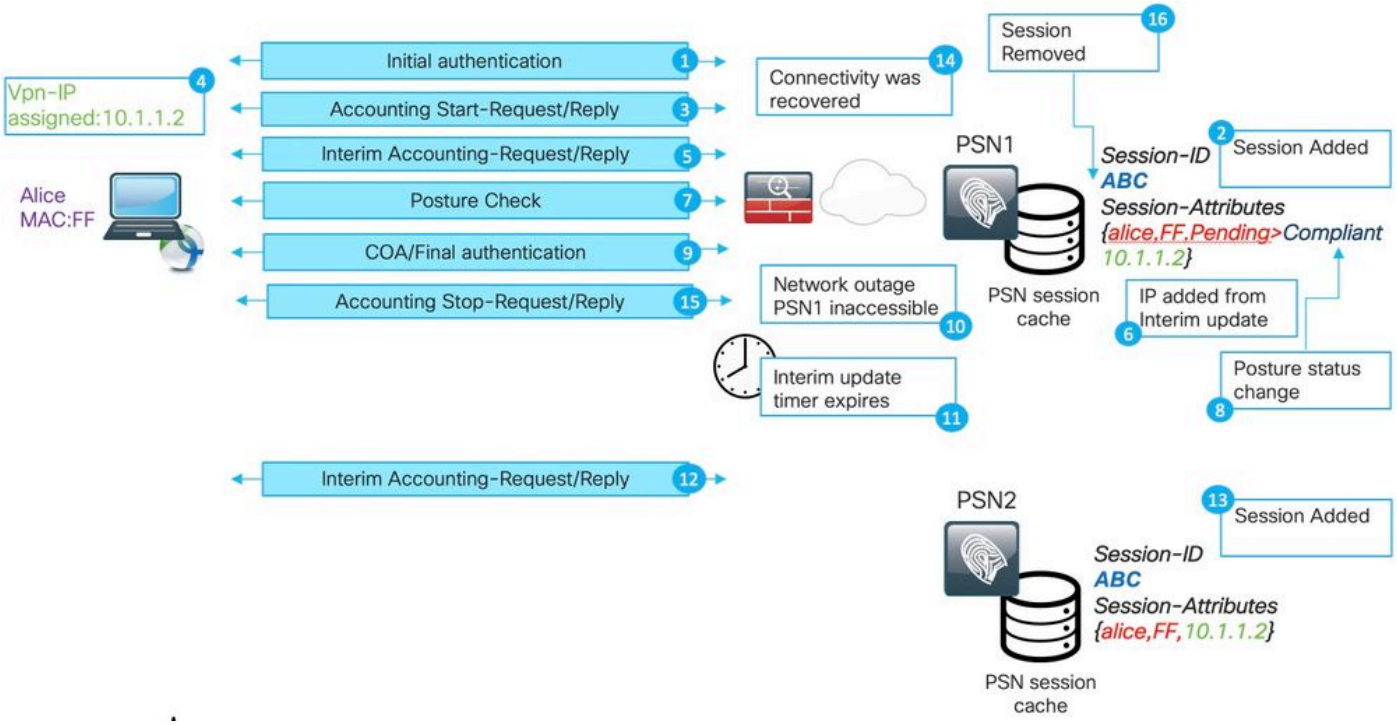
La capture d'écran suivante est un exemple de session fantôme où des problèmes temporaires sur le chemin du réseau vers PSN1 :



---

1. L'authentification initiale de la session ABC est effectuée par PSN.
2. PSN1 crée une entrée pour la session ABC dans le cache local.
3. Le message syslog pour l'authentification réussie est transféré au noeud MNT.
4. Une entrée pour la session ABC est créée dans la base de données TimesTen avec l'état Authenticated.
5. Le message de début de comptabilisation pour la session ABC atterrit sur PSN 1.
6. Une entrée de cache de session pour la session ABC est mise à jour avec les informations de Accounting-Start.
7. Le message Syslog pour Accounting-Start est transféré au noeud MNT.
8. L'état de la session est mis à jour à Démarré.
9. La mise à jour de la comptabilité intermédiaire pour la session ABC est transmise à PSN2.
10. PSN2 crée une entrée pour la session ABC dans le cache local.
11. Le compte-arrêt de la session ABC est transféré à PSN1.
12. L'entrée de la session ABC est supprimée du cache de session sur PSN1.
13. Un message Syslog pour Accounting-Stop est transmis par PSN1 à MNT.
14. La session ABC est marquée comme terminée sur MNT.

Ceci décrit un scénario de la session fantôme telle que créée pour la connexion VPN à vie longue :



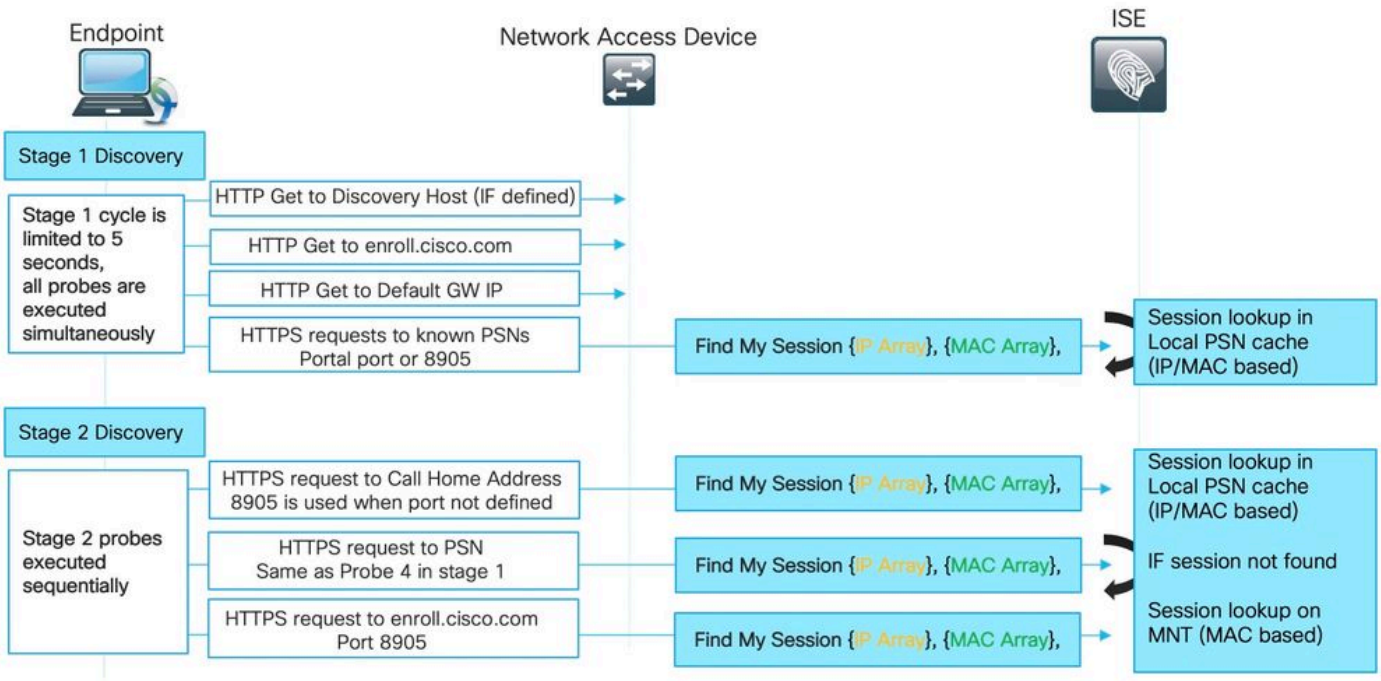
---

1. Authentification initiale sur PSN1.
2. La session ABC est créée dans le cache de session.
3. La gestion des comptes lance le message traité par le PSN.
4. La nouvelle adresse IP est attribuée à l'adaptateur de réseau privé virtuel (VPN).
5. Une mise à jour comptable intermédiaire avec les informations d'adresse IP atterrit sur le PSN.
6. Les informations d'adresse IP sont ajoutées au cache de session.
7. L'évaluation de la posture se produit avec PSN1.
8. L'état de la position est mis à jour dans la session.
9. Une poussée de certificat d'authenticité est exécutée par ISE ; cela déclenche l'attribution d'un nouveau niveau d'accès.
10. Il y a une panne sur le chemin réseau, ce qui rend PSN1 inaccessible.
11. Après l'expiration d'un intervalle de mise à jour intermédiaire, ASA/FTD détecte que PSN1 est inaccessible.
12. La mise à jour comptable intermédiaire arrive sur PSN2.
13. La session fantôme est créée dans le cache de session PSN2.

Si PSN1 devient accessible plus tard (14), tous les messages de comptabilité suivants sont transférés (15,16), ce qui laisse la session ABC dans le cache de session PSN2 pendant une durée indéfinie.

Comment une session obsolète et une session fantôme rompent le processus de positionnement

Pour comprendre comment les sessions obsolètes et fantômes rompent la posture, vous pouvez consulter le processus de découverte du module de posture ISE AnyConnect :



Étape 1 Découverte :

Au cours de cette étape, le module de posture ISE exécute quatre sondes simultanées pour localiser le PSN qui authentifie le point d'extrémité.

Premièrement, trois sondes sur la figure sont basées sur la redirection (Default GW IP, Discovery host IP (si défini) et enroll.cisco.com IP) ; ces sondes pointent toujours l'agent vers le PSN de droite, car l'URL redirigée est extraite du NAD lui-même.

La sonde 4 est envoyée à tous les serveurs principaux présentés dans le fichier ConnectionData.xml. Ce fichier est créé après la première tentative de positionnement réussie. Le contenu du fichier peut être mis à jour ultérieurement si le client migre entre PSN.

Sur les systèmes Windows, l'emplacement du fichier est C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture\.

Puisque toutes les sondes de l'étape 1 sont exécutées simultanément, les résultats de la sonde 4 sont utilisés uniquement si les trois autres sondes échouent ou si le module de posture ISE ne peut pas établir une communication correcte avec le PSN renvoyé dans l'URL de redirection dans

les 5 secondes.

Lorsque la sonde 4 atterrit sur le PSN, elle contient une liste d'adresses IP et MAC actives découvertes sur le point d'extrémité. PSN utilise ces données pour rechercher une session pour ce point de terminaison dans le cache local. Si PSN dispose d'une session obsolète ou fantôme pour un terminal, cela peut entraîner l'affichage d'un état de position incorrect plus tard du côté client.

Lorsqu'un agent reçoit plusieurs réponses pour la quatrième sonde (ConnectionData.xml peut contenir plusieurs PSN principaux), la réponse la plus rapide est toujours utilisée.

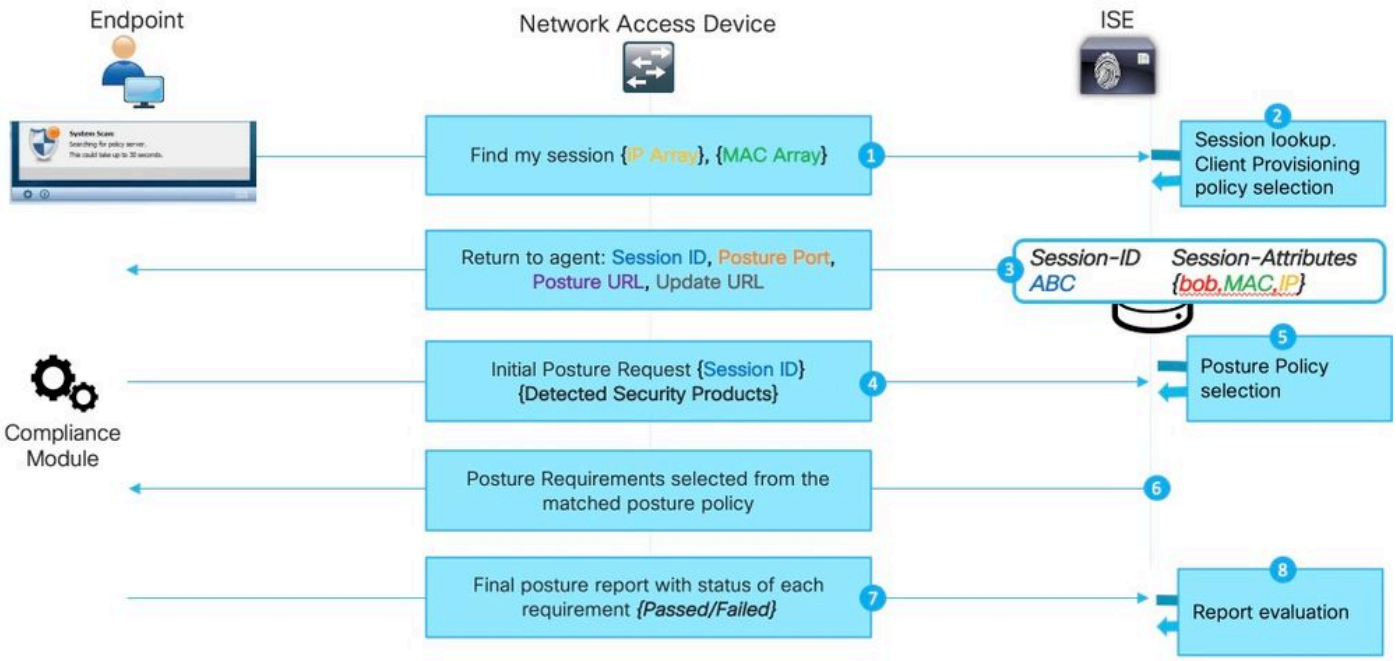
Étape 2 Découverte :

Toutes les sondes de détection de l'étape 2 sont sans redirection, ce qui signifie que chaque sonde déclenche une recherche de session sur le PSN de destination. Si le PSN ne peut pas localiser la session dans le cache de session local, il doit effectuer une recherche MNT (basée uniquement sur l'adresse MAC) pour trouver un propriétaire de session et renvoyer le nom du propriétaire à l'agent.

Comme toutes les sondes déclenchent la recherche de session, la détection de l'étape 2 peut être considérablement affectée par des problèmes résultant de sessions obsolètes ou fantômes.

Si PSN passe à l'étape 2, la sonde de détection qui existe dans le cache de session crée une entrée obsolète ou fantôme pour le même terminal. Il en résulte un état de posture incorrect renvoyé à l'utilisateur final.

Cet exemple montre comment la position apparaît lorsque PSN conserve une session obsolète ou une session fantôme :



Remarque : Ce problème ne peut se manifester que lorsque toutes les sondes de détection basées sur la redirection échouent ou lorsque la position de non-redirection est implémentée.

---

1. L'une des sondes Find my session émises par le module de posture ISE.
2. PSN effectue une recherche de session dans le cache de session. Si la session est détectée, un problème de session obsolète ou fantôme se produit.
3. PSN exécute la sélection de stratégie d'approvisionnement du client. Si une session fantôme ne dispose pas d'attributs d'authentification/autorisation et que toutes les stratégies configurées par vous sont spécifiques (par exemple, des stratégies sont créées pour des groupes Active Directory spécifiques), PSN ne peut pas attribuer une stratégie d'approvisionnement de client correcte. Cela peut se manifester dans le message d'erreur : "Ignorer l'analyse AnyConnect votre réseau n'est pas configuré pour utiliser Cisco NAC Agent".
    - Dans les cas où les stratégies d'approvisionnement du client sont génériques (les attributs disponibles dans la session fantôme sont suffisants pour faire correspondre la stratégie à une configuration AnyConnect), PSN répond en indiquant les détails nécessaires à la poursuite du processus d'évaluation.
    - À cette étape, lorsque vous travaillez avec des sessions obsolètes, PSN répond immédiatement avec un état de posture Conforme et toutes les étapes suivantes ne sont pas terminées. PSN n'envoie pas de certificat d'authenticité car il pense que la session est déjà conforme. Dans les journaux Radius Live, aucun événement de session n'est affiché avec l'état Conforme.

4. Pour le scénario de session fantôme, le module de posture ISE continue avec la demande de

posture initiale. Cette demande contient des informations sur tous les produits de sécurité et de gestion des correctifs détectés sur le terminal.

---

5. PSN utilise les informations des attributs de requête et de session pour correspondre à la stratégie de position appropriée. La session fantôme ne dispose pas d'attributs à ce stade et il n'existe aucune stratégie à mettre en correspondance. Dans ce cas, PSN répond au terminal qu'il est conforme. Il s'agit du comportement ISE par défaut si la stratégie de position ne correspond pas.

 Remarque : Lorsqu'une stratégie générique peut être sélectionnée à partir des attributs de session fantôme, vous pouvez passer à l'étape 6.

---

6. PSN renvoie les politiques de posture sélectionnées à l'agent.

 Remarque : Lorsqu'aucune stratégie ne peut être sélectionnée, PSN retourne avec un état Conforme.

---

7. L'agent renvoie les statuts « réussi » ou « échec » pour chaque règle/condition.

---

8. L'évaluation du rapport a lieu sur ISE et l'état de la session passe à Conforme.

 Remarque : Si des problèmes de posture sont causés par la session fantôme, l'administrateur ISE peut remarquer certains certificats d'authenticité de posture défaillants. Si c'est le cas, les demandes de certificat d'authenticité sont exécutées à partir des PSN incorrects et pour les ID de session incorrects.

Le processus de découverte ne démarre pas lors d'une nouvelle tentative d'authentification

Le module de posture ISE est conçu pour surveiller un nombre limité d'événements sur le terminal afin de déclencher un processus de détection.

Événements qui déclenchent la découverte :

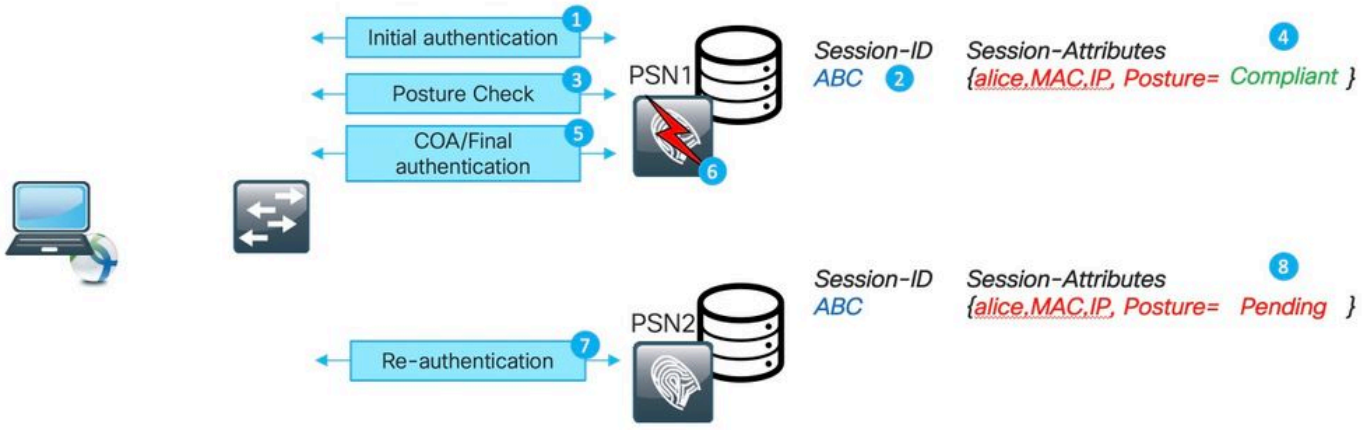
- Installation initiale du module de posture ISE.
- Connexion utilisateur.
- Événements d'alimentation.
- Changement d’état d’interface.
- Reprise du système d'exploitation après veille.
- Modification de la passerelle par défaut (DG)
- Échec de la réévaluation de position (PRA), voir l'ID de bogue Cisco CSCvo69557. La nouvelle authentification dot1x, le déverrouillage du PC et le changement d'adresse IP ne sont pas détectés par le module de position ISE.

Le module de posture ISE ne peut pas détecter une nouvelle tentative d'authentification ou de réauthentification dans les scénarios suivants :

- La réauthentification frappe un PSN différent (soit en raison de décisions LB, soit de problèmes avec le PSN d'origine).
- NAD génère un nouvel ID de session lors de la réauthentification.

Réauthentification sur un PSN différent

Ce schéma illustre un exemple de réauthentification sur un PSN différent causée par la panne du PSN d'origine. Un scénario avec un équilibreur de charge ressemble à cela. Dans le cas d'un équilibreur de charge, la réauthentification est dirigée vers le PSN différent à la suite de l'expiration d'un temporisateur de collage.

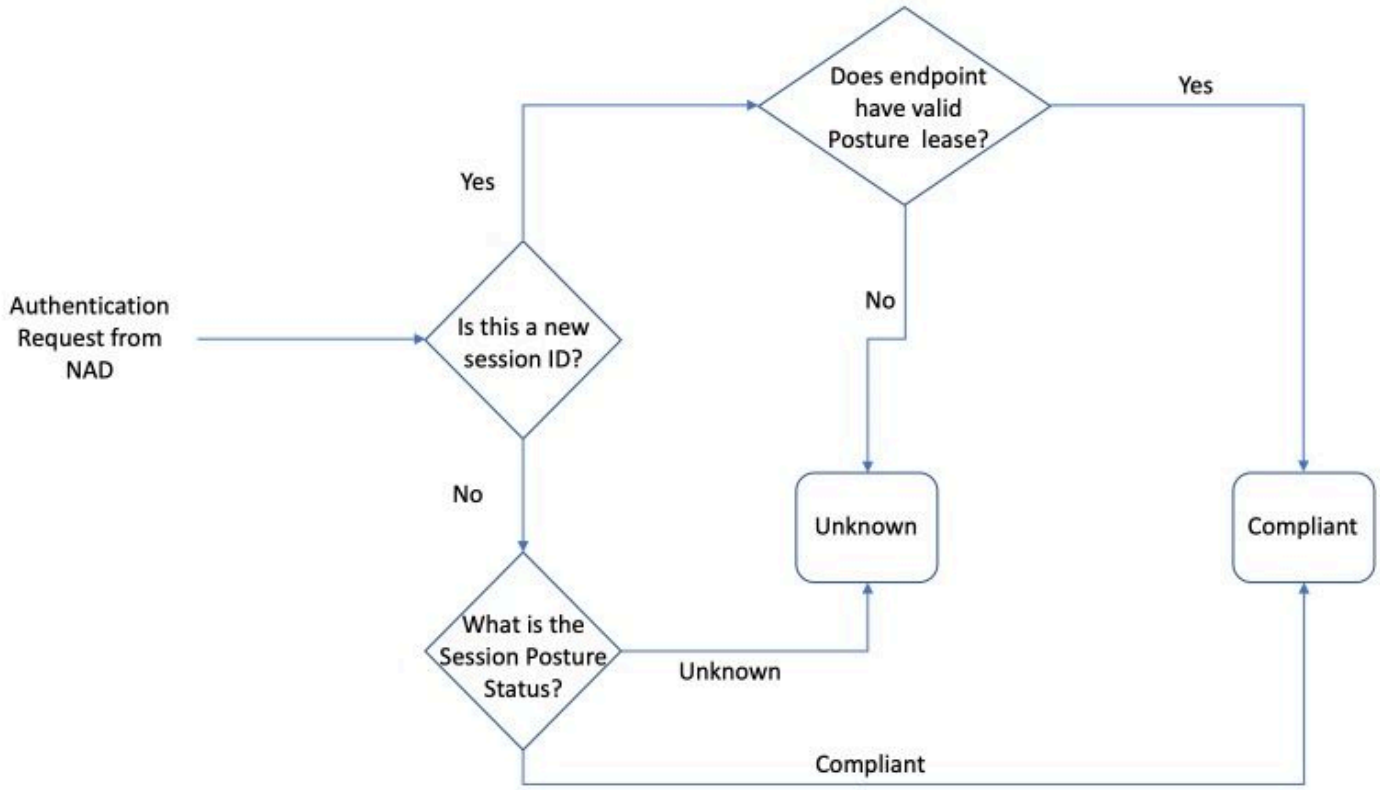


---

1. Authentification initiale sur PSN1.

2. La session ABC est créée dans le cache de session PSN1.
3. L'évaluation de la posture est effectuée avec PSN1.
4. L'état de la position ABC de la session passe à Conforme.
5. Le certificat d'authenticité est déclenché par le changement d'état de la position et entraîne une nouvelle authentification du terminal pour appliquer le niveau d'accès suivant.
6. PSN1 devient indisponible.
7. La réauthentification de la session ABC est effectuée sur PSN2.
8. Étant donné qu'il s'agit d'une nouvelle session pour PSN2, l'état de la session passe à En attente.

L'état de la position initiale est attribué par PSN à la session :



Remarque : State-machine décrit uniquement une sélection initiale de l'état de la posture. Chaque session est initialement marquée comme Inconnue et peut devenir plus tard Conforme ou Non conforme en fonction de l'évaluation du rapport reçue du module de posture ISE.

NAD génère un nouvel ID de session lors de la réauthentification

Cela peut se produire dans les deux scénarios les plus courants :

- La réauthentification n'est pas correctement configurée côté ISE (la solution à ce problème est traitée plus loin dans ce document).
- Comportement répréhensible du côté de la NAD ; Normalement, NAD conserve le même ID de session pendant la tentative de réauthentification. Il s'agit d'un comportement potentiellement bogué qui doit être étudié sur NAD.
    - Le nouvel ID de session peut être généré dans d'autres scénarios. Par exemple, dans certains cas, l'itinérance sans fil peut être une cause.
    - ISE PSN place toujours une nouvelle session à l'état Position en attente, à moins que le bail de position ne soit configuré. Le bail de posture est décrit plus loin dans ce document.

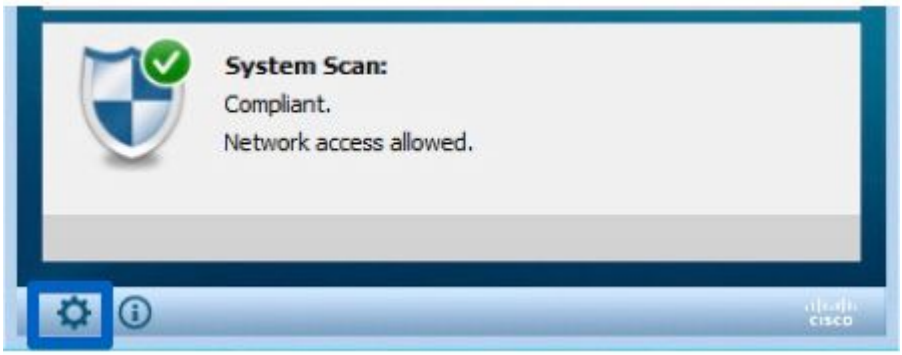
Méthodes rapides pour identifier le moment où un problème a été causé par une session obsolète/fantôme

Identifier si AnyConnect affiche la conformité lorsque l'état de redirection est causé par la session obsolète/fantôme. Vous devez obtenir l'accès au point de terminaison lorsque celui-ci est à l'état problématique.

Examiner les détails de l'analyse système

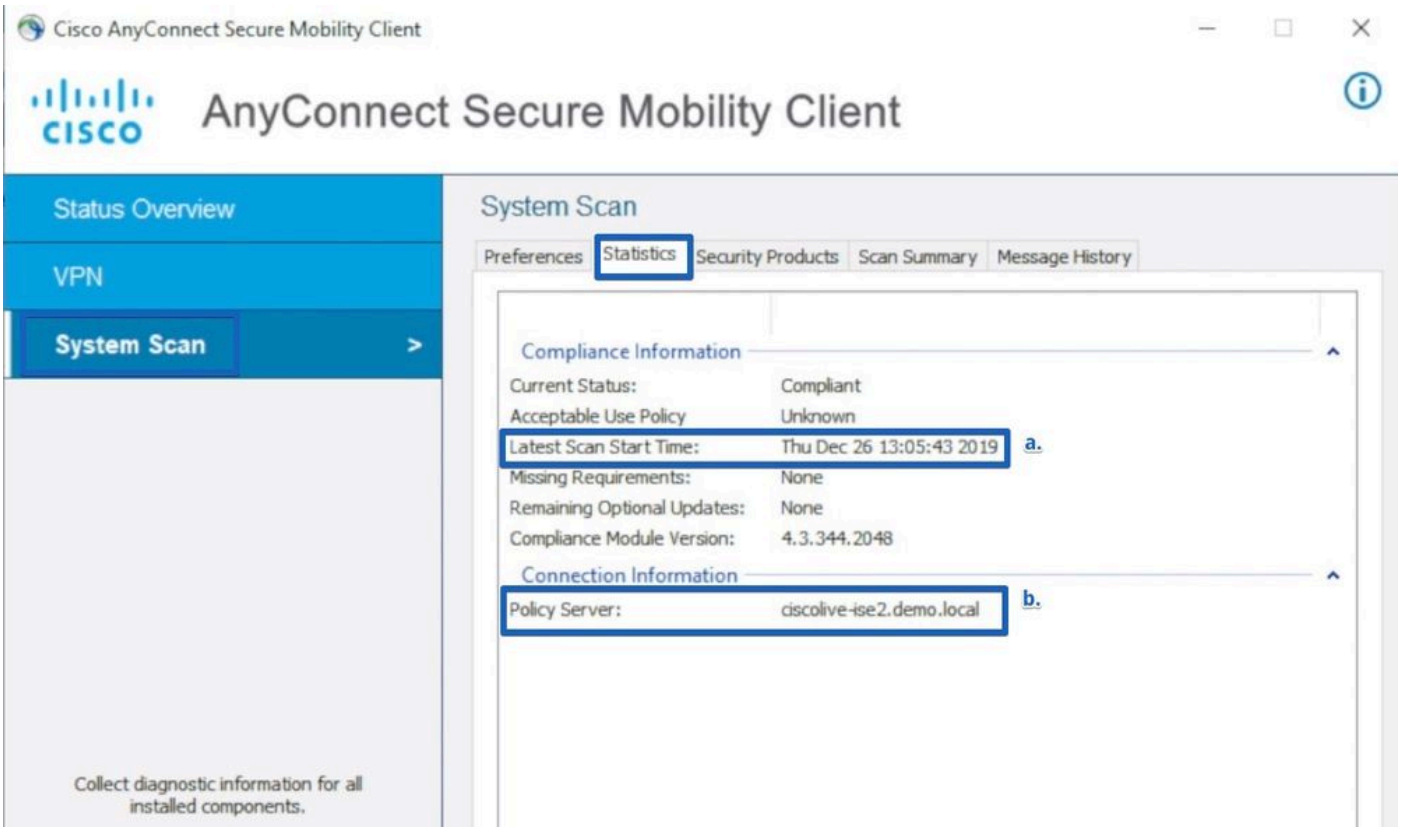
---

1. Cliquez sur l'icône d'engrenage dans l'interface utilisateur AnyConnect.



---

2. Dans la nouvelle fenêtre, accédez à Analyse système > Statistiques.

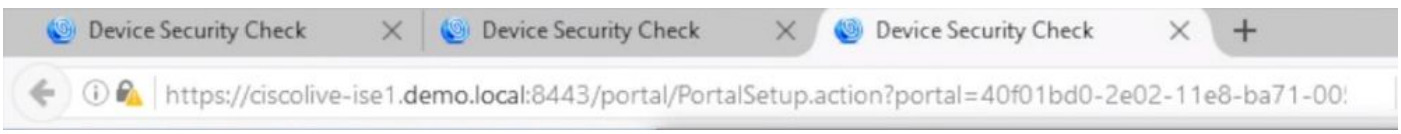


Ensuite, prêtez attention à deux éléments importants :

- Heure de début de la dernière analyse : L'horodatage ici doit être proche de l'heure à laquelle le problème a été découvert.
- Serveur de stratégie : Ce champ indique le nom du serveur de stratégies qui effectue une évaluation de la position du point de terminaison. Le nom de domaine complet doit être comparé au nom de domaine complet de l'URL de redirection (pour la position de base de redirection) ou au nom PSN tiré de la dernière tentative d'authentification (pour la position sans redirection).

---

1. Comparez le nom de domaine complet (FQDN) du serveur de stratégies des statistiques d'analyse du système avec le nom du noeud qui a authentifié le point d'extrémité :



La démonstration montre l'enregistrement des étapes requises pour l'identification du problème :

Dépannage avancé des sessions obsolètes/fantômes

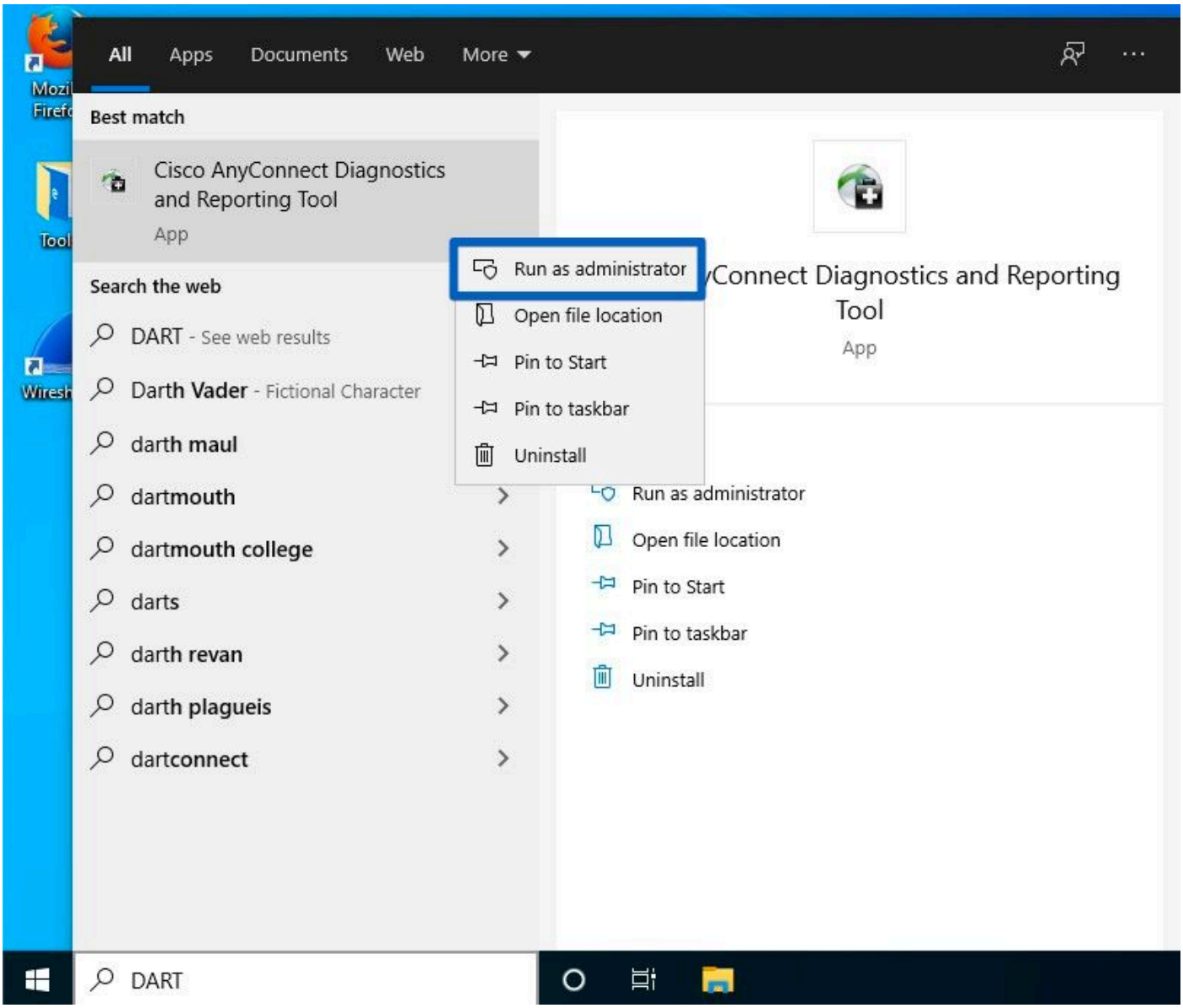
L'exemple précédent distingue le problème d'une session obsolète ou fantôme du problème du processus de détection qui n'a pas démarré. En même temps, vous devez identifier la session qui a déclenché le problème pour comprendre comment il devient un problème de session obsolète ou fantôme. Bien que dans certains scénarios, les sessions obsolètes et fantômes ne puissent pas être évitées, vous devez vous assurer que les meilleures pratiques sont mises en oeuvre, afin d'empêcher la création de sessions obsolètes/fantômes dans un environnement.

Collection d'offres groupées DART

Analysez un bundle DART pris à partir du terminal qui reproduit le problème.

---

1. Conservez uniquement les journaux importants dans DART et il est recommandé d'effacer les journaux avant que le problème ne se reproduise.
2. Pour ce faire, l'utilitaire d'ensemble DART doit démarrer en tant qu'administrateur et effectuer un nettoyage du journal.
3. Sous Windows, accédez à Démarrer et tapez DART > clic droit, puis choisissez - Exécuter en tant qu'administrateur.



---

4. Dans le premier écran de l'Assistant, cliquez sur Suivant.



---

5. Sur l'écran suivant de l'assistant, cliquez sur Effacer tous les journaux.

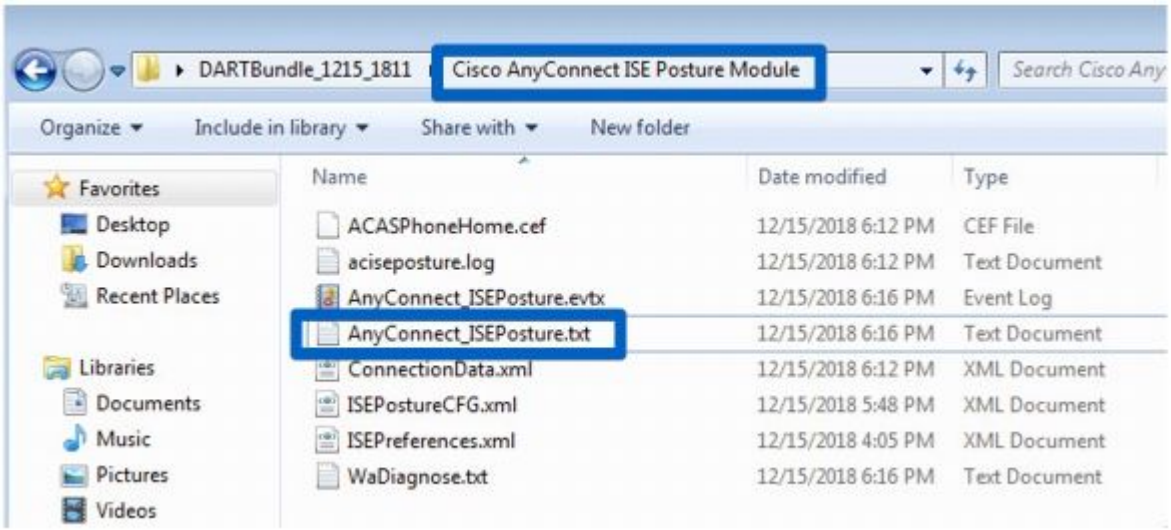


---

6. Une fois le problème reproduit, DART peut être collecté à partir d'ici ; cliquez sur Next.

Analyse du bundle DART

Une fois l'ensemble DART collecté, désarchivez-le et concentrez-vous sur le fichier AnyConnect_ISEPosture.txt situé dans le dossier Cisco AnyConnect ISE Posture Module. Ce fichier contient tous les événements liés à la détection.



---

1. Commencez le dépannage et identifiez tous les moments de redémarrage de la détection. Les mots clés à rechercher sont Redémarrage de la détection ou Détection HTTP. Accédez à la ligne avec le redémarrage de la détection qui s'est produit au moment problématique :

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

---

2. Plusieurs lignes après le redémarrage de la détection, il y a une ligne qui contient, Probing no MNT stage cibles (il s'agit d'un indicateur de début de la détection de l'étape 1) :

```
SwiftHttpRunner::collectNoMntTargets Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\Swi
ftHttpRunner.cpp Line: 1157 Level: debug  Probing no MNT stage targets (#5):
Redirection target 192.168.255.1, Redirection target enroll.cisco.com,
Auth-Status target ciscolive-ise2.demo.local with path /auth/status,
Auth-Status target ciscolive-ise1.demo.local with path /auth/status,
```

---

3. Il est recommandé de mettre en surbrillance toutes les sondes basées sur la redirection avec la même couleur et les PSN précédemment connectés provenant de ConnectionData.xml (cibles d'état d'authentification) dans une couleur différente. Normalement, les FQDN PSN sont similaires et peuvent être difficiles à détecter.

---

4. Lisez les fichiers journaux pour voir les résultats de chaque sonde (il s'agit d'un exemple de l'aspect d'une sonde défaillante) :

```
2018/12/15 18:12:01 [Information] aciseagent Function: Target::Probe Thread Id: 0x1130
File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libnaccommon\Target.
cpp Line: 200 Level: debug Status of Redirection target enroll.cisco.com is 6 <Not
Reachable.>.
```

---

5. Quelque part dans le fichier après le redémarrage de la détection pour l'étape 1 ou l'étape 2, vous voyez une réponse positive d'un ou plusieurs PSN :

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

---

5. Plusieurs lignes plus loin, il y a une ligne avec le mot clé MSG_NS_SWISS_NEW_SESSION. Cette ligne contient un ID de session réel qui a été sélectionné par PSN à la suite de la recherche de session. Utilisez cet ID de session pour approfondir les recherches sur ISE et déterminer comment la session est devenue obsolète/fantôme :

```
SwiftHttpRunner::invokePosture Thread Id: 0x1340 File:
C:\temp\build\thehoff\Logan_MR30.436724056525\Logan_MR3\posture\ise\libswift\Swi
ftHttpRunner.cpp Line: 1407 Level: debug  MSG_NS_SWISS_NEW_SESSION,
{{ise_fqdn="ciscolive-ise2.demo.local"}, {posture_port="8443"},
{posture_path="/auth/perfigo_validate.jsp"},
{posture_domain="posture_domain"}, {posture_status="Compliant"},
{session_id="0a3e949c000002585cf00588"},
{config_uri="/auth/anyconnect?uuid=f62337c2-7f2e-4b7f-a89a-3508d761173c"},
{acpack_uri="/auth/provisioning/download/066ac0d6-2df9-4a2c-a129-fabf1ace36aa"},
 {acpack_port="8443"}, {acpack_ver="4.6.3049.0"}, {pra_enabled=0}}.
```

Enquête sur les journaux ISE

1. Dans le journal guest.log avec le composant client-webapp activé dans DEBUG, le PSN répond

avec la session Stale/Phantom, qui peut être vu.

---

2. PSN reçoit une demande de l'agent de posture ISE. Il s'agit d'une demande d'AnyConnect en raison de la valeur 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
```

---

3. La requête contient des tableaux d'adresses IP et d'adresses MAC. Dans cet exemple, chaque

tableau ne contient qu'une seule valeur. Le journal indique que l'ID de session de la demande est null, ce qui indique qu'il s'agit d'une demande provenant de l'analyseur non basé sur la redirection. Vous pourrez voir plus tard comment les valeurs des tableaux sont utilisées pour localiser un ID de session :

<#root>

```
cpm.client.provisioning.utils.ProvisioningUtil -::- the input ipAddress from the list currently process

cpm.client.provisioning.utils.ProvisioningUtil -::- the ipAddress that matched the http request remote

cpm.client.provisioning.utils.ProvisioningUtil -::- the clientMac from the macarray list for the for lo

cisco.cpm.client.posture.PostureStatusServlet -::- Found Client IP matching the remote IP 192.168.255.2

cpm.client.provisioning.utils.ProvisioningUtil -::-

Session = 0a3e949c000000495c216240
```

---

4. Après la ligne contenant les mots clés Sent http response, vous pouvez afficher le contenu de la réponse :

<#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_validat

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://clemea1

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

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

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.

cpm.client.provisioning.utils.ProvisioningUtil -::- header X-ISE-SessionId value is 0a3e949c000000495c2

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
```

Enquête sur les rapports ISE

Une fois que l'ID de la session obsolète/fantôme est connu, vous pouvez examiner le rapport Radius Accounting pour mieux comprendre ce qui a provoqué l'obsolescence/fantôme de la session :

---

1. Accédez à Operations > Reports > Endpoints and Users > Radius Accounting report et exécutez ce rapport pendant 7 jours ; utiliser un ID de point de terminaison comme clé de filtre.

---

2. Voici un exemple de rapport qui montre comment la session obsolète a été laissée sur ciscolive-ise2 :

2019-05-30 16:42:13.36	3 Stop	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise1
2019-05-30 16:32:20.819	2 Interim-Update	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2
2019-05-30 16:32:16.263	1 Start	alice	C0:4A:00:1F:6B:39	0a3e949c000002585cf00588	DEMO-WLC	ciscolive-ise2

- Le début de la comptabilisation de la session est arrivé sur PSN ciscolive-ise2.
- La mise à jour intermédiaire de la session a été traitée sur le même PSN.
- Un message d'arrêt de la gestion des comptes pour l'ID de session problématique est arrivé à un PSN différent (ciscolive-ise1.)

Comment identifier le moment où un problème a été causé par l'absence d'un redémarrage de détection

La même logique s'applique au problème précédent, mais la seule différence est que vous devez vous concentrer sur l'heure de début de la dernière analyse. Pour ce type de problème, l'horodatage de la dernière analyse est dans le passé.

Normalement, lorsqu'un utilisateur final découvre un problème, une analyse est effectuée. Dans les journaux ISE Radius Live, les tentatives d'authentification récentes du point d'extrémité problématique sont visibles.

La démonstration montre l'enregistrement des étapes nécessaires à l'identification du problème :

Dépannage avancé de l'absence de redémarrage de la détection

Cette approche est similaire à la section Dépannage avancé des sessions obsolètes/fantômes. L'élément de dépannage principal est l'investigation de l'ensemble DART.

Dans le bundle DART, vous pouvez rechercher des redémarrages de détection (comme indiqué pour le problème précédent) et confirmer qu'il n'y a pas eu de redémarrages de détection au moment où le problème a été signalé.

Côté ISE, concentrez-vous sur le rapport d'authentification Radius Live Logs/Radius pour confirmer qu'il y a eu un basculement entre PSN ou qu'un nouvel ID de session a été généré par NAD.

Solution

Approche classique - Évitement des problèmes

Auparavant, aucune fonctionnalité d'ISE ne permettait de résoudre les problèmes décrits dans ce document. Par conséquent, le seul moyen était de s'appuyer sur l'ensemble des meilleures pratiques mises en oeuvre sur le réseau et côté ISE pour minimiser les risques.

Meilleures pratiques permettant de réduire le nombre de sessions obsolètes ou fantômes dans le déploiement ISE

Toujours implémenter une posture basée sur la redirection si possible

Un contre-argument courant à cette recommandation est qu'une mauvaise expérience utilisateur apparaît dans le système d'exploitation ou les navigateurs sont vus. Cela indique une redirection tandis que le module de posture AnyConnect ISE en arrière-plan effectue un processus d'évaluation.

Pour résoudre ce problème, il est possible de rediriger UNIQUEMENT les sondes de détection de module de posture ISE et d'autoriser sélectivement tout autre trafic. Cet exemple montre une liste de contrôle d'accès de redirection conçue pour rediriger uniquement les requêtes HTTP vers l'hôte de découverte (10.1.1.1 dans cet exemple) et enroll.cisco.com (172.16.1.80) :

```
ip access-list extended REDIRECT-DH-ENROLL
 permit tcp any host 10.1.1.1 eq www
 permit tcp any host 172.16.1.80
 deny   ip any any
```

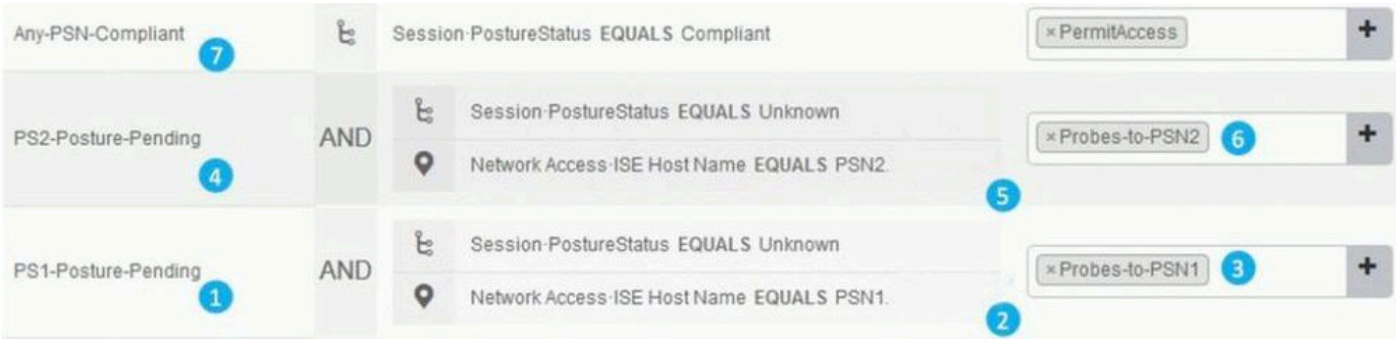
Pour maintenir un niveau de sécurité acceptable, une liste de contrôle d'accès de redirection peut être combinée à une liste de contrôle d'accès attribuée par ISE.

L'état En attente autorise uniquement les connexions à PSN lorsque le point de terminaison a été authentifié

Cette approche est utile pour les environnements où la redirection d'URL n'est pas prise en charge (mises en oeuvre avec les NAD tiers).

En guise de solution, implémentez plusieurs stratégies d'autorisation Posture Pending (une par PSN). Chaque politique doit contenir, parmi les conditions, le nom du PSN où l'authentification a eu lieu. Dans le profil d'autorisation, tous les PSN doivent être bloqués, à l'exception du noeud où l'authentification a eu lieu.

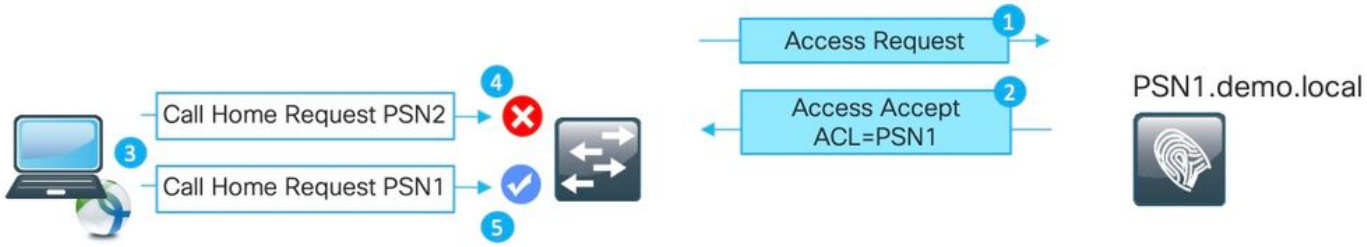
Créez des stratégies d'autorisation pour deux noeuds :



---

1. Stratégie de position en attente pour PSN1.
2. Le nom PSN1 est utilisé comme condition dans la stratégie.
3. Le profil d'autorisation avec ACL bloque l'accès à tous les PSN à l'exception de PSN1.
4. Stratégie de position en attente pour PSN2.
5. Le nom PSN2 est utilisé comme condition dans la stratégie.
6. Le profil d'autorisation avec ACL bloque l'accès à tous les PSN à l'exception de PSN2.
7. Stratégie d'autorisation « Conforme » de la position.

La figure suivante explique le fonctionnement de cette approche :



---

1. L'authentification atteint PSN1.
2. En raison des stratégies d'autorisation configurées, PSN1 attribue le profil d'autorisation, qui bloque l'accès à tous les autres noeuds, à l'exception de PSN1.
3. Le module de posture AnyConnect ISE redémarre le processus de détection.
4. La sonde vers PSN2 est bloquée par le NAD comme par une liste de contrôle d'accès attribuée précédemment.
5. L'analyse vers PSN1 est autorisée par la liste de contrôle d'accès attribuée sur NAD.

Meilleures pratiques des équilibreurs de charge

- Activez la rémanence sur l'équilibreur de charge pour l'authentification et la comptabilité avec Calling-Station-ID comme clé de rémanence. Reportez-vous aux meilleures pratiques pour ISE avec le Guide de déploiement Cisco et F5 : Équilibrage de charge ISE avec BIG-IP.
- Utilisez un minuteur de rémanence plus long qu'une journée de travail moyenne pour couvrir le moment où le PC passe en mode veille (par exemple, 10 heures au lieu de 8 heures).
- Si la réauthentification est implémentée, utilisez le compteur de réauthentification légèrement plus bas que le compteur d'adhésion (utilisez 8 heures si l'adhésion est configurée pendant 10 heures). Cela permet de prolonger l'intervalle d'adhésion par une nouvelle authentification.

Cas d'utilisation de Posture Over VPN

Assurez-vous que l'intervalle de mise à jour intermédiaire de la gestion des comptes est supérieur ou égal à vpn-session-timeout. Cela minimise le battement de compte entre les PSN pendant de longues sessions VPN. Cet exemple montre l'intervalle de mise à jour de la comptabilité intermédiaire configuré pour 20 heures. Cela n'empêche pas la mise à jour intermédiaire initiale qui transporte l'adresse IP attribuée au point d'extrémité.

```
aaa-server ISE protocol radius

 interim-accounting-update periodic 20

group-policy SSL-VPN attributes

 vpn-idle-timeout 1200

 vpn-session-timeout 1200
```

Les Méthodes Recommandées peuvent être mises en oeuvre pour minimiser l'impact de l'absence de redémarrage du module de détection de position ISE

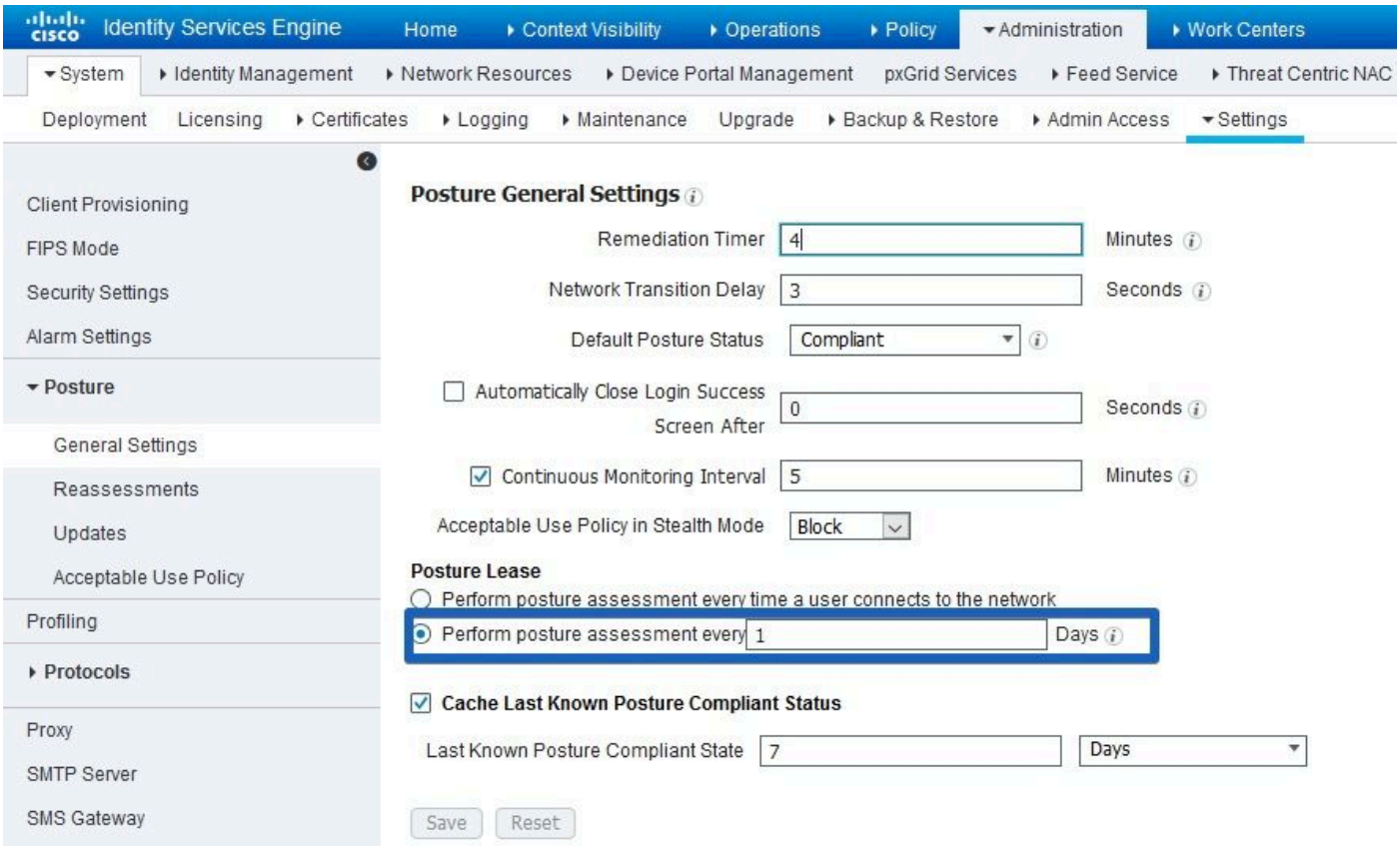
Activer le bail de position

Il s'agit d'une fonctionnalité d'ISE qui marque le terminal comme conforme pour une période définie (1 à 365 jours). La valeur de bail de posture est un attribut de point d'extrémité qui signifie qu'il est stocké sur la base de données ISE. Tous les attributs de point de terminaison qui incluent le bail de position sont répliqués sur tous les noeuds du déploiement ISE.

Lorsque PSN reçoit une nouvelle session pour le point d'extrémité, le bail de position peut être utilisé pour marquer la session comme conforme immédiatement. Pour prendre cette décision, PSN utilise 3 valeurs, à savoir :

---

1. Nombre de jours définis pour le bail de position dans les paramètres ISE : Accédez à Administration > System > Posture > General Settings :



---

2. La valeur de l'attribut PostureExpiry est un attribut de point de terminaison qui contient un horodatage Epoch. La valeur PostureExpiry est initialement renseignée lors de la première tentative de posture réussie pour le point de terminaison après l'activation du bail de posture par l'administrateur ISE. Plus tard, cette valeur est mise à jour lors de la prochaine tentative de posture réussie qui se produit après l'expiration du bail. Vous pouvez voir un PostureExpiry dans Context Visibility > Endpoints pendant que l'un des terminaux affichés est ouvert :

PostureExpiry	1586332942236
PostureOS	Windows 10 Professional 64-bit

---

3. Cette valeur peut être convertie en l'horodatage lisible par l'utilisateur, par exemple, ici - https://www.epochconverter.com/

Convert epoch to human-readable date and vice versa

1586332942236 | Timestamp to Human date | [batch convert]

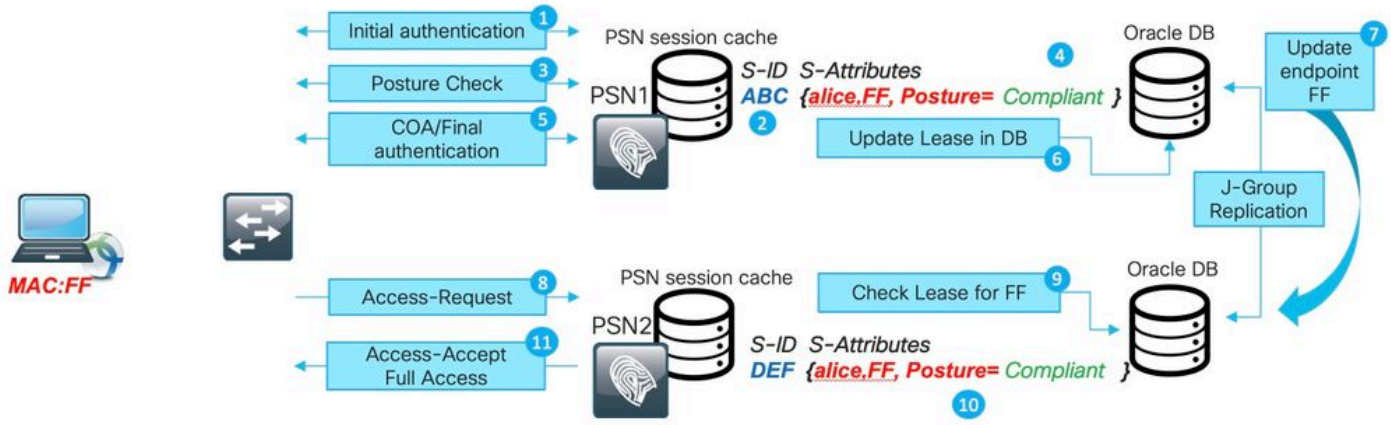
Supports Unix timestamps in seconds, milliseconds, microseconds and nanoseconds.

Assuming that this timestamp is in **milliseconds**:
GMT: Wednesday, 8 April 2020 r., 8:02:22.236

---

3. Lorsque l'authentification d'un point de terminaison avec posture lease atteint PSN, elle utilise PostureExpiry et la date système pour récupérer le nombre de jours écoulés depuis la dernière vérification de posture réussie. Si la valeur de résultat est comprise dans un intervalle de bail de position défini dans les paramètres, la session reçoit un état Conforme. Si la valeur du résultat est supérieure à la valeur du bail, la session reçoit un état Inconnu. Cela déclenche la posture à exécuter à nouveau et la nouvelle valeur PostureExpiry peut être enregistrée.

Ce schéma décrit le processus de basculement :

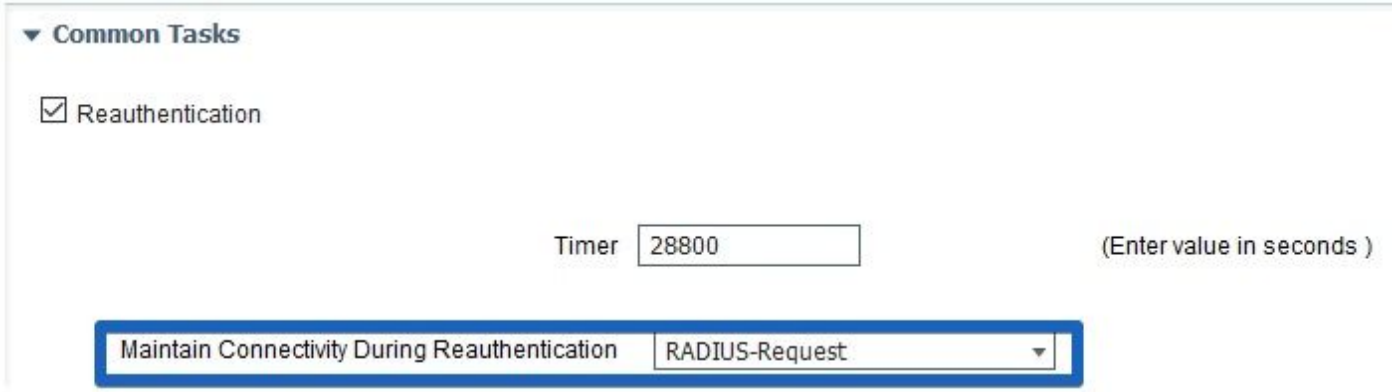


---

1. L'authentification initiale se produit avec PSN1.
2. La session ABC est créée dans le cache de session.
3. L'évaluation de la posture a lieu.
4. L'état de la session devient Conforme.
5. Le certificat d'authenticité est déclenché par un changement d'état de position et entraîne une nouvelle authentification du terminal pour l'appliquer au niveau d'accès suivant.
6. La valeur PostureExpiry est enregistrée dans le point de terminaison.
7. Les données des terminaux sont répliquées sur tout le déploiement.
8. L'authentification suivante atteint PSN2.
9. PSN2 vérifie si le point de terminaison se trouve dans un bail d'état valide.
10. La session est ajoutée au cache de session en tant que Conforme.
11. En raison du bail valide, la session est créée avec l'état de position Conforme.

Implémentation de réauthentification

Poussez toujours le minuteur de réauthentification à partir d'ISE avec la requête RADIUS, qui est sélectionnée dans Maintenir la connectivité pendant la réauthentification. Ce paramètre garantit que NAD conserve le même ID de session lors de la réauthentification.



Environnements avec équilibreurs de charge

Le même ensemble de meilleures pratiques (expliqué dans la section session obsolète/fantôme) peut être mis en oeuvre.

Différents sous-réseaux peuvent être utilisés pour les états En attente et Conforme

Lorsque les conceptions de réseau permettent d'utiliser différents sous-réseaux tels que les états En attente et Conforme, cette approche garantit que chaque modification de l'état de la position entraîne une modification de la passerelle par défaut.

Évaluation de la position utilisée dans le même intervalle qu'un minuteur de réauthentification

L'évaluation de la position peut être activée avec un intervalle égal au minuteur de réauthentification. Lorsque le PSN d'origine n'est pas disponible, l'échec PRA redémarre le processus de détection.

Approche moderne - Partage d'état de posture

Dans le cadre d'une amélioration implémentée (dans l'ID de bogue Cisco CSCvi35647) du patch 6

pour ISE 2.6, il existe une nouvelle fonctionnalité qui implémente le partage de l'état de la position de session sur tous les noeuds du déploiement ISE.

Cette amélioration est intégrée dans les versions futures des correctifs 2 et 3.0 d'ISE 2.7.

Cette nouvelle fonctionnalité est basée sur le mécanisme LSD (Light Session Directory) introduit dans ISE 2.6. Dans les versions plus récentes, cette fonctionnalité a été renommée LDD (Light Data Distribution) Radius Session Directory. Light Data Distribution est activé par défaut et permet le partage d'un contexte de session limité entre les noeuds ISE. Il n'y a pas de réplication de contexte de session complète entre les PSN, seulement une quantité limitée d'attributs partagés pour chaque session.

Light Session Directory supprime la nécessité d'exécuter des appels d'API coûteux en ressources vers MNT lorsque l'un des noeuds du déploiement doit déterminer le propriétaire actuel de la session. La recherche du propriétaire est requise lorsque le flux de certificat d'authenticité démarre. Avec LDD, chaque PSN peut trouver un propriétaire de la session à partir du cache local du répertoire de session Radius.

Architecture de distribution de données légères

Cette fonctionnalité contient les éléments suivants :

- Cache RSD (Radius Session Directory) : ce cache existe sur chaque noeud ISE et stocke toutes les sessions actives présentées dans le déploiement ISE. Chaque session a une quantité limitée d'attributs dans le cache. Voici des exemples d'attributs stockés dans le répertoire de session Radius pour chaque session :
    - ID de session
    - MAC du terminal
    - CallingStationID
    - Adresse IP du terminal
    - PSN IP - PSN où l'authentification a lieu
    - FQDN PSN
    - Adresse IP du NAS
    - NAS-IPv6-Address
    - État : authentifié, démarré, arrêté

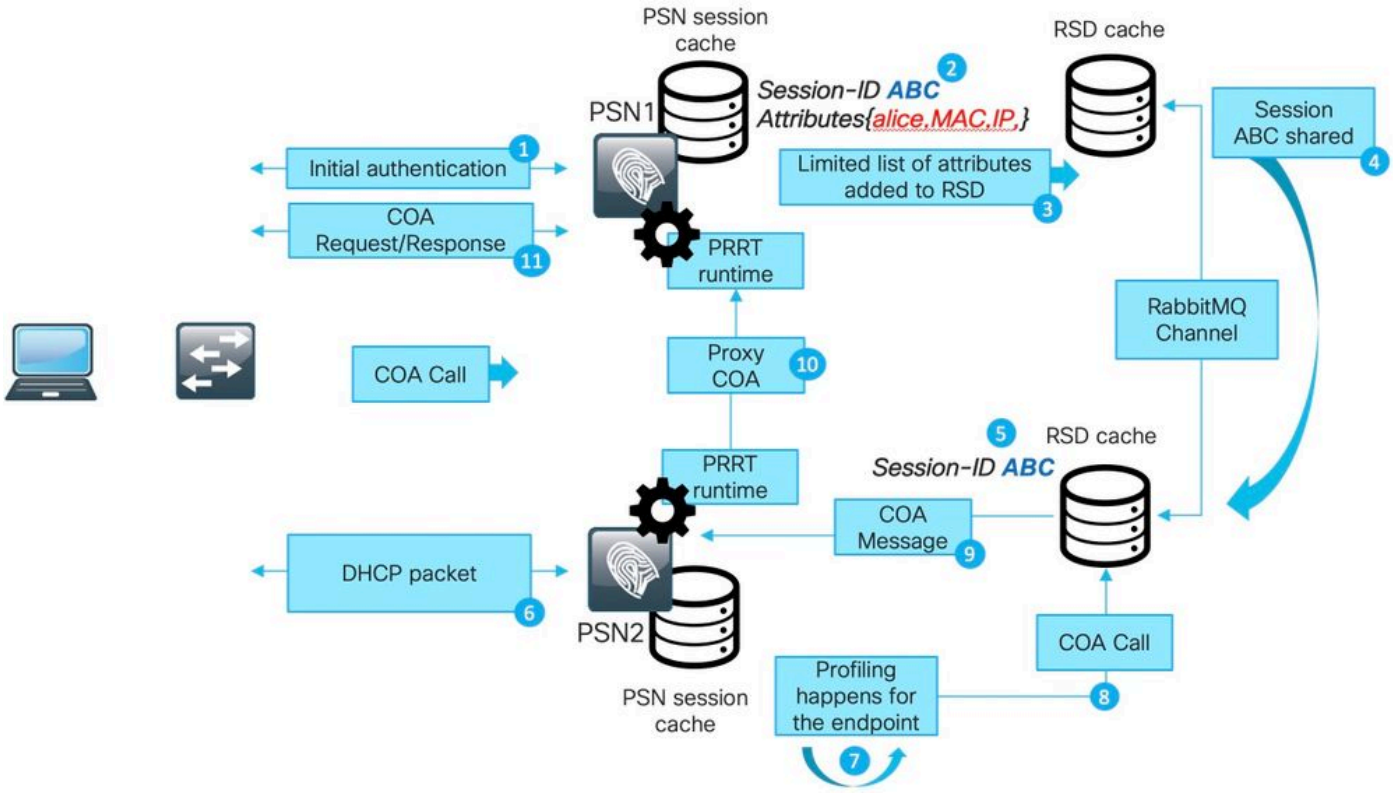
- RabbitMQ Exchange : il existe un échange formé où le serveur de publication, la file d'attente associée et le consommateur sont présentés sur chaque noeud du déploiement ISE. Cela garantit que la topologie à maillage global se forme entre tous les noeuds ISE.

- Éditeur : le répertoire de session Radius représente un éditeur. Lorsqu'une nouvelle authentification réussie est traitée par un PSN, une nouvelle session est créée dans le cache de session PSN. Pour cette session, un ensemble limité d'attributs est placé dans le répertoire de session Radius.

- Consommateur : Sur tous les autres noeuds, le répertoire de session Radius représente un consommateur.

Remarque : La terminologie et l'architecture de General RabbitMQ ne sont pas abordées dans ce document.

L'exemple suivant explique comment le flux COA fonctionne avec le cache RSD :

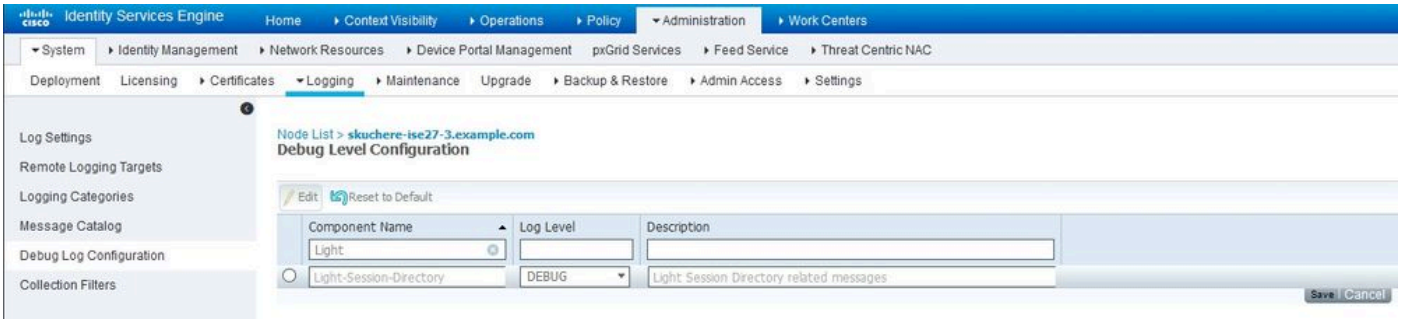


---

1. L'authentification initiale se produit avec PSN1.
2. La session ABC est créée dans le cache de session.
3. Les attributs requis sont enregistrés dans RSD.
4. La session est partagée sur RabbitMQ avec tous les autres noeuds ISE.
5. La session est créée dans le cache RSD sur tous les noeuds ISE.
6. De nouvelles données de profil arrivent sur PSN2.

7. Le point de terminaison est reprofilé et (en cas de modification nécessitant l'exécution du certificat d'authenticité, PSN2) passe à l'étape suivante.
8. Un appel d'API interne est envoyé au cache RSD pour exécuter le certificat d'authenticité.
9. Les données du cache RSD sont utilisées pour préparer un message Proxy COA. Il se déplace d'un noeud ISE à un autre et contient tous les détails que le noeud de destination peut utiliser pour émettre une requête CAO à NAD. Le message de certificat d'authenticité est d'abord transféré en interne vers PRRT Runtime (serveur AAA réel dans ISE).
10. PSN2 envoie un message de certificat d'authenticité à PSN1.
11. PSN1 envoie un message de certificat d'authenticité à NAD.

Pour dépanner la communication sur LDD sur l'ISE, activez le composant Light-Session-Directory dans DEBUG :



Voici un exemple de message de débogage provenant du fichier lsd.log pour une création et une publication de session sur le PSN d'origine :

```
DEBUG  [pool-45-thread-6][] cisco.cpm.lsd.service.LSDRedisClient -::::- Mapping Session ID 0a3e94980000

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

DEBUG  [PrRTEvents-Executor-2][] cisco.cpm.lsd.service.SessionPublisher -::::- Forwarding session 07a26
```

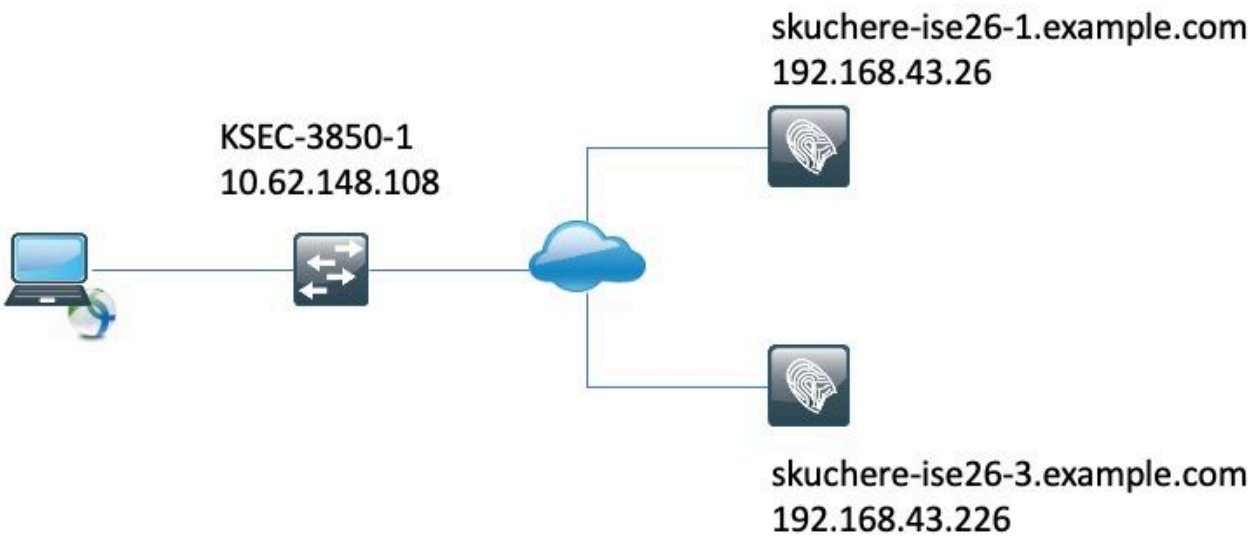
Sur tous les autres noeuds ISE, vous voyez comment une session a été utilisée :

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

Partage d'état de posture sur RSD

Le partage d'état de posture résout les problèmes lorsque la cause principale est une session obsolète/fantôme ou une réauthentification sur un PSN différent qui n'a pas déclenché le redémarrage de la détection. Dès que la session devient conforme, ces informations sont placées dans la session RSD et peuvent ensuite être utilisées par chaque PSN dans le déploiement.

Il existe d'autres cas d'angle que la fonction décrite ne peut pas résoudre. Par exemple, lorsque NAD exécute la réauthentification sur le même PSN mais avec un ID de session différent. Ces scénarios peuvent être traités à l'aide des meilleures pratiques décrites dans ce document. Cette figure illustre la topologie utilisée pour tester le partage de l'état de position :



Partage d'état de position sur RSD - Session obsolète/fantôme

Pour créer une session obsolète, l'authentification doit d'abord être effectuée sur skuchere-ise26-1. Ensuite, NAD doit être reconfiguré pour envoyer la comptabilisation à skuchere-ise26-3. Après qu'un message de comptabilisation a été transféré au PSN incorrect, NAD doit être reconfiguré (à nouveau) pour renvoyer la comptabilisation à skuchere-ise26-1.

Cette image montre un rapport de comptabilité qui prouve la présence de la session fantôme sur skuchere-ise26-3 :

	Stop	3.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296
	Interim-Update	2.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-3	0A3E946C0000007D5B679296
	Start	1.	bob@example.com	00:50:56:B6:0B:C6	skuchere-ise26-1	0A3E946C0000007D5B679296

---

1. Messages Accounting-Start traités par skuchere-ise26-1.
2. Interim Accounting-Update pour la même session traitée par skuchere-ise26-3.
3. La session se termine plus tard sur skuchere-ise26-1.

Le point d'extrémité se connecte au réseau, mais la redirection ne fonctionne plus. Dans le journal guest.log de PSN pour skuchere-ise26-3, vous pouvez voir ces messages de journal avec le composant client-webapp activé dans DEBUG :

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

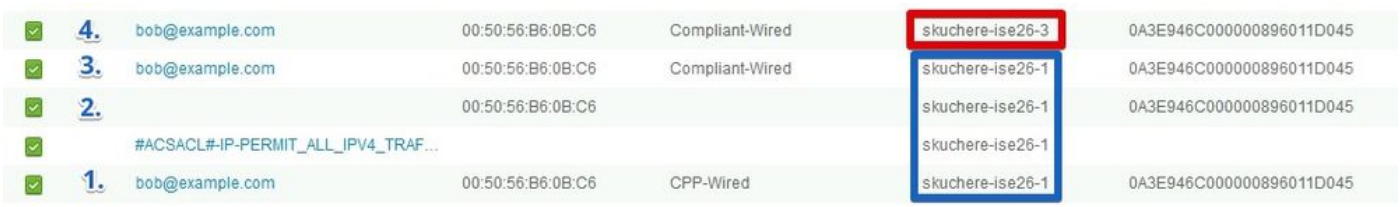
Lorsque PSN détecte qu'il détient une session obsolète/fantôme pour le terminal, il ne répond pas au module de posture ISE et cela vous permet d'obtenir des informations de PSN où la dernière authentification a eu lieu.

Comme solution au problème de session obsolète/fantôme au moment de la recherche de session, PSN vérifie la présence de toute nouvelle session pour le terminal dans le RSD. Si RSD contient un ID de session différent de celui de PSN dans le cache de session local, il suppose que la session (présentée dans le cache de session) est périmée.

Partage d'état de position sur RSD - Basculement entre PSN

Pour reproduire ce scénario, un temporisateur de réauthentification courte est activé dans le profil d'autorisation affecté au point d'extrémité d'état conforme. Par la suite, NAD est reconfiguré pour envoyer l'authentification et la gestion des comptes à un autre PSN (skuchere-ise26-3). À l'expiration du minuteur de réauthentification, la même session n'est pas authentifiée sur le PSN différent.

La figure suivante illustre un rapport d'authentification qui montre le basculement pour la même session de skuchere-ise26-1 à skuchere-ise26-3 :



☑	4.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-3	0A3E946C000000896011D045
☑	3.	bob@example.com	00:50:56:B6:0B:C6	Compliant-Wired	skuchere-ise26-1	0A3E946C000000896011D045
☑	2.		00:50:56:B6:0B:C6		skuchere-ise26-1	0A3E946C000000896011D045
☑		#ACSACL#-IP-PERMIT_ALL_IPV4_TRAF...			skuchere-ise26-1	
☑	1.	bob@example.com	00:50:56:B6:0B:C6	CPP-Wired	skuchere-ise26-1	0A3E946C000000896011D045

---

1. L'authentification se produit sur skuchere-ise26-1, le profil d'autorisation avec redirection est attribué.
2. COA après évaluation de la posture réussie.
3. L'authentification suivante du profil d'autorisation à l'état conforme est attribuée.
4. L'authentification atteint un PSN différent, mais elle reçoit toujours un profil d'autorisation pour l'état conforme.

La session a l'état de conformité sur le nouveau PSN après le basculement dans ise-psc.log avec les composants epm-pip et nsf-session activés dans 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 con
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.PIPManager -::::- Returning a PIP co
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.api.ExecutionContext -::::- Execution con
2020-04-09 11:06:42,176 DEBUG [Thread-7979][] cpm.nsf.session.impl.SessionCache -::::- Looking up sessi
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 se
IndexValues: {}

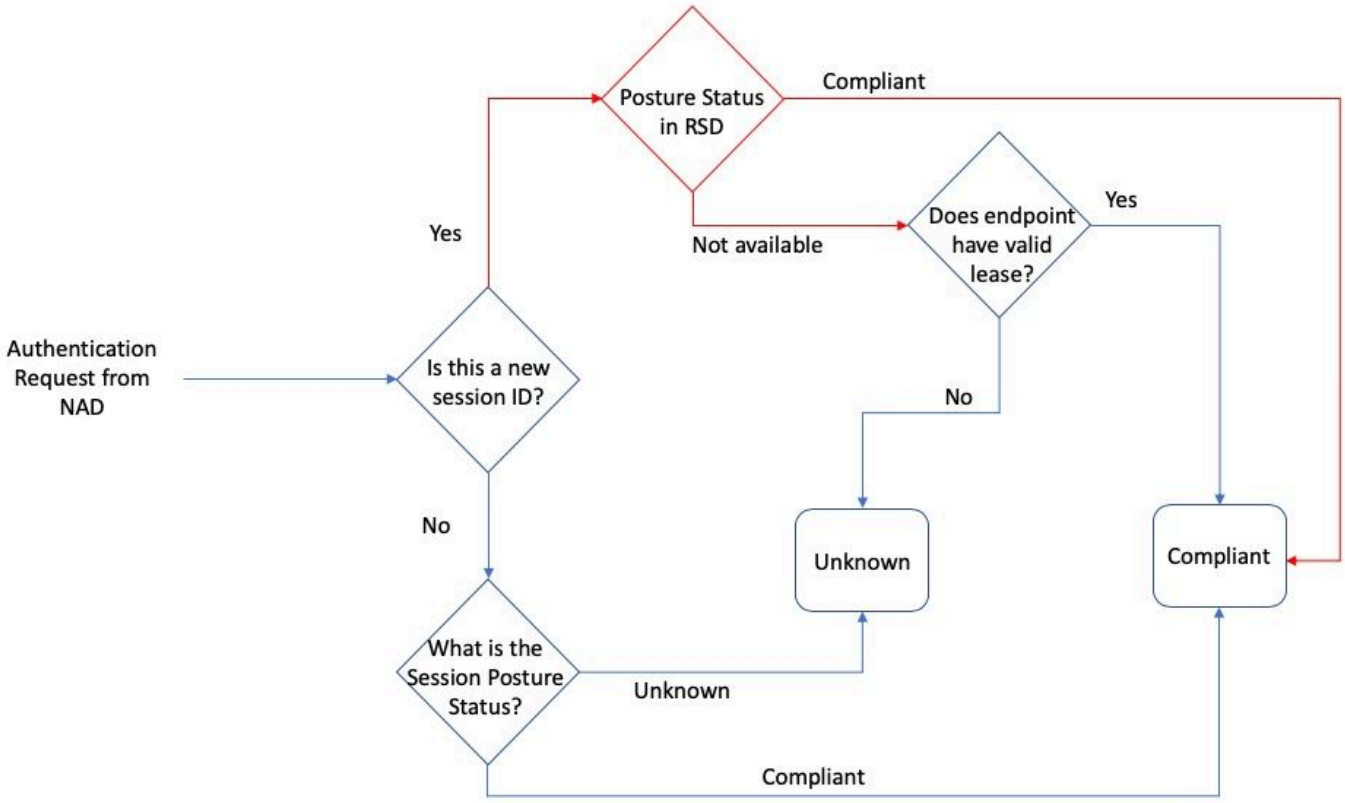
2020-04-09 11:06:42,177 DEBUG [Thread-7979][] cisco.cpm.posture.pip.PostureStatusPIP -::::-

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
```

Le problème initial est résolu par l'ajout d'une logique supplémentaire dans le processus de sélection de l'état de posture. Cette figure illustre ce qui a été modifié (les modifications sont surlignées en rouge) :


Posture Status in RSD
Compliant
Yes
Not available
Does endpoint have valid lease?
Yes
Authentication Request from NAD
Is this a new session ID?
No
No
Unknown
Compliant
What is the Session Posture Status?
Unknown
Compliant

À propos de cette traduction
Cisco a traduit ce document en traduction automatisée vérifiée par une personne dans le cadre d'un service mondial permettant à nos utilisateurs d'obtenir le contenu d'assistance dans leur propre langue.

Il convient cependant de noter que même la meilleure traduction automatisée ne sera pas aussi précise que celle fournie par un traducteur professionnel.