Fehlerbehebung bei Fehlern der VPN- und RADIUS-Authentifizierung nach ISE 3.4

Inhalt

Problem

Bei ISE 3.4 Patch 4-Bereitstellungen treten Authentifizierungsfehler auf, wenn ein sekundärer Administrationsknoten (SAN) ausfällt. Authentifizierungsanforderungen, die an den Primary Policy Administration Node (PPAN) gerichtet sind, schlagen ebenfalls fehl, was zu Unterbrechungen bei ASA-VPN-Verbindungen und RADIUS-Authentifizierungen führt. Der SAN-Knoten wird im ISE-Bereitstellungs-Dashboard als getrennt angezeigt, und die Protokolle weisen auf EAP/TLS-bezogene Fehler und Probleme bei der Sitzungsverfolgung hin.

Umwelt

- Cisco Identity Services Engine (ISE)
- Netzwerkzugriffsgeräte (NADs): Umfasst Meraki-Geräte und/oder ASA-Firewall
- Topologie: Multi-Node ISE-Bereitstellung mit SAN und PPAN

Auflösung

1.- Entfernen Sie alle Personen vom SAN-Knoten über die Cisco ISE-Administrationsoberfläche, indem Sie zu Administration > System > Deployment navigieren. Dadurch werden die Authentifizierungsversuche für den ausgefallenen Knoten angehalten, und nicht betroffene Knoten können die Verarbeitung fortsetzen.

 Anmerkung: Nach dem Entfernen des Benutzers wird der SAN-Knoten im Bereitstellungs-

---

Dashboard weiterhin als nicht verbunden (Rotes X) angezeigt.

2.- Erzwingen Sie die ASA-Firewall manuell, den SAN-Knoten als FEHLGESCHLAGEN zu betrachten, sodass keine weiteren Authentifizierungsversuche an das nicht verfügbare SAN weitergeleitet werden. Diese Aktion wird in der ASA-Konfiguration durchgeführt, um ein Failover auf betriebsbereite ISE-Knoten sicherzustellen.

3.- Überprüfen Sie die ISE-Bereitstellung auf ordnungsgemäße Synchronisierung und überwachen Sie Integritätsmetriken wie CPU, Arbeitsspeicher und Festplattennutzung.

4.- Überprüfen Sie, ob die Authentifizierungsdienste funktionsfähig sind, indem Sie überprüfen, ob neue Dot1x- und RADIUS-Anforderungen von den nicht betroffenen ISE-Knoten verarbeitet werden.

5.- Sammeln von DEBUG-Protokollen und Paketerfassungen bei Authentifizierungsfehlern, um die EAP/TLS-Verhandlungszeit und die Sitzungsrücksetzung zu analysieren.

6.- Setzen Sie die Überwachung der ISE-Systemstatusmetriken und des Authentifizierungsverhaltens nach SAN-Failover-Ereignissen fort.

7.- Überprüfen Sie das Meraki RADIUS-Failover-Verhalten. Beachten Sie dabei, dass die ISE RADIUS-Pakete mit "Status-Server" für die Erkennung der Serververfügbarkeit nicht unterstützt.

Beispiel für Protokollnachrichten

```
Accounting start was received for non-existing session
```

```
Error getting peer certificate from SSL Connection
```

```
packet for this endpoint 58-6D-67-XX-XX-XX is being processed right now so drop the new EAP session
```

```
Long step latency ;2=57290
```

```
Endpoint 58-6D-67-XX-XX-XX abandoned EAP session xxxxxxxxx/552628443/4183334 and started EAP session
```

Ursache

Die Hauptursache ist ein Ausfall eines SAN-Knotens aufgrund eines ISP-Verbindungsfehlers, der zu Inkonsistenzen bei der Sitzungsverfolgung und EAP/TLS-Verhandlungsfehlern zwischen den Supplicant-, NAD- und ISE-Knoten führt. Meraki-Geräte verwenden für die Failover-Erkennung "Status-Server"-RADIUS-Pakete, die von der Cisco ISE nicht unterstützt werden. Dies führt zu fortgesetzten Authentifizierungsversuchen für den ausgefallenen SAN-Knoten.

Verwandte Inhalte

- Vorgehensweise: Integration von Meraki-Netzwerken mit der ISE
- Konfiguration eines Remote-Access-VPN mit RADIUS-Authentifizierung auf der ISE und Zuordnung von Gruppenrichtlinien
- Technischer Support und Downloads von Cisco

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.