Solución de problemas de autenticación RADIUS y VPN ISE 3.4

Contenido

Problema

Las implementaciones del parche 4 de ISE 3.4 experimentan fallos de autenticación cuando un nodo de administración secundario (SAN) sufre una interrupción. Las solicitudes de autenticación dirigidas al nodo de administración de políticas principal (PPAN) también fallan, lo que provoca interrupciones en las conexiones VPN ASA y las autenticaciones RADIUS. El nodo SAN se muestra como desconectado en el panel de implementación de ISE y los registros indican errores relacionados con EAP/TLS y problemas de seguimiento de sesiones.

Entorno

- Cisco Identity Services Engine (ISE)
- Dispositivos de acceso a la red (NAD): Incluye dispositivos Meraki o firewall ASA
- Topología: Implementación de ISE de varios nodos con SAN y PAN

Resolución

1.- Elimine todas las personas del nodo SAN a través de la interfaz de administración de Cisco ISE navegando hasta Administration > System > Deployment. Esto detiene los intentos de autenticación en el nodo fallido y permite que los nodos no afectados reanuden el procesamiento.

Nota: Tras la eliminación de persona, el nodo SAN continúa apareciendo como desconectado (X roja) en el panel de implementación.

2.- Forzar manualmente al firewall ASA a considerar el nodo SAN como FALLIDO, evitando que se dirijan más intentos de autenticación hacia la SAN no disponible. Esta acción se realiza en la configuración de ASA, lo que garantiza la conmutación por error a los nodos ISE operativos.

3.- Revisar la implementación de ISE para la sincronización adecuada y supervisar las métricas de estado, incluida la utilización de la CPU, la memoria y el disco.

4.- Verifique que los servicios de autenticación estén operativos comprobando que los nodos ISE no afectados procesen las nuevas solicitudes Dot1x y RADIUS.

5.- Recopilar registros DEBUG y capturas de paquetes durante los fallos de autenticación para analizar el tiempo de negociación EAP/TLS y los reinicios de sesión.

6.- Seguir supervisando las métricas de estado del sistema ISE y el comportamiento de autenticación tras los eventos de fallo de SAN.

7.- Validar el comportamiento de conmutación por fallo Meraki RADIUS, teniendo en cuenta que ISE no admite paquetes RADIUS de "servidor de estado" para la detección de disponibilidad del servidor.

Ejemplo de mensajes de registro

```
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
```

Causa

La causa raíz es una interrupción del nodo SAN debido a un fallo del enlace ISP, que provoca incoherencias en el seguimiento de la sesión y errores de negociación EAP/TLS entre los nodos del solicitante, NAD e ISE. Además, los dispositivos Meraki se basan en paquetes RADIUS de "servidor de estado" para la detección de fallos, que Cisco ISE no admite, lo que provoca continuos intentos de autenticación del nodo SAN que ha fallado.

Contenido relacionado

- CÓMO: Integre las redes Meraki con ISE
- Configuración de VPN de acceso remoto con autenticación RADIUS en ISE y asignación de políticas de grupo
- Soporte técnico y descargas de Cisco

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).