Agotamiento del contexto RADIUS de ISE hace que el nodo deje de responder

Contenido

Problema

Un nodo de Cisco Identity Services Engine (ISE) deja de responder intermitentemente a las solicitudes de autenticación RADIUS, lo que provoca que los dispositivos de red lo marquen como "RADIUS DEAD". El nodo afectado recibe solicitudes RADIUS (confirmadas a través de los registros del firewall y las capturas de paquetes), pero no puede responder. Se observan los siguientes síntomas:

- Mensajes de retransmisión RADIUS en dispositivos de red
- Aparecen alarmas críticas de "Error en la asignación de contexto de RADIUS" en ISE
- Mensajes de registro que indican "Límite de conteo de contexto de aciertos. ¡Descarte de solicitud!"
- La GUI de ISE se vuelve inaccesible durante el problema a pesar de que todos los servicios se muestran como en ejecución
- Los reinicios del nodo resuelven temporalmente el problema durante aproximadamente 30 minutos antes de que se repita

Entre los mensajes de error específicos observados se incluyen:

```
033057: Mar 11 09:33:59.015: RADIUS: Retransmit to (10.0.5.11:1812,1813) for id 1645/127
033058: Mar 11 09:33:59.015: RADIUS: PAC key found while sending request (rctx:0x75EB6A555690)
033059: Mar 11 09:33:59.015: RADIUS: Message Authenticator encoded
033060: Mar 11 09:33:59.015: RADIUS(00000000): Started 4 sec timeout
```

Y en los registros de ISE:

```
RadiusListener,2026-06-28 23:21:22,149,WARN ,0x7efea2055700,NIL-CONTEXT,Hit context count limit. Droppi
```

Entorno

- Cisco Identity Services Engine (ISE) versión 3.5.0.331 (parche 3)
- Nodo que sirve a varios roles: Nodo de administración principal (PAN), Administración de sesiones y solución de problemas (SMNT) y Nodo de servicios de políticas (PSN)
- Métodos de autenticación: Tanto 802.1X como MAB están activados en los puertos del switch de acceso
- Fuentes de identidad externas: Integración con Microsoft Entra ID
- Dispositivos de red configurados con ISE como servidor RADIUS para la autenticación

Resolución

El problema se resolvió mediante la aplicación de una revisión proporcionada por Cisco que aborda una condición de interbloqueo en el proceso ISE SessionUpdater. Siga estos pasos para implementar la resolución:

Paso 1: Obtener e instalar la revisión

Descargue los archivos de revisión de Cisco y transfiéralos al repositorio de nodos de ISE. Los archivos de revisión son:

- ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (archivo de instalación)
- ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz (archivo de rollback)

Paso 2: Aplicar la revisión

Instale la revisión mediante el comando CLI:

```
application install ise-apply-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

⚠Precaución: Posible. Los detalles mencionados aquí parecen contener procedimientos o comandos que podrían causar un impacto significativo si se ejecutan. Asegúrese de que una PYME o una unidad de negocio ha evaluado los procedimientos o comandos anteriores antes de ejecutarlos o recomendarlos.

Paso 3: Verificar instalación

Verifique la instalación de la revisión mediante uno de estos comandos:

```
show logging application hotpatch.log
```

O bien:

```
show version
```

Paso 4: Supervisión del sistema

Después de la instalación, supervise el nodo de ISE durante un mínimo de dos semanas para asegurarse de que el problema no se repita. La instalación de la revisión requiere un reinicio del servicio, por lo que debe planificarse durante una ventana de mantenimiento.

Opcional: Procedimiento de reversión

Si es necesario, la revisión se puede eliminar mediante el comando rollback:

```
application install ise-rollback-CSCwv71473_3.5.0.527_patch3-SPA.tar.gz <repository name>
```

Comandos de resolución de problemas para supervisión

Para supervisar la asignación de contexto RADIUS, utilice:

```
show logging application prrt-server.log | include ContextN
```

Habilite los debugs AAA en tiempo de ejecución antes de cualquier troubleshooting futuro:

```
debug aaa runtime
```

Causa

La causa raíz se identificó como una condición de interbloqueo en el proceso ISE SessionUpdater. Cuando se produjeron eventos de inicio y detención de cuentas simultáneas para la misma sesión, dos subprocesos entraron en un escenario de espera circular:

- Hilo-162: cacheLock propio, se esperó el bloqueo SessionInfo
- Hilo-125: bloqueo SessionInfo propio, se esperó a cacheLock

Esta espera circular provocó fugas de ContextN y una cola de procesamiento RADIUS en continuo crecimiento. La acumulación de colas acabó agotando los contextos RADIUS disponibles, lo que provocó que la latencia de autenticación y los dispositivos de red marcaran el nodo ISE como RADIUS DEAD.

El problema se documenta con el ID de bug de Cisco CSCwv71473.

Contenido relacionado

- ID de bug de Cisco CSCwv71473
- 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).