Resolución de problemas de ISE Agentless Posture Not Triggering after Session Reauthentication

Contenido

Problema

La funcionalidad de estado sin agente de Identity Services Engine (ISE) 3.3 no se activa tras los eventos de reautenticación de sesión. Durante la autenticación inicial, la condición sin agente funciona correctamente y los terminales cumplen las normativas. Sin embargo, cuando se produce una nueva autenticación, los extremos reciben eventos de actualización intermedia de cuentas RADIUS en lugar de eventos de inicio de cuentas, lo que hace que no se invoque el flujo de estado sin agente. Como resultado, los terminales coinciden con una política de estado desconocida y permanecen en un estado desconocido, lo que afecta al acceso a la red de los dispositivos afectados.

El problema se manifiesta con los terminales atascados en el estado "Postura pendiente" o "Desconocido" después de la reautenticación, con aproximadamente 800 de los 1200 terminales afectados en el entorno notificado. El análisis de registro muestra que, durante la reautenticación, ISE recibe eventos ACCOUNTING_UPDATE con agentEnabled=true, pero no se vuelve a invocar el flujo de estado para el ID de sesión existente.

Entorno

- Parche 4 de Identity Services Engine (ISE) versión 3.3
- Autenticación 802.1X por cable con derivación de autenticación MAC (MAB)
- Configuración de estado sin agente habilitada
- Temporizadores de reautenticación de sesión configurados (tiempo de espera de 420 segundos)
- Switches Cisco Catalyst como dispositivos de acceso a la red
- Aproximadamente 1200 terminales en el entorno

Resolución

Se espera este comportamiento y está diseñado en ISE. La postura sin agente sólo es activada por los eventos de inicio de cuentas RADIUS y no debe ser invocada de nuevo por los eventos de actualización intermedia de cuentas durante la reautenticación de sesión cuando la dirección IP entramada permanece sin cambios.

Análisis técnico

La ruta de código de ISE NetAccessEventHandler solo reorganiza el flujo de estado sin agente en paquetes de inicio de cuentas RADIUS nuevos. Durante la reautenticación, los dispositivos de red normalmente envían paquetes de actualización intermedia de cuentas con el mismo Acct-Session-Id, lo que hace que la función shouldInvokePostureFlow() devuelva false, lo que impide la reevaluación del estado.

Evidencia de registro que muestra el comportamiento:

Autenticación inicial (desencadenado por estado sin agente):

```
2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle

2026-04-01 11:28:20,466 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Reautenticación (postura sin agente no activada):

```
2026-04-01 11:35:37,669 DEBUG [PrRTEvents-Executor-2][[]] cisco.cpm.posture.events.NetAccessEventHandle
```

Solución alternativa recomendada

Para mitigar el impacto de este comportamiento, configure la configuración de arrendamiento de estado para mantener la conformidad de los terminales durante los escenarios de reautenticación:

Paso 1: Configure la duración de arrendamiento del estado adecuada en las políticas de estado de ISE para garantizar que los terminales no pierdan acceso a la red entre las evaluaciones de estado.

Paso 2: Supervise el estado de los terminales y ajuste los temporizadores de arrendamiento en función de los requisitos de seguridad y la frecuencia de reautenticación de su organización.

Causa

Este es el comportamiento esperado documentado en el ID de bug de Cisco CSCwu48086. La postura sin agente en ISE está diseñada para activarse sólo en eventos de inicio de cuentas RADIUS y no es activada por eventos de actualización de cuentas provisionales. Durante la reautenticación de la sesión, los dispositivos de acceso a la red envían actualizaciones intermedias de cuentas con la misma dirección IP entramada e ID de sesión, que no vuelven a invocar el proceso de evaluación de estado sin agente. El código ISE comprueba específicamente si hay nuevas sesiones (eventos ACCOUNTING_START) antes de iniciar flujos de estado sin agente.

Contenido relacionado

- ID de bug de Cisco CSCwu48086
- 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).