Acceso VPN AnyConnect de cliente seguro denegado debido a problemas de cumplimiento de condición de seguridad de terminales

Contenido

Problema

Varios usuarios no pueden conectarse a AnyConnect VPN ni a Zero Trust Access (ZTA) y reciben el mensaje de error "Login denied. Su entorno no cumple los criterios de acceso definidos por el administrador."

El problema está relacionado con el cumplimiento del estado del terminal, donde se informa que el requisito de Endpoint Security Agent no coincide. Los usuarios experimentan una denegación de acceso a VPN y ZTA cuando intentan conectarse a través de Cisco Secure Client.

La evaluación del estado muestra que el estado de Trellix Endpoint Security está fallando en los terminales afectados, lo que impide una autenticación correcta en el servicio VPN.

Entorno

- Cisco Secure Client (AnyConnect y acceso de confianza cero)
- Trellix Endpoint Security Agent versión 5.8.4.505
- Perfil de postura de VPN: KFIN_SECURE_VPN con aplicación de agentes de seguridad de terminales
- Requisito de posición: Agente de seguridad de terminales en ejecución con actualizaciones en los últimos 14 días
- Terminales de Windows con Trellix Agent Service en ejecución
- Procesos de Umbrella Agent detectados en terminales

Resolución

El problema se resolvió al resolver los problemas de cumplimiento de estado del agente de Trellix Endpoint Security. Se implementaron los pasos de solución de problemas y resolución descritos en las siguientes secciones.

Paso 1: Validar configuración del perfil de postura

Revise el perfil de estado de VPN para confirmar los requisitos del agente de seguridad del terminal. El perfil KFIN_SECURE_VPN exige que un agente de seguridad de terminal se esté ejecutando y actualizando en los últimos 14 días.

Paso 2: Verificar el estado de seguridad del terminal Trellix

Compruebe el estado actual del agente de seguridad de terminales de Trellix en los terminales afectados:

```
Trellix Agent Service: masvc.exe
Version: 5.8.4.505
Install Location: C:\Program Files\McAfee\Agent\
Display Name: Trellix Agent
Publisher: Trellix
```

Paso 3: Reinstale Trellix Endpoint Security

Realice una reinstalación completa de Trellix Endpoint Security en los terminales afectados:

1. Desinstale por completo el agente de Trellix Endpoint Security existente.

2. Reinicie el sistema.

3. Instale la última versión aprobada del agente de Trellix según los estándares de la

organización.

4. Asegúrese de que el agente se está ejecutando correctamente tras la instalación.

5. Confirme que las actualizaciones de firma/contenido se han completado correctamente.

Paso 4: Habilitar el registro de TRACE para Cisco Secure Client (ZTA)

Active el registro detallado para capturar los detalles de evaluación de estado.

Cree el archivo logconfig.json con este contenido:

```
{ "global": "DBG_TRACE" }
```

Coloque el archivo en el directorio correspondiente:

- Windows: C:\ProgramData\Cisco\Cisco Secure Client\ZTA
- macOS: /opt/cisco/secureclient/zta

Reinicie el servicio Cisco Secure Client/ZTA después de crear el archivo.

Paso 5: Recopilar paquete DART actualizado

Después de implementar los cambios, recopile un nuevo paquete DART para validar la resolución y confirmar la detección de cumplimiento de estado adecuada.

Causa

La causa raíz se identificó como problemas de cumplimiento de estado del agente de Trellix Endpoint Security. El perfil de estado de VPN requería que un agente de seguridad de terminales

se ejecutara con actualizaciones en los últimos 14 días, pero el agente de seguridad de terminales de Trellix no cumplía estos criterios de conformidad. El módulo de evaluación de estado no ha podido detectar o validar correctamente el estado del agente de seguridad de terminales, lo que ha provocado la denegación de acceso para las conexiones VPN y ZTA. El problema estaba específicamente relacionado con la configuración del agente de Trellix y requirió la intervención del equipo de soporte de Trellix para resolver los problemas de cumplimiento del agente subyacente.

Contenido relacionado

- Recopilar registros detallados de ZTNA para la resolución de problemas
- 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).