Resolución de problemas de errores APP_UNREACHABLE para aplicaciones privadas en Secure Access

Contenido

Problema

Al intentar acceder a las aplicaciones de acceso a red de confianza cero (ZTNA) a través de Cisco Secure Access, los usuarios encuentran un mensaje de error de "Aplicación inalcanzable".

- El conector muestra estado saludable/activo en el panel y su propietario confirma que está ejecutando la aplicación.
- La falla puede afectar a todos los usuarios de una aplicación, mientras que otras aplicaciones suministradas por el mismo conector funcionan normalmente.
- En las implementaciones de conjunto de conectores, los fallos pueden parecer intermitentes: las sesiones se realizan correctamente o fallan en función del conector del conjunto que se seleccione.

Entorno

- Implementación de Cisco Secure Private Access con ZTNA
- Recursos privados configurados para el acceso ZTNA
- Implementación del conector de recursos para el acceso a recursos privados

Resolución

Paso 1. Pruebe la disponibilidad directa desde el segmento de red de conectores

- El conector de recursos es un dispositivo bloqueado y no proporciona acceso al shell para ejecutar comandos como curl o nc directamente. En su lugar, realice la prueba de disponibilidad desde un host de prueba (o una VM temporal) ubicado en la misma subred/VLAN que el conector, de modo que obedezca las mismas reglas de ruta de red, ruteo y firewall a la aplicación:

```
curl -v http://APP_IP:PORT/health
nc -zv APP_IP PORT
```

- Si esto falla, el problema se confirma en la ruta de red o en el servidor de aplicaciones. Solucione este problema antes de revisar cualquier configuración de Secure Access.

Nota: Una prueba de una subred diferente no es concluyente: las reglas de firewall y el ruteo se evalúan por origen, ya que el origen de prueba debe reflejar la ubicación IP del conector lo más cerca posible.

Paso 2. Verificar la Configuración de Recursos Privados

- En el panel de Secure Access, navegue hasta Resources > Private Resources, abra el recurso privado afectado y compare la IP configurada, FQDN y carácter por carácter del puerto con la dirección de enlace y el puerto reales de la aplicación en ejecución.
- Cualquier discordancia (IP obsoleta después de una migración de servidor, puerto incorrecto, HTTP frente a HTTPS) produce APP_UNREACHABLE incluso con una ruta de red perfectamente correcta.

Paso 3. Validar la resolución DNS para el conector

- Si el recurso privado está definido por FQDN, compruebe que los servidores DNS asignados al conector pueden resolverlo. Desde la CLI del conector de recursos (las implementaciones de VM proporcionan una CLI de diagnóstico con comandos de solución de problemas de Linux estándar compatibles), ejecute:

```
nslookup app.internal.company.com <internal_DNS_server_IP>
```

- Confirme que se devuelve la IP privada correcta. Asegúrese de que los puntos de configuración de red del conector se encuentren en servidores DNS internos que puedan resolver los FQDN de las aplicaciones privadas; un conector configurado con resolvers públicos no puede resolver zonas internas.

Paso 4. Revisar la ruta del firewall

- Confirme que las reglas de firewall (firewalls de red y firewall de host en el servidor de aplicaciones) permiten el tráfico desde la dirección IP del conector a la IP del servidor de aplicaciones en el puerto requerido.

Paso 5. Capture Traffic with tcpdump on the Resource Connector

- Ejecute una captura de paquetes en el conector de recursos para observar los últimos intentos de conexión de milla hacia la aplicación. La utilidad tcpdump está disponible en el Conector de recursos; consulte la guía Ejecutar tcpdump en conectores de recursos.

Consejo: Para que la captura sea determinista en una implementación de grupo de conectores, mantenga temporalmente un conector de recursos habilitado en el grupo para que todas las sesiones del recurso lo atraviesen y, a continuación, ejecute la captura filtrada en el servidor de aplicaciones y el puerto.

- Por ejemplo:

```
tcpdump 'host x.x.x.x and tcp port 443'
```

(donde x.x.x.x es la IP del servidor de aplicaciones y 443 es el puerto de la aplicación)

- Interpretar los resultados: los SYN salientes sin SYN-ACK indican una caída del firewall o que la aplicación no escucha; un RST inmediato indica que el host es alcanzable pero no

hay nada enlazado al puerto; ningún paquete hacia la aplicación indica que la sesión no está llegando a este conector o que el DNS se ha resuelto en una dirección inesperada.

- Vuelva a habilitar los conectores restantes en el grupo una vez que se complete la captura.

Causa

- Firewall que bloquea el tráfico de conector a aplicación: Un firewall de red o basado en host bloquea el puerto necesario entre la IP de host del conector y la IP del servidor de aplicaciones.
- Discordancia de configuración de recursos privados en Secure Access: La IP, FQDN o puerto configurado en la definición de recurso privado (Recursos > Recursos privados) no coincide con lo que la aplicación escucha realmente (por ejemplo, la aplicación se movió a una nueva IP o escucha en 8443 mientras que 443 está configurado).
- Error de resolución DNS para el conector: El recurso privado está definido por FQDN, pero los servidores DNS del conector no resuelven FQDN de aplicaciones privadas.
- Servidor de aplicaciones inactivo o sin escucha: El servidor parece saludable según otras medidas pero no está enlazado al puerto esperado, o el servicio falló mientras el host permanecía activo.
- Alcance parcial en un conjunto de conectores: Uno o más conectores del conjunto se encuentran en un segmento de red que no puede alcanzar la aplicación, por lo que solo fallan las sesiones asignadas a esos conectores.

Contenido relacionado

- Solución de problemas y recopilación de información básica para Cisco Secure Access
- 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).