

Resolución de problemas de acceso privado con ZTNA CLAP/BAP a través de conectores de recursos debido a una falla de DNS

Contenido

[Problema](#)

[Entorno](#)

[Resolución](#)

[Paso 1: Comparar la configuración DNS entre entornos](#)

[Paso 2: Probar configuración alternativa de servidor DNS](#)

[Paso 3: Validar resolución DNS y conectividad](#)

[Causa](#)

[Contenido relacionado](#)

- [Problema](#)
 - [Entorno](#)
 - [Resolución](#)
 - [Paso 1: Comparar la configuración DNS entre entornos](#)
 - [Paso 2: Probar configuración alternativa de servidor DNS](#)
 - [Paso 3: Validar resolución DNS y conectividad](#)
 - [Causa](#)
 - [Contenido relacionado](#)
-

Problema

Un recurso privado configurado para el acceso a red de confianza cero (ZTNA) funciona correctamente cuando se utiliza un conector de recursos en el entorno de desarrollo. Sin embargo, cuando se cambia la configuración de recursos privados para utilizar el conector de recursos en el entorno de producción, el acceso al recurso privado o la conexión no se realiza correctamente y se producen errores relacionados con DNS. La conexión cumple la regla de bloqueo predeterminada, lo que impide la validación correcta del nuevo conector de recursos de producción antes de enrutar los recursos privados de producción a través de él.

Los síntomas específicos incluyen:

- Errores de falla de DNS registrados para el conector de recursos de producción
- Fallos de conexión debido a la aplicación de la regla de bloqueo predeterminada en el informe de búsqueda de actividades
- Incapacidad para validar la funcionalidad del conector de recursos de producción
- Impacto potencial en el acceso a recursos privados a través de ZTNA CLAP mediante Resource Connector

Se ha verificado la conectividad de red, incluida la resolución correcta de DNS del nombre de host del servidor web privado directamente desde el conector de recursos y la conectividad TCP al puerto 8443 en el servidor Ubuntu. Todo bien, pero aún así tenemos alerta de falla de DNS en el conector de recursos de producción ¿POR QUÉ?

Entorno

- Tecnología: Asistencia para soluciones (SSPT, contrato necesario)
- Subtecnología: Acceso seguro: acceso sin confianza (ZTNA, estado, basado en el cliente, inscripción, recurso privado)
- Familia de productos: Secure Access, Zero Trust/ZTNA, conector de recursos
- Aplicación/servidor privado de destino: Servidor Ubuntu accesible en el puerto TCP 8443
- Componentes de red: Conectores de recursos en entornos DEV y PROD

Resolución

El enfoque de solución de problemas se centra en las diferencias de configuración DNS entre los conectores de recursos de desarrollo y producción. Tenga en cuenta que el conector de recursos de desarrollo funciona correctamente: se puede acceder correctamente a los recursos privados. El conector de recursos de producción no funciona, el PR no está accesible y arroja un error de falla de DNS en RC > Conexiones de red > conector de recursos > Falla de DNS.

Siga estos pasos sistemáticos para identificar y resolver los problemas de resolución de DNS.

Paso 1: Comparar la configuración DNS entre entornos

Realice una comparación completa de la configuración DNS entre los conectores de recursos DEV y PROD:

- 1.- Documentar las configuraciones del servidor DNS en los conectores de recursos de desarrollo y producción.
- 2.- Identificar si el conector de desarrollo utiliza la configuración predeterminada de DNS o servidores DNS alternativos.
- 3.- Comparar la configuración de DNS del conector de producción con la configuración de desarrollo en funcionamiento.
- 4.- Anote cualquier diferencia en los métodos de resolución de DNS, tiempos de espera o configuraciones de reserva.

Paso 2: Probar configuración alternativa de servidor DNS

Si el conector de recursos de producción utiliza la configuración predeterminada de DNS y el conector de desarrollo utiliza servidores DNS alternativos, o viceversa:

- Configure el conector de recursos de producción para que utilice los mismos valores de configuración del servidor DNS que el conector de desarrollo en funcionamiento
- También puede especificar servidores DNS alternativos en la configuración del conector de recursos de producción
- Pruebe la conectividad de recursos privados después de cada cambio de configuración de DNS
- Supervise los registros del conector para ver si la resolución de DNS se ha realizado correctamente o si persisten los errores al utilizar el diagnóstico, tcpdump a la IP de destino de PR



Nota: Ambos conectores de recursos pueden resolver el nombre de dominio completo (FQDN) del RP cuando se utiliza el DNS predeterminado configurado en el RC, pero no

coincide con el DNS interno configurado en la configuración de recursos privados para el RC que no funciona o de producción.

Paso 3: Validar resolución DNS y conectividad

Debe actualizar el conector de recursos de producción para utilizar los servidores DNS internos para que coincidan con la configuración PR para resolver el problema. Haga clic en el ID del conector de recurso y haga clic en Editar para seleccionar Usar DNS alternativo. Puede explorar la sección Usar servidores DNS alternativos para resolver recursos privados según la configuración de dominio en la configuración del conector. Esto le permite especificar manualmente el dominio y el servidor DNS para probar si la conectividad mejora. Después de este cambio, puede acceder correctamente al recurso privado o al servidor de Ubuntu.

Después de implementar los cambios de configuración de DNS:

- 1.- Verificar que la resolución DNS funcione correctamente desde el conector de recursos de producción
- 2.- Confirmar que el recurso privado ya no llega a la regla de bloqueo por defecto
- 3.- Probar la conectividad de extremo a extremo a través del conector de producción

Causa

La causa raíz del problema estaba relacionada con las diferencias de configuración de DNS entre los conectores de recursos de desarrollo y producción. El entorno de producción utilizaba servidores DNS diferentes de forma predeterminada. Este fallo en la resolución de DNS hace que la conexión vuelva a las políticas de seguridad predeterminadas, lo que provoca que el tráfico se bloquee por la regla de bloqueo predeterminada en lugar de enrutarse correctamente a través del marco ZTNA. El Conector de recursos de desarrollo está configurado para utilizar los servidores DNS internos que coinciden con los DNS internos configurados en la configuración de recursos privados.

El conector de recursos de producción, sin embargo, está configurado para utilizar el DNS predeterminado, que difiere de los servidores DNS internos mencionados en la configuración de PR.

El conector de recursos de producción se actualizó para utilizar los servidores DNS internos de modo que coincidan con la configuración de PR para resolver el problema.

Contenido relacionado

- [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).