

Solução de problemas de acesso privado com ZTNA CLAP/BAP via conectores de recursos devido a falha de DNS

Contents

[Problema](#)

[Ambiente](#)

[Resolução](#)

[Passo 1: Comparar configuração DNS entre ambientes](#)

[Passo 2: Testar configuração de servidor DNS alternativo](#)

[Passo 3: Validar a resolução e a conectividade DNS](#)

[Causa](#)

[Conteúdo relacionado](#)

- [Problema](#)
 - [Ambiente](#)
 - [Resolução](#)
 - [Passo 1: Comparar configuração DNS entre ambientes](#)
 - [Passo 2: Testar configuração de servidor DNS alternativo](#)
 - [Passo 3: Validar a resolução e a conectividade DNS](#)
 - [Causa](#)
 - [Conteúdo relacionado](#)
-

Problema

Um recurso privado configurado para ZTNA (Zero Trust Network Access) funciona corretamente ao usar o conector de recurso no ambiente de desenvolvimento. No entanto, quando a configuração do recurso privado é alterada para usar o conector de recurso no ambiente de produção, o acesso ao recurso privado ou à conexão falha com erros relacionados ao DNS. A conexão atinge a regra de bloqueio padrão, impedindo a validação bem-sucedida do novo conector de recurso de produção antes de rotear recursos privados de produção por meio dele.

Os sintomas específicos incluem:

- Erros de falha de DNS registrados para o conector de recurso de produção

- Falhas de conexão devido ao cumprimento da regra de bloqueio padrão no relatório de pesquisa de atividades
- Incapacidade de validar a funcionalidade do conector de recurso de produção
- Impacto potencial para acessar o recurso privado via ZTNA CLAP usando o conector de recursos

A conectividade de rede foi verificada, incluindo a resolução DNS bem-sucedida do nome de host do servidor Web privado diretamente da produção do conector de recursos e a conectividade TCP para a porta 8443 no servidor Ubuntu. Tudo bem, mas ainda recebemos alerta de falha de DNS no conector de recursos de produção POR QUÊ?

Ambiente

- Tecnologia: Suporte à solução (SSPT - contrato necessário)
- Subtecnologia: Acesso seguro - acesso sem confiança (ZTNA, postura, baseado em cliente, inscrição, recurso privado)
- Linha de produtos: Acesso seguro, Zero Trust/ZTNA, conector de recursos
- Aplicativo/servidor privado de destino: Servidor Ubuntu acessível na porta TCP 8443
- Componentes de rede: Conectores de recursos nos ambientes DEV e PROD

Resolução

A abordagem de solução de problemas concentra-se nas diferenças de configuração de DNS entre os conectores de recursos de desenvolvimento e produção. Observe que o conector de recurso de desenvolvimento está funcionando no cenário - Capaz de acessar o recurso privado com êxito.

O conector de recurso de produção não está funcionando, a PR não está acessível e lançando o erro de falha de DNS em RC > Conexões de rede > conector de recurso > Falha de DNS.

Siga estas etapas sistemáticas para identificar e resolver os problemas de resolução de DNS.

Passo 1: Comparar configuração DNS entre ambientes

Faça uma comparação abrangente das configurações DNS entre os conectores de recursos DEV e PROD:

- 1.- Documente as configurações do servidor DNS nos conectores dos recursos de desenvolvimento e produção.
- 2.- Identifique se o conector de desenvolvimento usa configurações DNS padrão ou servidores DNS alternativos.
- 3.- Compare a configuração DNS do conector de produção com a configuração de desenvolvimento em funcionamento.
- 4.- Observe quaisquer diferenças nos métodos de resolução DNS, tempos limite ou configurações de fallback.

Passo 2: Testar configuração de servidor DNS alternativo

Se o conector de recursos de produção estiver usando configurações DNS padrão e o conector de desenvolvimento usar servidores DNS alternativos, ou vice-versa:

- Configurar o conector de recursos de produção para usar as mesmas configurações de servidor DNS que o conector de desenvolvimento em funcionamento
- Como alternativa, especifique servidores DNS alternativos na configuração do conector de recurso de produção
- Testar a conectividade do recurso privado após cada alteração de configuração de DNS
- Monitore os logs do conector para obter êxito na resolução DNS ou erros contínuos ao usar diagnósticos, tcpdump para o IP de destino PR



Note: Ambos os conectores de recursos podem resolver o nome de domínio totalmente qualificado (FQDN) do PR quando você usa o DNS padrão configurado no RC, mas ele não corresponde ao DNS interno configurado na configuração de recurso privado para o RC de produção ou não funcional.

Passo 3: Validar a resolução e a conectividade DNS

Você deve atualizar o Conector de Recursos de Produção para usar os servidores DNS internos para corresponder à configuração do PR a fim de resolver o problema. Clique no ID do conector de recurso e clique em Edit para selecionar Use Alternate DNS. Você pode explorar a opção Usar servidores DNS alternativos para resolver recursos privados com base na configuração de domínio na configuração do conector. Isso permite especificar manualmente o domínio e o servidor DNS para testar se a conectividade melhora. Após essa alteração, você pode acessar com êxito o recurso privado ou o servidor Ubuntu.

Depois de implementar as alterações de configuração do DNS:

- 1.- Verifique se a resolução DNS funciona corretamente a partir do conector de recursos de produção
- 2.- Confirme se o recurso privado não atinge mais a regra de bloqueio padrão
- 3.- Teste a conectividade fim-a-fim através do conector de produção

Causa

A causa raiz do problema está relacionada às diferenças de configuração de DNS entre os conectores de recursos de desenvolvimento e produção. O ambiente de produção estava usando diferentes servidores DNS por padrão. Essa falha de resolução de DNS faz com que a conexão volte para as políticas de segurança padrão, fazendo com que o tráfego seja bloqueado pela regra de bloqueio padrão em vez de ser roteado corretamente através da estrutura ZTNA. O Conector de Recursos de Desenvolvimento é configurado para usar os servidores DNS internos que correspondem ao DNS interno configurado na configuração de recursos privados.

O Conector de Recursos de Produção, no entanto, é configurado para usar o DNS padrão, que difere dos servidores DNS internos mencionados na configuração do PR.

O Conector de Recursos de Produção foi atualizado para usar os servidores DNS internos para corresponder à configuração de RP para resolver o problema.

Conteúdo relacionado

- [Suporte técnico e downloads da Cisco](#)

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês ([link fornecido](#)) seja sempre consultado.