

Solucione problemas de falhas APP_UNREACHABLE para aplicativos privados em acesso seguro

Contents

Problema

Ao tentar acessar aplicativos Zero Trust Network Access (ZTNA) por meio do Cisco Secure Access, os usuários encontram uma mensagem de erro "Aplicativo inalcançável".

- O Conector mostra íntegro/ativo no painel e a execução do aplicativo foi confirmada pelo proprietário.
- A falha pode afetar todos os usuários de um aplicativo, enquanto outros aplicativos atendidos pelo mesmo Conector funcionam normalmente.
- Em implantações de pool de conectores, as falhas podem parecer intermitentes — as sessões são bem-sucedidas ou falham, dependendo de qual conector no pool está selecionado.

Ambiente

- Implantação do Cisco Secure Private Access com ZTNA
- Recursos privados configurados para acesso ZTNA
- Implantação do conector de recursos para acesso a recursos privados

Resolução

Etapa 1. Testar o alcance direto a partir do segmento de rede de conectores

- O conector de recursos é um dispositivo bloqueado e não fornece acesso ao shell para executar comandos como curl ou nc diretamente. Em vez disso, execute o teste de acessibilidade de um host de teste (ou de uma VM temporária) colocado na mesma sub-rede/VLAN que o Conector, para que ele obedeça às mesmas regras de caminho de rede, roteamento e firewall para o aplicativo:

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

- Se isso falhar, o problema será confirmado no caminho da rede ou no servidor de aplicativos — corrija-o primeiro antes de revisar qualquer configuração de Acesso Seguro.



Note: Um teste de uma sub-rede diferente não é conclusivo — as regras de firewall e o roteamento são avaliados por origem, pois a origem do teste deve espelhar o posicionamento IP do Conector o mais próximo possível.

Etapa 2. Verificar a Configuração de Recurso Privado

- No painel de controle do Secure Access, navegue para Resources > Private Resources, abra o recurso privado afetado e compare o caractere IP, o FQDN e a porta de cada caractere configurados com o endereço e a porta de ligação reais do aplicativo em execução.
- Qualquer incompatibilidade (IP obsoleto após uma migração de servidor, porta incorreta, HTTP vs HTTPS) produz APP_UNREACHABLE mesmo com um caminho de rede perfeitamente íntegro.

Etapa 3. Validar a Resolução DNS para o Conector

- Se o recurso privado for definido pelo FQDN, verifique se os servidores DNS atribuídos ao Conector podem resolvê-lo. Na CLI do conector de recursos (as implantações de VM fornecem uma CLI de diagnóstico com comandos de solução de problemas Linux padrão

suportados), execute:

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

- Confirme se o IP privado correto foi retornado. Verificar os pontos de configuração de rede do Conector nos servidores DNS internos que podem resolver FQDNs de aplicativos privados; um Conector configurado com resolvedores públicos não pode resolver zonas internas.

Etapa 4. Revisar o caminho do firewall

- Confirme se as regras de firewall (firewalls de rede e o firewall do host no servidor de aplicativos) permitem o tráfego do endereço IP do Conector para o IP do servidor de aplicativos na porta necessária.

Etapa 5. Capturar o tráfego com tcpdump no conector de recursos

- Execute uma captura de pacote no Conector de Recursos para observar as tentativas de conexão do último quilômetro em direção ao aplicativo. O utilitário tcpdump está disponível no Conector de Recursos — consulte o guia [Executar tcpdump em Conectores de Recursos](#).



Tip: Para tornar a captura determinística em uma implantação de grupo de conectores, mantenha temporariamente apenas um Conector de Recursos ativado no grupo para que todas as sessões do recurso passem por ele e execute a captura filtrada no servidor da aplicação e na porta.

-
- Por exemplo:

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

(onde x.x.x.x é o IP do servidor de aplicativos e 443 é a porta do aplicativo)

- Interprete os resultados: SYNs de saída sem SYN-ACK indicam uma queda de firewall ou o aplicativo não está escutando; um RST imediato indica que o host está acessível, mas nada está vinculado à porta; nenhum pacote em direção ao aplicativo indica que a sessão não está alcançando esse conector ou o DNS está resolvido para um endereço inesperado.
- Reative os conectores restantes no grupo depois que a captura for concluída.

Causa

- Firewall bloqueando tráfego de conector para aplicativo: Um firewall de rede ou baseado em host bloqueia a porta necessária entre o IP do host do Connector e o IP do servidor de aplicativos.
- Incompatibilidade de configuração de recurso privado no Secure Access: O IP, o FQDN ou a porta configurada na definição de recurso particular (Recursos > Recursos Particulares) não corresponde ao que o aplicativo realmente escuta (por exemplo, o aplicativo foi movido para um novo IP ou escuta no 8443 enquanto o 443 está configurado).
- Falha na resolução DNS do Conector: O recurso privado é definido pelo FQDN, mas os servidores DNS do Conector não estão resolvendo FQDNs de aplicativos privados.
- Servidor de aplicativos inoperante ou sem escuta: O servidor parece íntegro devido a outras medidas, mas não está vinculado à porta esperada ou o serviço falhou enquanto o host permaneceu ativo.
- Acessibilidade parcial em um pool de conectores: Um ou mais conectores no pool ficam em um segmento de rede que não pode acessar o aplicativo, portanto, somente as sessões atribuídas a esses conectores falham.

Conteúdo relacionado

- [Solucionar problemas e coletar informações básicas do Cisco Secure Access](#)
- [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.