

Recursos de Link Privado Inacessíveis via Dispositivo Virtual de Acesso Seguro no Azure Devido à Configuração de DNS Interno

Contents

Problema

Os recursos de Link Privado do Azure não são acessíveis a partir de espaços de trabalho e cargas de trabalho do Azure quando o tráfego é roteado por meio de um Cisco Secure Access Virtual Appliance (VA) implantado no Azure. Esse problema persiste apesar da configuração de exceções de direcionamento de tráfego para ignorar o Secure Access para domínios privados do Azure, habilitando o backoff de DNS e configurando o DNS privado no VA.

As tentativas de acessar os pontos de extremidade do Link Privado do Azure a partir das cargas de trabalho do Azure por trás do VA de Acesso Seguro resultam em falha na resolução e conectividade.

Ambiente

- Cisco Secure Access Virtual Appliance (VA) implantado no Azure
- Espaços de trabalho do Azure e cargas de trabalho hospedadas no Azure
- Link Privado do Azure habilitado para conectividade de recurso particular do Azure
- Exceções de direcionamento de tráfego configuradas para ignorar o Acesso Seguro para domínios privados do Azure
- Backoff de DNS habilitado dentro do Secure Access VA
- Zonas DNS privadas configuradas no acesso seguro VA
- Versão de software: ALL (o problema não depende da versão)

Resolução

A resolução envolveu a atualização da configuração DNS no Cisco Secure Access VA para incluir entradas do servidor DNS interno que são capazes de resolver domínios de Link Privado do Azure. Estas etapas detalham a solução de problemas e as ações corretivas executadas:

Diagnosticar Configuração de DNS Local em VA de Acesso Seguro

1. Para examinar a configuração DNS existente e confirmar se os servidores DNS internos estão definidos, use este comando no VA de acesso seguro:

```
config localdns show
```

1. Exemplo de saída (com o nome do dispositivo substituído):

```
device# config localdns show
No internal DNS servers configured.
Conditional forwarders present for Azure private domains.
```

Adicionar Entradas do Servidor DNS Interno ao VA de Acesso Seguro

1. Para habilitar a resolução adequada de domínios de Link Privado do Azure, adicione os endereços IP do servidor DNS interno apropriado usando este comando:

```
config localdns add <internal-DNS-server-IP>
```

1. Substitua <internal-DNS-server-IP> pelo endereço IP real do seu servidor DNS interno que pode resolver domínios de Link Privado do Azure.

Verificar a Resolução DNS para Domínios de Link Privado do Azure

1. Depois de atualizar a configuração DNS, verifique se os domínios de Link Privado do Azure podem ser resolvidos por meio do Secure Access VA. Use este comando para confirmar a configuração do servidor DNS:

```
config localdns show
```

1. Exemplo de saída (nome do dispositivo substituído):

```
device# config localdns show
Internal DNS servers configured:
- x.x.x.x
Conditional forwarders present for Azure private domains.
```

1. Nenhum comando CLI encontrado que mostre a alteração de `config localdns show` sem servidores DNS para um estado de funcionamento com resolução confirmada.

Validar Conectividade para Recursos de Link Privado do Azure

Quando o DNS estiver resolvendo corretamente, teste a conectividade das cargas de trabalho do Azure por trás do Secure Access VA para os pontos de extremidade do Azure Private Link pretendidos para garantir o acesso apropriado.

Causa

A causa raiz do problema foi a ausência de configurações de servidor DNS interno no Cisco Secure Access VA. O VA foi configurado com encaminhadores condicionais para domínios privados do Azure, mas faltavam servidores DNS internos necessários para a resolução DNS adequada de domínios de Link Privado do Azure. Adicionar as entradas internas do servidor DNS resolveu 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.