

Recursos de link privado inaccesibles a través de Secure Access Virtual Appliance en Azure debido a la configuración de DNS interno

Contenido

Problema

No se puede tener acceso a los recursos de Azure Private Link desde los espacios de trabajo y las cargas de trabajo de Azure cuando el tráfico se enruta a través de un dispositivo virtual de Cisco Secure Access (VA) implementado en Azure. Este problema persiste a pesar de configurar excepciones de direccionamiento del tráfico para omitir Secure Access para dominios privados de Azure, habilitar la desconexión de DNS y configurar DNS privado en el VA.

Los intentos de acceder a los terminales de Azure Private Link desde las cargas de trabajo de Azure detrás del VA de Secure Access dan como resultado una resolución y conectividad erróneas.

Entorno

- Dispositivo virtual Cisco Secure Access (VA) implementado en Azure
- Espacios de trabajo de Azure y cargas de trabajo alojadas en Azure
- Azure Private Link habilitado para la conectividad de recursos privados de Azure
- Excepciones de direccionamiento de tráfico configuradas para omitir Secure Access para dominios privados de Azure
- Respaldo de DNS activado en el dispositivo virtual de acceso seguro
- Zonas DNS privadas configuradas en el dispositivo virtual de acceso seguro
- Versión del software: ALL (el problema es independiente de la versión)

Resolución

La resolución implicaba la actualización de la configuración de DNS en el dispositivo virtual de Cisco Secure Access para incluir entradas de servidor DNS interno que puedan resolver dominios de Azure Private Link. Estos pasos detallan la solución de problemas y las acciones correctivas realizadas:

Diagnosticar configuración de DNS local en el dispositivo virtual de acceso seguro

1. Para examinar la configuración DNS existente y confirmar si los servidores DNS internos están configurados, utilice este comando en el dispositivo virtual de acceso seguro:

```
config localdns show
```

1. Ejemplo de salida (con el nombre del dispositivo sustituido):

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

Agregar entradas internas del servidor DNS al dispositivo virtual de acceso seguro

1. Para habilitar la resolución adecuada de los dominios de Azure Private Link, agregue las direcciones IP de servidor DNS interno correspondientes mediante este comando:

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

1. Reemplace <internal-DNS-server-IP> por la dirección IP real de su servidor DNS interno que puede resolver los dominios de Azure Private Link.

Comprobar la resolución DNS para los dominios de vínculo privado de Azure

1. Después de actualizar la configuración de DNS, compruebe que los dominios de Azure Private Link se pueden resolver a través del VA de acceso seguro. Utilice este comando para confirmar la configuración del servidor DNS:

```
config localdns show
```

1. Ejemplo de salida (nombre de dispositivo sustituido):

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

1. No se encontró ningún comando CLI que muestre el cambio de `config localdns show` with no DNS servers a un estado de funcionamiento con resolución confirmada.

Validar la conectividad a los recursos de Azure Private Link

Una vez que DNS se resuelva correctamente, pruebe la conectividad de las cargas de trabajo de Azure detrás del dispositivo virtual de acceso seguro a los terminales de Azure Private Link para garantizar un acceso adecuado.

Causa

La causa raíz del problema fue la ausencia de configuraciones de servidor DNS interno en el dispositivo virtual de Cisco Secure Access. El dispositivo virtual se configuró con reenviadores condicionales para los dominios privados de Azure, pero no tenía los servidores DNS internos necesarios para la resolución DNS adecuada de los dominios de Azure Private Link. La adición de las entradas internas del servidor DNS resolvió 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).