對Google Cloud Docker上的安全訪問資源聯結器部署和連線進行故障排除

目錄

問題

嘗試在Docker上部署安全訪問資源聯結器失敗。

雖然聯結器安裝正確，但無法建立與Cisco Secure Access的連線。

診斷檢查報告隧道斷開和伺服器通訊錯誤。

該環境使用託管在Google雲中的Red Hat 9虛擬機器，通過Fortinet防火牆連線，並具有「any」規則。

故障排除發現網路介面之間可能存在的MTU不匹配是促成因素。

環境

- 技術：解決方案支援（SSPT — 需要合約）
- 子技術：安全訪問 — 資源聯結器（安裝、升級、註冊、連線、專用資源）
- 平台：Google Cloud上的Red Hat 9虛擬機器
- 網路：安全訪問和虛擬機器之間的Fortinet防火牆（已建立「任意」規則）
- 聯結器區域： iuvz83r.mxc1.acgw.sse.cisco.com
- Google雲VPC預設MTU:1460位元組
- Docker bridge(docker0)預設MTU: 1500位元組（更改前）
- 每個VM的單個網路介面(eth0)

解析

按照以下步驟診斷並解決Docker/Google雲環境中的安全訪問資源聯結器連線問題：

檢查聯結器區域的DNS解析

使用`nslookup`確認可以從VM解析安全訪問區域。

```
nslookup iuvz83r.mxc1.acgw.sse.cisco.com
```

輸出示例：

```
Server:         64.102.6.247
Address:        64.102.6.247#53
Non-authoritative answer:
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.72
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.70
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.66
Name:   iuvz83r.mxc1.acgw.sse.cisco.com
Address: 163.129.128.68
```

檢查網路連線和安全訪問

使用ping和telnet驗證從VM到Secure Access的連線。

```
ping iuvz83r.mxc1.acgw.sse.cisco.com
```

輸出示例：

```
PING iuvz83r.mxc1.acgw.sse.cisco.com (163.129.128.66) 56(84) bytes of data.
64 bytes from 163.129.128.66: icmp_seq=1 ttl=57 time=44.7 ms
64 bytes from 163.129.128.66: icmp_seq=2 ttl=57 time=43.8 ms
...
telnet iuvz83r.mxc1.acgw.sse.cisco.com 443
```

輸出示例：

```
Trying 163.129.128.66...
Connected to iuvz83r.mxc1.acgw.sse.cisco.com.
Escape character is '^]'.
```

檢查通道連線並運行診斷程式

運行聯結器診斷實用程式以檢查隧道狀態。

```
/opt/connector/data/bin/diagnostic
```

輸出示例：

```
###check tunnel connection:
error: tunnel is not connected
```

驗證網路介面和MTU設定

使用ifconfig和ip a檢查所有介面的IP地址和MTU。

```
ifconfig
ip a
```

eth0和docker0的輸出示例：

```
[root@degcpprcra02 ~]# ifconfig
docker0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1500
inet x.x.x.x netmask x.x.x.x broadcast x.x.x.x
inet6 fe80::1c66:46ff:fe1d:8bed prefixlen 64 scopeid 0x20<link>
ether 1e:66:46:1d:8b:ed txqueuelen 0 (Ethernet)
RX packets 974 bytes 119775 (116.9 KiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 848 bytes 161554 (157.7 KiB)
TX errors 0 dropped 2 overruns 0 carrier 0 collisions 0
eth0: flags=4163<UP,BROADCAST,RUNNING,MULTICAST> mtu 1460
inet x.x.x.x netmask x.x.x.x broadcast 0.0.0.0
ether 42:01:c0:a8:80:b0 txqueuelen 1000 (Ethernet)
RX packets 20175 bytes 7755728 (7.3 MiB)
RX errors 0 dropped 0 overruns 0 frame 0
TX packets 21550 bytes 31402300 (29.9 MiB)
TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0
```

檢查是否已擷取TCP流量

使用tcpdump捕獲VM和安全訪問區域之間的流量。

```
tcpdump -i eth0 host iuvz83r.mxc1.acgw.sse.cisco.com
```

輸出示例（顯示未捕獲資料包）：

```
listening on eth0, link-type EN10MB (Ethernet), snapshot length 262144 bytes
```

```
^C
0 packets captured
6 packets received by filter
0 packets dropped by kernel
```

銷毀並重新安裝聯結器（如有必要）

如果診斷程式和技術支援不工作，請停止並銷毀聯結器：

```
/opt/connector/install/connector.sh stop --destroy
cd /opt
rm -rf connector
```

重新安裝聯結器並生成技術支援輸出

重新安裝後，生成技術支援以捕獲錯誤日誌：

```
/opt/connector/data/bin/techsupport > techsupport.txt
Sample output showing connection errors:
2026-02-13 23:48:20.398772500  >> warning: Connection attempt has failed.
2026-02-13 23:48:20.398775500  >> warning: Unable to contact iuvz83r.mxc1.acgw.sse.cisco.com.
2026-02-13 23:48:20.398775500  >> error: Connection attempt has failed due to server communication erro
2026-02-13 23:48:20.398887500  >> state: Disconnected
```

調整Docker MTU以匹配Google雲VPC和VM介面

更改Docker網橋介面上的MTU以匹配Google Cloud VPC預設值（1460位元組）：

```
ip link set dev docker0 mtu 1460
```

驗證MTU更改：

```
ip a
```

輸出示例：

```
docker0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1460 qdisc noqueue state UP group default
```

```
link/ether 1e:66:46:1d:8b:ed brd ff:ff:ff:ff:ff:ff
inet x.x.x.x brd x.x.x.x scope global docker0
    valid_lft forever preferred_lft forever
inet6 fe80::1c66:46ff:fe1d:8bed/64 scope link
    valid_lft forever preferred_lft forever
```

在/etc/docker/daemon.json中保留Docker MTU更改

編輯`/etc/docker/daemon.json`並新增或更新`mtu`值：

```
{
  ...
  "mtu": 1460
}
```

重新啟動虛擬機器以應用MTU配置

重新啟動完整的VM以確保MTU設定已完全應用。這是必要的，因為可能只有重新啟動Docker服務不會對所有網路元件強制實施MTU更改。

執行以下步驟後，已成功建立與Secure Access的連線，並且可以完成配置。

原因

根本原因是Docker網橋介面(docker0)和Google雲VPC/VM網路介面(eth0)之間的MTU不匹配。Google雲VPC和VM介面的預設MTU為1460位元組，而Docker的預設MTU為1500位元組。

這種不匹配導致分段或丟棄資料包，阻止安全訪問資源聯結器建立隧道。對MTU值進行調整解決了連線問題。

相關內容

- https://securitydocs.cisco.com/docs/csa/olh/120695.dita
- https://securitydocs.cisco.com/docs/csa/olh/120776.dita
- https://securitydocs.cisco.com/docs/csa/olh/120727.dita
- https://securitydocs.cisco.com/docs/csa/olh/120772.dita
- https://securitydocs.cisco.com/docs/csa/olh/120762.dita
- https://securitydocs.cisco.com/docs/csa/olh/120685.dita
- 思科技術支援與下載

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。