Call failed with 54 (Connection reset by peer)

- Parallels Device Management

Symptoms

PMM agent can't download policies from MP or connect to IBCM Proxy.

`pma_agent.log` contains records like this:

```
12-12 19:33:27.835 D RpcLocator /CmProxyCommUtils:152:307/ Calling CM Proxy
at https://example.com
/ParallelsMacManagement/.rpc
12-12 19:33:27.882 D /RpcClientCpp:152:2103/ Connecting to example.com'
(1.2.3.4)...
12-12 19:33:27.952 D /RpcClientCpp:152:260b/ Successfully connected to
'1.2.3.4'
12-12 19:33:28.055 W RpcLocator /CmProxyCommUtils:152:1e03/ Call failed with
54 (Connection reset by peer)
```

curl executed against IBCM Proxy URL with keys **`--http1.1 --tlsv1.1`** fails:

```
C:\Users\kpavlov>curl -k -v https://example.com/ParallelsMacManagement/.rpc
--http1.1 --tlsv1.1
*   Trying 1.2.3.4...
* TCP_NODELAY set
* Connected to example.com (1.2.3.4) port 443 (#0)
* schannel: SSL/TLS connection with example.com port 443 (step 1/3)
* schannel: disabled server certificate revocation checks
* schannel: verifyhost setting prevents Schannel from comparing the supplied
target name with the subject names in server certificates.
* schannel: sending initial handshake data: sending 121 bytes...
* schannel: sent initial handshake data: sent 121 bytes
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: failed to receive handshake, need more data
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: failed to receive handshake, SSL/TLS connection failed
* Closing connection 0
* schannel: shutting down SSL/TLS connection with example.com port 443
* Send failure: Connection was reset
* schannel: failed to send close msg: Failed sending data to the peer (bytes
written: -1)
* schannel: clear security context handle
curl: (35) schannel: failed to receive handshake, SSL/TLS connection failed
```

With key **`--tlsv1.2`** it connects successfully:

```
C:\Users\kpavlov>curl -k -v https://example.com/ParallelsMacManagement/.rpc
--http1.1 --tlsv1.2
*   Trying 1.2.3.4...
* TCP_NODELAY set
* Connected to example.com (1.2.3.4) port 443 (#0)
* schannel: SSL/TLS connection with example.com port 443 (step 1/3)
* schannel: disabled server certificate revocation checks
```

```
* schannel: verifyhost setting prevents Schannel from comparing the supplied
target name with the subject names in server certificates.
* schannel: sending initial handshake data: sending 173 bytes...
* schannel: sent initial handshake data: sent 173 bytes
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: failed to receive handshake, need more data
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: encrypted data got 4047
* schannel: encrypted data buffer: offset 4047 length 4096
* schannel: sending next handshake data: sending 214 bytes...
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: encrypted data got 107
* schannel: encrypted data buffer: offset 107 length 4096
* schannel: SSL/TLS handshake complete
* schannel: SSL/TLS connection with example.com port 443 (step 3/3)
* schannel: stored credential handle in session cache
> GET /ParallelsMacManagement/.rpc HTTP/1.1
> Host: example.com
> User-Agent: curl/7.55.1
> Accept: */*
>
* schannel: client wants to read 102400 bytes
* schannel: encdata_buffer resized 103424
* schannel: encrypted data buffer: offset 0 length 103424
* schannel: encrypted data got 85
* schannel: encrypted data buffer: offset 85 length 103424
* schannel: decrypted data length: 0
* schannel: decrypted data added: 0
* schannel: decrypted data cached: offset 0 length 102400
* schannel: remote party requests renegotiation
* schannel: renegotiating SSL/TLS connection
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: encrypted data buffer: offset 0 length 103424
* schannel: sending next handshake data: sending 261 bytes...
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: encrypted data got 4181
* schannel: encrypted data buffer: offset 4181 length 103424
* schannel: sending next handshake data: sending 1647 bytes...
* schannel: SSL/TLS connection with example.com port 443 (step 2/3)
* schannel: encrypted data got 367
* schannel: encrypted data buffer: offset 367 length 103424
* schannel: encrypted data length: 181
* schannel: SSL/TLS handshake complete
* schannel: SSL/TLS connection with example.com port 443 (step 3/3)
* schannel: SSL/TLS connection renegotiated
* schannel: decrypted data length: 110
* schannel: decrypted data added: 110
* schannel: decrypted data cached: offset 110 length 102400
* schannel: encrypted data buffer: offset 0 length 103424
* schannel: decrypted data buffer: offset 110 length 102400
* schannel: schannel_recv cleanup
* schannel: decrypted data returned 110
* schannel: decrypted data buffer: offset 0 length 102400
< HTTP/1.1 403 Forbidden
< Server: Microsoft-IIS/10.0
< Date: Fri, 13 Dec 2019 16:59:09 GMT
< Content-Length: 0
<
```

```
* Connection #0 to host example.com left intact
```

Cause

The SCCM Management Point is configured to accept only TLS1.2 connections.

Resolution

Upgrade PMM server components and Mac agents to version 7.3.2.7 or newer.

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.