

Troubleshooting

- [F5 APM: Convert attribute values](#)
- [VPN Client Troubleshooting](#)
- [F5 Big-IP Advanced Troubleshooting](#)
- [Send Logfiles to F5 Support and compress them](#)

F5 APM: Convert attribute values

Status

The problem with APM LDAP auth is that LDAP-attributes with values of ASCII chars can be used in further scripts without problems.

If you have some UTF8 characters in the value the F5 APM will convert the string to a HEX-string:

Aus dem F5 Manual: https://support.f5.com/kb/en-us/products/big-ip_apm/manuals/product/apm-authentication-single-sign-on-11-5-0/5.html

About how APM handles binary values in LDAP attributes

For LDAP, Access Policy Manager (APM) converts an attribute value to hex only if the value contains unprintable characters.

If the session variable contains several values, and one or more of those values is unprintable, then APM converts only those particular values to hex.

Case 1:

Handling of attributes with single value:

```
9302eb80.session.ldap.last.attr.objectGUID 34 / 0xfef232d3039be9409a72bfc60bf2a6d0
```

Case 2:

Handling of attributes with multiple values (mix of binary and non-binary values):

```
29302eb80.session.ldap.last.attr.memberOf 251 | / CN=printable group,OU=groups,OU=someco,DC=smith, \
/ DC=labt,DC=fp,DC=somelabnet,DC=com | /
0x434e3d756e7072696e7461626c6520c2bdc2a12067726f75702c4f553d67726f7570732c4f553d66352c \
/ 44433d73686572776f6642c44433d6c6162742c44433d66702c44433d66356e65742c44433d636f6d |
```

Possible solution

Devcentral: <https://devcentral.f5.com/questions/looking-for-irule-to-convert-non-ascii-character-to-ascii>

In 12.0.0

ID 399693:

“ It is now possible to use the -decode option for mcget command of a branch rule to decode a session variable before using it.

When you create an agent and add a branch rule, the default value of the rule contains an mcget command to fetch the session variable. By default, the session variable is HEX encoded if it contains non-ASCII characters.

You need to modify the command in advanced mode and insert the -decode option for mcget command, for example:

```
expr { [mcget -decode {session.ad.last.attr.memberOf}] contains "non-ASCII-
characters" }
```

VPN Client Troubleshooting

Problem

To troubleshoot for example an error message like "Machine Cert Auth Error - unable to get local issuer certificate" you need to get log from the VPN Client.

Client Troubleshooting Utility (CTU)

The *f5wininfo.exe* utility can be used on the client to do a very good troubleshooting.

You will get the utility from your F5 APM on URL:
<https://<fqdn or ip>/public/download/f5wininfo.exe>

With *f5wininfo.exe* you're able to export a diagnostic report of the client as a html file with all the very detail information you need.

Example Output

grafik.png
image not found or type unknown

Links

For more informations about the troubleshooting on the client check the following links:

- [K12444: Overview of the Client Troubleshooting Utility for Windows](#)
- [K00819308: Gathering F5 VPN client logs](#)
- [K32311645: BIG-IP Edge Client operations guide | Chapter 7: Troubleshooting](#)

F5 Big-IP Advanced Troubleshooting

I work with F5 since many years and I always need some advanced troubleshooting tools which I documented here a little bit.

CLI Commands

Show pool members monitoring status

```
tmsh show ltm pool all members field-fmt | grep -P "(ltm\ pool|active-member-cnt|addr|monitor-status)"
```

Count pool members with monitoring status "monitor-status checking"

```
tmsh show ltm pool all members field-fmt | grep "monitor-status\ checking" | wc -l
```

Show Health Monitor status

Example with ICMP health monitor:

```
tmsh show ltm monitor icmp icmp
```

Answer:

Destination: 1.7.3.55:0

State time: up for 527hrs:54mins:45sec

| Last error: N/A @2019.11.12 10:58:51

Destination: 1.7.3.56:0

State time: up for 527hrs:54mins:45sec

| Last error: N/A @2019.11.12 10:58:51

Destination: 1.7.3.131:0

State time: down for 527hrs:54mins:45sec

| Last error: No successful responses received before deadline. @2019.11.12 10:58:51

Destination: 1.7.3.139:0

State time: down for 527hrs:54mins:45sec

| Last error: No successful responses received before deadline. @2019.11.12 10:58:51

K53851362 - Displaying and deleting connection table entries from the command line

The BIG-IP connection table contains information about all the sessions that are currently established on BIG-IP system. You can display and delete the contents of the BIG-IP connection table from the command line using the tmsh connection command.

Important: On systems with a large number of connections, executing the following commands with a large output may result in excessive output causing device instability. It is recommended you limit the output to specific IP address and/or port combination as demonstrated in the examples below.

Display Connection Table Entries:

1. To display the BIG-IP connection table entries for a particular virtual server, use the following tmsh command syntax:

```
tmsh show /sys connection cs-server-addr <vs_ip> cs-server-port <vs_port>
```

For example, to display the BIG-IP connection table entries for 10.10.2.2:443 virtual server, you would type the following command:

```
tmsh show /sys connection cs-server-addr 10.10.2.2 cs-server-port 443
```

2. To display the BIG-IP connection table entries for a particular client IP address, use the following tmsh command syntax:

```
tmsh show /sys connection cs-client-addr <client_ip>
```

For example, to display the BIG-IP connection table entries for 10.10.20.2 client IP address, you would type the following command:

```
tmsh show /sys connection cs-client-addr 10.10.20.2
```

3. To display the BIG-IP connection table entries for a particular pool member, use the following tmsh command syntax:

```
tmsh show /sys connection ss-server-addr <pool_member_ip> ss-server-port <pool_member_port>
```

For example, to display the BIG-IP connection table entries for 192.168.10.2:80 pool member, you would type the following command:

```
tmsh show /sys connection ss-server-addr 192.168.10.2 ss-server-port 80
```

4. To display additional information about particular connection such as Idle timeout, number of packets sent etc, use the following tmsh command syntax:

```
tmsh show /sys connection cs-client-addr <client_ip> cs-client-port <client_port> cs-server-addr <vs_ip> cs-server-port <vs_port> all-properties
```

For example, to display specific details of connection established between 10.10.20.2:51435 (client) and 10.10.2.2:443 (virtual server), you would type the following command:

```
tmsh show /sys connection cs-client-addr 10.10.20.2 cs-client-port 51435 cs-server-addr 10.10.2.2 cs-server-port 443 all-properties
```

Delete the connection table entries:

1. To delete the BIG-IP connection table entries for a particular client IP and virtual server, use the following tmsh command syntax:

```
tmsh delete /sys connection cs-client-addr <client_ip> cs-server-addr <vs_ip> cs-server-port <vs_port>
```

For example, to delete the BIG-IP connection table entries for 10.10.20.2 client IP address and 10.10.2.2:443 virtual server, you would type the following command:

```
tmsh delete /sys connection cs-client-addr 10.10.20.2 cs-server-addr 10.10.2.2 cs-server-port 443
```

F5 Support Solution Link

[K53851362: Displaying and deleting BIG-IP connection table entries from the command line](#)

K7318: Overview of the bigtop utility

The **bigtop** tool is a command line utility that displays real-time statistical information for BIG-IP LTM system objects such as virtual servers and nodes. For example, the following items are displayed when using the **bigtop** utility:

- Current time
- Network activity in bits, bytes, packets, or requests
- Nodes available for virtual servers
- Current state of nodes

Example:

```
bigtop -n
```

		bits since			bits in prior			current
		Mar 23 21:59:50			4 seconds			time
BIG-IP	ACTIVE	---In---	Out---	Conn-	---In---	Out---	Conn-	12:01:37
		149.7G	2.694G	769374	6880	3584	4	
VIRTUAL ip:port		---In---	Out---	Conn-	---In---	Out---	Conn-	-Nodes Up--
/Common/192.168.20.106:443		1.431G	2.282G	261093	1856	1312	1	0
/Common/192.168.20.106:80		537.5M	410.8M	215520	5024	2272	3	0
/Common/192.168.20.107:443		1.120M	660720	105	0	0	0	0
/Common/192.168.20.107:80		7728	4888	1	0	0	0	0
NODE ip:port		---In---	Out---	Conn-	---In---	Out---	Conn-	--State----
/Common/node1:80		0	0	0	0	0	0	DOWN
/Common/node2:80		0	0	0	0	0	0	DOWN

F5 Support Solution Link

[K7318: Overview of the bigtop utility](#)

Send Logfiles to F5 Support and compress them

If you need to send all logfiles to F5 Support you need to compress them all.

You can do this like this as root user:

1. Log in to the command line.
2. Create a **tar** archive in the **/var/tmp** directory that contains all the files in the **/var/log** directory, by typing the following command:

```
tar zcvf /var/tmp/$HOSTNAME-logs.tar.gz /var/log/*
```
3. This will generate a file in /var/tmp with the name of the device followed by the -logs.tar.gz suffix. You need to transfer this file out of the system using an utility like scp/WinSCP