Issues

ValueError: q must be exactly 160, 224, or 256 bits long

Exception raised on client:

```
ssh: Unknown exception: q must be exactly 160, 224, or 256 bits long
ssh: Traceback (most recent call last):
ssh:   File "/usr/lib/python3/dist-packages/paramiko/transport.py", line
2109, in run
ssh:     handler(self.auth_handler, m)
ssh:   File "/usr/lib/python3/dist-packages/paramiko/auth_handler.py", line
298, in _parse_service_accept
ssh:     sig = self.private_key.sign_ssh_data(blob)
ssh:   File "/usr/lib/python3/dist-packages/paramiko/dsskey.py", line 108,
in sign_ssh_data
ssh:     key = dsa.DSAPrivateNumbers(
ssh:   File "/usr/lib/python3/dist-
packages/cryptography/hazmat/primitives/asymmetric/dsa.py", line 250, in
private_key
ssh:     return backend.load_dsa_private_numbers(self)
ssh:   File "/usr/lib/python3/dist-
packages/cryptography/hazmat/backends/openssl/backend.py", line 853, in
load_dsa_private_numbers
ssh:     dsa._check_dsa_private_numbers(numbers)
ssh:   File "/usr/lib/python3/dist-
packages/cryptography/hazmat/primitives/asymmetric/dsa.py", line 147, in
_check_dsa_private_numbers
ssh:     _check_dsa_parameters(parameters)
ssh:   File "/usr/lib/python3/dist-
packages/cryptography/hazmat/primitives/asymmetric/dsa.py", line 139, in
_check_dsa_parameters
ssh:     raise ValueError("q must be exactly 160, 224, or 256 bits long")
ssh: ValueError: q must be exactly 160, 224, or 256 bits long
ssh:
BackendException: ssh connection to niziak-backup@192.168.179.90:22 failed:
q must be exactly 160, 224, or 256 bits long
```

Client is Debian 11 (paramiko version 2.7.2) Remote side was upgraded to Debian 12 (paramiko version 2.12.0)

Upgrading paramiko on client helps:

```
python3 -m pip install -U paramiko
```

Invalid packet blocking

```
ssh: Exception: Invalid packet blocking
ssh: Traceback (most recent call last):
ssh:   File "/usr/lib/python3/dist-packages/paramiko/transport.py", line 2055, in run
ssh:     ptype, m = self.packetizer.read_message()
ssh:                ^^^^^^^^^^^^^^^^^^^^^^^^^^^^^^
ssh:   File "/usr/lib/python3/dist-packages/paramiko/packet.py", line 493, in read_message
ssh:     raise SSHException("Invalid packet blocking")
ssh: paramiko.ssh_exception.SSHException: Invalid packet blocking
ssh:
Attempt of put Nr. 1 failed. EOFError:
Attempt of put Nr. 2 failed. OSError: Socket is closed
Attempt of put Nr. 3 failed. OSError: Socket is closed
Attempt of put Nr. 4 failed. OSError: Socket is closed
Giving up after 5 attempts. OSError: Socket is closed
Attempt of put Nr. 1 failed. OSError: Socket is closed
Attempt of put Nr. 2 failed. OSError: Socket is closed
```

Not known reason or solution. SSH connection on remote side gently disconnects.

Workaround: Bump duplicity version on client side (from 0.8.22 to 1.2.2)

failed: not a valid RSA private key file

```
--- Start running command BKP at 02:17:02.067 ---
BackendException: ssh connection to mybackup@192.168.64.251:22 failed: not a valid RSA private key file
02:17:02.740 Task 'BKP' failed with exit code '23'.
--- Finished state FAILED 'code 23' at 02:17:02.740 - Runtime 00:00:00.673 ---
```

Reason: paramiko doesn't accept OpenSSH key format Solution: `ssh-keygen -p -m PEM -f ~/.ssh/id_rsa`

From:
https://niziak.spox.org/wiki/ - **niziak.spox.org**

Permanent link:
https://niziak.spox.org/wiki/linux:backup:duply:issues

Last update: **2024/01/10 08:50**