Permission denied (publickey) with OpenSSH client #579

New issue

Closed **adilsond** opened this issue on Oct 21, 2016 · 16 comments

adilsond commented on Oct 21, 2016

Hello.

I have installed teleport at work because it is a very interesting and safe solution for acessing the servers. I have only one problem: Not everyone has access to the web interface or the tsh client. So I follow the instructions from the admin guide to access the server with the openssh client.

The cluster keys was exported and added to the ~/.ssh/known_hosts. Then I configured /etc/ssh/ssh_config to use the proxy, run the tsh agent on the server. But, when I try to access the proxy I got the following message.

adilsond@clienttest:~$ ssh adilson@teleporttest.some.proxy.net The authenticity of host '[some.proxy.net]:3023 ([10.200.12.184]:3023)' can't be established.
RSA key fingerprint is SHA256:kQxOib8/WbBGblybi6MTqv2qc7m+DgBoWYVBXAl1dEY.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[some.proxy.net]:3023,[10.200.12.184]:3023' (RSA) to the list of known hosts.
Permission denied (publickey).
ssh_exchange_identification: Connection closed by remote host

I only got this error without any log or message.

Is there anything wrong with the config? Both machines used for the test are Ubuntu 14.04 (teleport server) and Ubuntu 16.10 (openssh client). The teleport version is 1.2.0 build from the git sources.

kontsevoy commented on Oct 22, 2016 Contributor

@adilsond let us try to reproduce. will be back to you asap.

mebezac commented on Jan 12 • edited Contributor

@kontsevoy @adilsond having this exact same issue on teleport v1.3.2. I spun up two servers on AWS following exactly the instructions in the guides, one as the proxy/auth and one as a node to do some testing. I can use `tsh` perfectly fine or the web interface to login into the node.

I then followed https://github.com/gravitational/teleport/blob/master/docs/admin-guide.md#using-teleport-with-openssh on my local OSX machine and no matter what I try, all I get is:

```
OpenSSH_7.3p1, LibreSSL 2.4.1
debug1: Reading configuration data /Users/zac/.ssh/config
debug1: /Users/zac/.ssh/config line 14: Applying options for *
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 3: Applying options for *.cluster.dev
debug1: Executing proxy command: exec ssh -p 3023 ubuntu@cluster.dev -s proxy:node.cluster
debug1: identity file /Users/zac/.ssh/zac_clay type 1
debug1: key_load_public: No such file or directory
debug1: identity file /Users/zac/.ssh/zac_clay-cert type -1
```

Assignees

russjones

Labels

P1

Projects

None yet

Milestone

2.0

5 participants

```
debug1: identity file /Users/zac/.ssh/id_rsa type 1
debug1: key_load_public: No such file or directory
debug1: permanently_drop_suid: 501
debug1: identity file /Users/zac/.ssh/id_rsa-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.3
The authenticity of host '[cluster.dev]:3023 ([54.200.53.237]:3023)' can't be established.
RSA key fingerprint is SHA256:TlmHWylF8klShD17kdzsqb7ZcFUO9yiFa+eliVYq6mk.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '[cluster.dev]:3023,[54.200.53.237]:3023' (RSA) to the list of
debug1: Remote protocol version 2.0, remote software version OpenSSH_7.2p2 Ubuntu-4ubuntu2
debug1: match: OpenSSH_7.2p2 Ubuntu-4ubuntu2.1 pat OpenSSH* compat 0x04000000
debug1: Authenticating to node.cluster.dev:22 as 'ubuntu'
debug1: SSH2_MSG_KEXINIT sent
debug1: SSH2_MSG_KEXINIT received
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ecdsa-sha2-nistp256
debug1: kex: server->client cipher: chacha20-poly1305@openssh.com MAC: <implicit> compress
debug1: kex: client->server cipher: chacha20-poly1305@openssh.com MAC: <implicit> compress
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug1: Server host key: ecdsa-sha2-nistp256 SHA256:J1wp0Y1eoV6HTnIYTxIPLj/WBcZC+af+s61//B
The authenticity of host 'node.cluster.dev (<no hostip for proxy command>)' can't be estab
ECDSA key fingerprint is SHA256:J1wp0Y1eoV6HTnIYTxIPLj/WBcZC+af+s61//B8axs4.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added 'node.cluster.dev' (ECDSA) to the list of known hosts.
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug1: rekey after 134217728 blocks
debug1: SSH2_MSG_NEWKEYS received
debug1: SSH2_MSG_EXT_INFO received
debug1: kex_input_ext_info: server-sig-algs=<rsa-sha2-256,rsa-sha2-512>
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug1: Authentications that can continue: publickey
debug1: Next authentication method: publickey
debug1: Offering RSA-CERT public key:
debug1: Authentications that can continue: publickey
debug1: Offering RSA public key: /Users/zac/.ssh/zac_clay
debug1: Authentications that can continue: publickey
debug1: Offering RSA public key: /Users/zac/.ssh/id_rsa
debug1: Authentications that can continue: publickey
debug1: No more authentication methods to try.
Permission denied (publickey).
Killed by signal 1.
```

And the teleport proxy running in debug shows this:

```
INFO[0023] [SSH:proxy] new connection 174.102.71.236:57575 -> 172.31.3.255:3023 vesion: SSH
DEBU[0023] [SSH] ssh.dispatch(req=subsystem, wantReply=true)  component=proxy fields=map[l
DEBU[0023] parse_proxy_subsys(proxy:node.cluster.dev:22)  file=srv/proxy.go:59 func=srv.pa
DEBU[0023] [SSH] subsystem request: proxySubsys(site=, host=node.cluster.dev, port=22)  co
DEBU[0023] proxy_subsystem: execute(remote: 174.102.71.236:57575, local: 172.31.3.255:3023
DEBU[0023] proxy_subsystem: no site specified. connecting to default: 'fc57ac3e-d067-4945-
DEBU[0023] Dial(addr=node.cluster.dev:22)               component=reversetunnel fields=ma
INFO[0023] web.getEvents(event=session.start&event=session.end&from=2017-01-08T05%3A00%3A0
INFO[0023] auditLog.SearchEvents(2017-01-08 05:00:00 +0000 UTC, 2017-01-12 04:59:59 +0000
INFO[0023] auditLog.findInFile(/var/lib/teleport/log/2017-01-12.00:00:00.log, map[_:[14841
DEBU[0023] [SSH] proxySubsys(site=, host=node.cluster.dev, port=22) finished with result:
DEBU[0023] [SSH] client 174.102.71.236:57575 disconnected  component=proxy fields=map[loca
```

kontsevoy commented on Jan 18 Contributor

@mebezac @adilsond hey guys, sorry for the delay. **@russjones** you're playing with this, right?

russjones commented on Jan 21 Contributor

@kontsevoy I also ran into the same issues when setting up a Teleport cluster that plays well with OpenSSH. I think it's caused by some issues in OpenSSH and some issues in Teleport. Let me try and address them individually:

1. Host authentication behaves in a somewhat unexpected manner for OpenSSH users.

This happens for two reasons.

1. When you add a node to a cluster with Teleport, Teleport will randomly generate a UUID and then create a host certificate with the Principle (kind of like common name in x509 certificates) as UUID + cluster name. For example, if you set your cluster name to `example.com`, you end up with a Principle that looks like this: `1728eb98-8bc4-4816-83e0-27cd63d80ffe.example.com` on your certificate. That means when you use OpenSSH to connect to a server by DNS name, even if you have included your cluster CA in `~/.ssh/known_hosts`, the connection will fail due the Principle mismatch on the certificate. When this happens, you see messages like this from OpenSSH:

```
key_cert_check_authority: invalid certificate
Certificate invalid: name is not a listed principal
The authenticity of host '[1.2.3.4]:3023 ([1.2.3.4]:3023)' can't be established.
RSA key fingerprint is SHA256:abcdefghijklmnopqrstuvwxyzabcdefghijklmnopq.
Are you sure you want to continue connecting (yes/no)?
```

2. For the same reasons as above, you can't use an IP addresses to directly connect to a Teleport node, because the Principle will not match. The good news is that this behavior has changed, as recently OpenSSH has started letting you set `HostKeyAlias` to UUID + cluster name and still connect via the IP addresses, take a look at the following thread: https://lists.mindrot.org/pipermail/openssh-unix-dev/2015-February/033443.html However this doesn't solve the issue of backward compatibility with older version of OpenSSH.

Proposed Solution

A potential solution would look like the following:

1. Add the hostname + cluster name into the Principle field of the certificate along with the host ID + cluster name that already exists. This would solve the problem for users trying to connect via DNS name to a Teleport node using OpenSSH.

2. Update the documentation to reflect that you can't use IP addresses directly when connecting to Teleport nodes with older version of OpenSSH. Users wishing to connect to Teleport nodes via IP address have two options: upgrade the OpenSSH client they are using and set `HostKeyAlias` or update `/etc/hosts` on the client (and proxy!) so that the Principle match succeeds.

2. OpenSSH is unable to find the private key needed to connect to a Teleport node when using the `tsh agent teleagent.`

When this happens you see messages like this from OpenSSH:

```
debug2: input_userauth_pk_ok: fp SHA256:abcdefghijklmnopqrstuvwxyzabcdefghijklmnopq
debug3: sign_and_send_pubkey: RSA-CERT SHA256:abcdefghijklmnopqrstuvwxyzabcdefghijklmnopq
debug1: sign_and_send_pubkey: no private key for certificate ""
```

This is actually a bug in OpenSSH and not Teleport, take a look at the following issue on the OpenSSH bug tracker: https://bugzilla.mindrot.org/show_bug.cgi?id=2550 Essentially, when you add a certificate to an agent, you can't just embed the private key within the certificate, you have to add the certificate and private key to the agent separately.

The problem is that many operating systems ship a version of OpenSSH that has this bug in it, so it's probably appropriate to workaround this issue in Teleport.

Proposed Solution

Two options exist, the path to take is up to the maintainers of Teleport.

1. Update `teleagent` to load the certificate (with embedded private key) as well as the private key upon start. This will allow `teleagent` to be backward backward compatible with older clients that exhibit this bug as well as forward compatible with new clients.

2. Get rid of `teleagent` completely. It doesn't seem to have any custom Teleport logic in it (but

perhaps I am wrong?) so why not just have `tsh` load certificates into the `ssh-agent` that is already running on a system. It's less code to maintain and will not break anyones workflow.

3. Teleport stores certificates and keys in the same format as OpenSSH but with a different naming convention.

This prevents users from bypassing the agent and directly using the certificate and keys when connecting to a Teleport node when issues like the above arise. In addition, the current permissions (`640` I think) for the keys are too open for OpenSSH which prefers `400` if I recall correctly.

Proposed Solution

A potential solution would look like the following:

1. Change the naming scheme for keys in the `.tsh` directory like so:

```
name.cert -> id_rsa-cert.pub
name.key  -> id_rsa
name.pub  -> id_rsa.pub
```

This would allow you to then by-pass the agent and use the keys directly like so:

```
ssh -i  ~/.tsh/keys/proxy.example.com/id_rsa \
    -o ProxyCommand="ssh -p 3023 proxy.example.com -s proxy:%h:%p" \
    -p 3022 node.example.com
```

2. Change the permissions from `640` to `400` when writing them to disk.

russjones commented on Jan 21 Contributor

Correction to the third issue I raised: you don't need to change the names for the files, you just need to set `IdentityFile` and `CertificateFile` like this (this is probably better done in `~/.ssh/config` to be honest):

```
ssh -o 'IdentityFile ~/.tsh/keys/proxy.example.com/user.key' \
    -o 'CertificateFile ~/.tsh/keys/proxy.example.com/user.cert' \
    -o 'ProxyCommand ssh -o "IdentityFile ~/.tsh/keys/proxy.example.com/user.key" -o "Cert
    -p 3022 node.example.com
```

However, permissions do need to be set correctly. The directories leading to the key file need to have permissions set to `700` and the key itself should be `600` .

This was referenced on Jan 25

Improved CLI UX + a bunch of regressions fixed #728 Merged

Multiple Principals #730 Merged

noriuky commented on Feb 3

I have similar problem.
I installed teleport on my 3 vps online:
Server1 have teleport full with admin
S2 and S3 just host.
They saw each other i can log into webpage and use all servers from there but
if i try to access via ssh it dont work, even if i follow the guide:here.
I got a doubt following the guide. i can access to my 3 vps only via ip, no dns.
so i dont really figreout how to config it.
I just replaced Host *.work.example.com with the ip of teleport server, then with the other 2 ip but nothing change.
i always receive this error:

[root@teleport-4 ~]# tsh --proxy=x.x.x.x ssh root@y.y.y.y
x509: certificate is valid for ::1, 127.0.0.1, not x.x.x.x
any help?
btw via ssh x.x.x.x i can access but teleport dont record session.

kontsevoy commented on Feb 4 Contributor

@noriuky this will be fixed in 2.0 (coming out in Feb)

👍 1

kontsevoy added this to the **2.0** milestone on Feb 4

russjones was assigned by **kontsevoy** 28 days ago

kontsevoy commented 28 days ago Contributor

@russjones this is probably related to #611 (i.e. if this one is fixed, then #611 should work with just a documentation update. AFAIK `--cluster` switch doesn't even matter when tsh agent is running)

kontsevoy added the **P1** label 28 days ago

This was referenced 26 days ago

LocalKeyAgent changes for OpenSSH interoperability #762 Merged

Update OpenSSH Documentation #763 Merged

russjones commented 24 days ago Contributor

With #730, #762, and #762 merged these issues should be resolved (on master).

I followed the instructions in our documentation myself and was able to connect to Teleport nodes using OpenSSH with the Teleport agent as well as the system SSH agent.

👍 1

adilsond commented 24 days ago

I still got the same message after rebuilding teleport with the latest changes:

adilsond@fett:~/.ssh$ ssh adilson@target.prox01.someproxy.net -v
OpenSSH_7.3p1 Ubuntu-1, OpenSSL 1.0.2g 1 Mar 2016
debug1: Reading configuration data /home/adilsond/.ssh/config
debug1: /home/adilsond/.ssh/config line 10: Applying options for *.prox01.someproxy.net
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug1: Executing proxy command: exec ssh -p 3023 adilson@prox01.someproxy.net -s proxy:target.prox01.someproxy.net:3022
debug1: permanently_drop_suid: 1000
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_rsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_rsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_dsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_dsa-cert type -1

debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ed25519-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.3p1 Ubuntu-1
Permission denied (publickey).
ssh_exchange_identification: Connection closed by remote host

The certiricate used is like this:
@cert-authority *.someproxy.net ssh-rsa
AAAAB3NzaC1yc2EAAAADAQABAAABAQC/3VmQGQg2c4i830SoQI2s+2SjvUlfnO8rUVNGC6piK0O1y
rHL2o0L14uboREWV1zqoFAhSRM+28734wsoiuweu8237987swwywuy72wywuywiuT+UTi2AcSap76o
xIGh5a7WF7GMROs4lwKGw9bxJz9GXCjlkU/bsaP3WBqqjySdk1MCJv+hrq46NCLf9AwuHWSCXX0u
Ww1n3Y5Aw2UGRvLIR/E3CjbpUN7d5VGAzABkUhgEUnmtNwV8lUA4h0Su+p+X32n7OURFscd5nVzk
07A/CCguZuvR3q/Il5zI+XNUnr7u2wLOoDvxKRSEx type=host

All server names can be resolved by dns or /etc/hosts. So I don't know what is wrong with the key or with the last changes

russjones commented 24 days ago • edited Contributor

@adilsond To help debug this, can you do the following:

1. In the same shell you are going to run `ssh` from, can you show us the output of `ssh-add -l`. This will verify that you have an SSH agent running, you can communicate with it, and the keys are correctly loaded in the agent.
2. Run the following command `ssh -vvv -p 3023 adilson@prox01.someproxy.net`. This increases the logging level and only connect to the proxy to simplify things. When everything works you should see a error message that says something to the effect of "no pty access", this is what you want to see.

adilsond commented 18 days ago

On the client machine the result of running 'ssh-add -l' is 'Error connecting to agent: No such file or directory'. So I tried to run the system ssh-agent first. Then the resut changes to 'The agent has no identities.' The result is the same running tsh agent from the teleport server.

Running 'ssh -vvv -p 3023 adilson@prox01.someproxy.net' gives me the same result. The server ask for connecting with another plain key and, then, rejects the connection with the 'Permission denied (publickey) message' because it uses the recently added key insead of the cert-authority one.

Here is the debug log when I try to connect below.

ssh -vvv -p 3023 adilson@prox01.someproxy.net
OpenSSH_7.3p1 Ubuntu-1, OpenSSL 1.0.2g 1 Mar 2016
debug1: Reading configuration data /home/adilsond/.ssh/config
debug1: /home/adilsond/.ssh/config line 1: Applying options for *
debug1: /home/adilsond/.ssh/config line 7: Applying options for prox01.someproxy.net
debug1: Reading configuration data /etc/ssh/ssh_config
debug1: /etc/ssh/ssh_config line 19: Applying options for *
debug2: resolving "10.20.32.13" port 3023
debug2: ssh_connect_direct: needpriv 0
debug1: Connecting to 10.20.32.13 [10.20.32.13] port 3023.
debug1: Connection established.
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_rsa type -1
debug1: key_load_public: No such file or directory

```
debug1: identity file /home/adilsond/.ssh/id_rsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_dsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_dsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ecdsa type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ecdsa-cert type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ed25519 type -1
debug1: key_load_public: No such file or directory
debug1: identity file /home/adilsond/.ssh/id_ed25519-cert type -1
debug1: Enabling compatibility mode for protocol 2.0
debug1: Local version string SSH-2.0-OpenSSH_7.3p1 Ubuntu-1
debug1: Remote protocol version 2.0, remote software version Teleport 2.0.0-alpha.6
debug1: no match: Teleport 2.0.0-alpha.6
debug2: fd 3 setting O_NONBLOCK
debug1: Authenticating to 10.20.32.13:3023 as 'adilson'
debug3: send packet: type 20
debug1: SSH2_MSG_KEXINIT sent
debug3: receive packet: type 20
debug1: SSH2_MSG_KEXINIT received
debug2: local client KEXINIT proposal
debug2: KEX algorithms: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-hellman-group16-
sha512,diffie-hellman-group18-sha512,diffie-hellman-group-exchange-sha1,diffie-hellman-group14-
sha256,diffie-hellman-group14-sha1,ext-info-c
debug2: host key algorithms: ssh-rsa-cert-v01@openssh.com,ssh-rsa
debug2: ciphers ctos: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
debug2: ciphers stoc: chacha20-poly1305@openssh.com,aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,aes256-gcm@openssh.com,aes128-cbc,aes192-cbc,aes256-cbc,3des-cbc
debug2: MACs ctos: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-
64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
debug2: MACs stoc: umac-64-etm@openssh.com,umac-128-etm@openssh.com,hmac-sha2-256-
etm@openssh.com,hmac-sha2-512-etm@openssh.com,hmac-sha1-etm@openssh.com,umac-
64@openssh.com,umac-128@openssh.com,hmac-sha2-256,hmac-sha2-512,hmac-sha1
debug2: compression ctos: none,zlib@openssh.com,zlib
debug2: compression stoc: none,zlib@openssh.com,zlib
debug2: languages ctos:
debug2: languages stoc:
debug2: first_kex_follows 0
debug2: reserved 0
debug2: peer server KEXINIT proposal
debug2: KEX algorithms: curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,diffie-hellman-group14-sha1,diffie-hellman-group1-sha1
debug2: host key algorithms: ssh-rsa-cert-v01@openssh.com
debug2: ciphers ctos: aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,arcfour256,arcfour128
debug2: ciphers stoc: aes128-ctr,aes192-ctr,aes256-ctr,aes128-
gcm@openssh.com,arcfour256,arcfour128
debug2: MACs ctos: hmac-sha2-256-etm@openssh.com,hmac-sha2-256,hmac-sha1,hmac-sha1-96
debug2: MACs stoc: hmac-sha2-256-etm@openssh.com,hmac-sha2-256,hmac-sha1,hmac-sha1-96
debug2: compression ctos: none
debug2: compression stoc: none
debug2: languages ctos:
debug2: languages stoc:
debug2: first_kex_follows 0
debug2: reserved 0
debug1: kex: algorithm: curve25519-sha256@libssh.org
debug1: kex: host key algorithm: ssh-rsa-cert-v01@openssh.com
```

```
debug1: kex: server->client cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug1: kex: client->server cipher: aes128-ctr MAC: hmac-sha2-256-etm@openssh.com
compression: none
debug3: send packet: type 30
debug1: expecting SSH2_MSG_KEX_ECDH_REPLY
debug3: receive packet: type 31
debug1: Server host certificate: ssh-rsa-cert-v01@openssh.com
SHA256:OwD5hMqSrrkNtmsvY4MNQ76KmlP73miOqwOrY+poFZM, serial 0 ID "" CA ssh-rsa
SHA256:pji2vTctxErbjflUnO/UpBCbkWIU5gIIDFGx0cd2tOI valid forever
debug2: Server host certificate hostname: 69994d0c-9908-4b56-a2e1-68ac8c942e80.someproxy.net
debug2: Server host certificate hostname: prox01.someproxy.net
debug3: put_host_port: [10.20.32.13]:3023
debug3: put_host_port: [10.20.32.13]:3023
debug3: hostkeys_foreach: reading file "/home/adilsond/.ssh/known_hosts"
debug1: checking without port identifier
debug3: hostkeys_foreach: reading file "/home/adilsond/.ssh/known_hosts"
debug1: No matching CA found. Retry with plain key
debug1: No matching CA found. Retry with plain key
debug1: checking without port identifier
debug3: hostkeys_foreach: reading file "/home/adilsond/.ssh/known_hosts"
The authenticity of host '[10.20.32.13]:3023 ([10.20.32.13]:3023)' can't be established.
RSA key fingerprint is SHA256:OwD5hMqSrrkNtmsvY4MNQ76KmlP73miOqwOrY+poFZM.
Are you sure you want to continue connecting (yes/no)? yes <- I think that this message should not
appear here. :/
Warning: Permanently added '[10.20.32.13]:3023' (RSA) to the list of known hosts.
debug3: send packet: type 21
debug2: set_newkeys: mode 1
debug1: rekey after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS sent
debug1: expecting SSH2_MSG_NEWKEYS
debug3: receive packet: type 21
debug2: set_newkeys: mode 0
debug1: rekey after 4294967296 blocks
debug1: SSH2_MSG_NEWKEYS received
debug2: key: /home/adilsond/.ssh/id_rsa ((nil))
debug2: key: /home/adilsond/.ssh/id_dsa ((nil))
debug2: key: /home/adilsond/.ssh/id_ecdsa ((nil))
debug2: key: /home/adilsond/.ssh/id_ed25519 ((nil))
debug3: send packet: type 5
debug3: receive packet: type 6
debug2: service_accept: ssh-userauth
debug1: SSH2_MSG_SERVICE_ACCEPT received
debug3: send packet: type 50
debug3: receive packet: type 51
debug1: Authentications that can continue: publickey
debug3: start over, passed a different list publickey
debug3: preferred gssapi-keyex,gssapi-with-mic,publickey,keyboard-interactive,password
debug3: authmethod_lookup publickey
debug3: remaining preferred: keyboard-interactive,password
debug3: authmethod_is_enabled publickey
debug1: Next authentication method: publickey
debug1: Trying private key: /home/adilsond/.ssh/id_rsa
debug3: no such identity: /home/adilsond/.ssh/id_rsa: No such file or directory
debug1: Trying private key: /home/adilsond/.ssh/id_dsa
debug3: no such identity: /home/adilsond/.ssh/id_dsa: No such file or directory
debug1: Trying private key: /home/adilsond/.ssh/id_ecdsa
debug3: no such identity: /home/adilsond/.ssh/id_ecdsa: No such file or directory
debug1: Trying private key: /home/adilsond/.ssh/id_ed25519
debug3: no such identity: /home/adilsond/.ssh/id_ed25519: No such file or directory
debug2: we did not send a packet, disable method
debug1: No more authentication methods to try.
Permission denied (publickey).
```

russjones commented 18 days ago Contributor

@adilsond It looks like the issue is you are not setting up your agent correctly. Try the following:

1. Open a Terminal window, type in `tsh --proxy=work.example.com agent`.
2. Open another Terminal window, copy the output from Step 1 into the new terminal window. What are you doing here is setting the `SSH_AUTH_SOCK` environment variable so Teleport and OpenSSH can find the agent.
3. If you have not logged in with `tsh` already, type `tsh --proxy=work.example.com login`. This will log you in and load your certificate into the agent. If you have already logged in you don't need to do anything, starting the agent in the pervious step will have loaded your certificates into the agent. Now run `ssh-add -l` to verify that your keys are loaded into the agent, you should see output like this:

```
$ ssh-add -l
2048 SHA256:abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQ teleport:foo (RSA-CERT)
2048 SHA256:abcdefghijklmnopqrstuvwxyzABCDEFGHIJKLMNOPQ teleport:foo (RSA)
```

4. Within the same Terminal window as the previous step, try to to connect to the proxy: `ssh -vvv -p 3023 work.example.com`.

adilsond commented 17 days ago

The error message changed for this before disconnecting.

proxy doesn't support request type 'pty-req'debug2: channel 0: written 44 to efd 7
debug3: receive packet: type 100
debug2: channel_input_status_confirm: type 100 id 0
PTY allocation request failed on channel 0

Trying to connect to another server show this message:

debug1: Local version string SSH-2.0-OpenSSH_7.2p2 Ubuntu-4ubuntu2.1
subsystem request failed on channel 0
ssh_exchange_identification: Connection closed by remote host

But I have to use another machine with teleport installed to log in.

So I still have the problem since I'm trying to connect from a machine that don't have teleport, tsh and tctl installed. So login with tsh first is not possible from this machine.

russjones commented 17 days ago • edited Contributor

@adilsond That's good, `proxy doesn't support request type 'pty-req'debug2: channel 0: written 44 to efd 7` means you were able to connect to the proxy and the proxy is telling you it doesn't support PTY requests. This is what you want to see because the Teleport proxy is configured to not support PTY requests for security reasons.

For Teleport and OpenSSH to interoperate, you'll need at least `tsh` installed on the machine you want to make connections from to a Teleport cluster. You need `tsh` because it will be used obtain certificates. The next step is to setup your `~/.ssh/config` file like the Admin Guide says:

```
# work.example.com is the jump host (proxy). credentials will be obtained from the
# teleport agent.
Host work.example.com
    HostName 192.168.1.2
    Port 3023

# connect to nodes in the work.example.com cluster through the jump
```

```
# host (proxy) using the same. credentials will be obtained from the
# teleport agent.
Host *.work.example.com
    HostName %h
    Port 3022
    ProxyCommand ssh -p 3023 %r@work.example.com -s proxy:%h:%p
```

Then you should be able to connect to your node within the cluster by simply typing something like `ssh database.work.example.com` .

russjones commented 13 days ago Contributor

@adilsond noriuky mebezac I'm going to close this issue for now. If any of you are still running into issues feel free to re-open/comment and I can dig in further but I think the issues here are resolved.

 **russjones** closed this 13 days ago