GTS 34 | SP 12/2019

GSH

Autenticação efêmera para servidores SSH

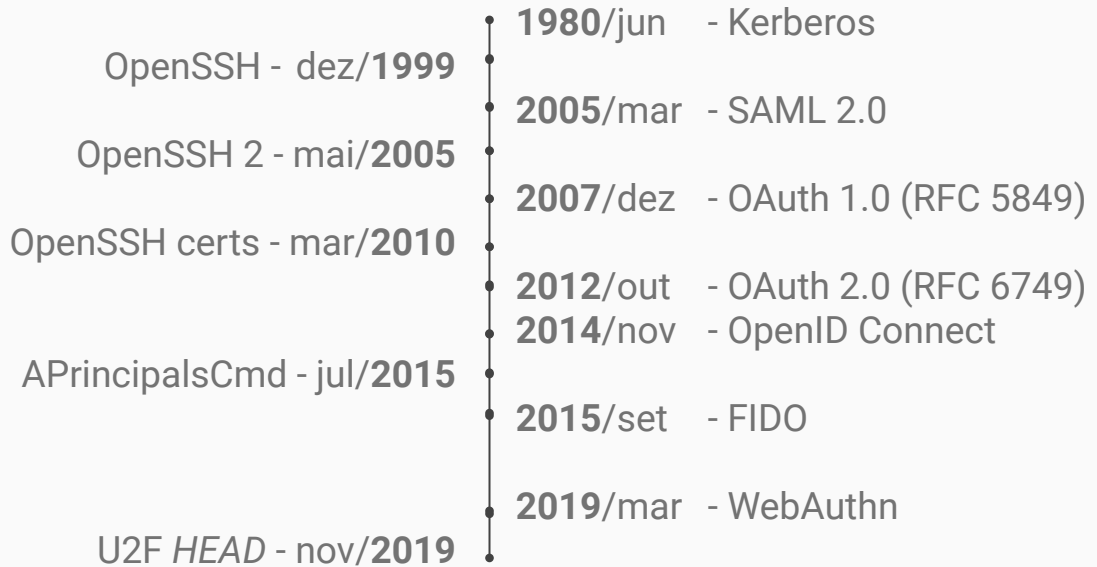
Manoel Domingues Junior
Globo

Agenda

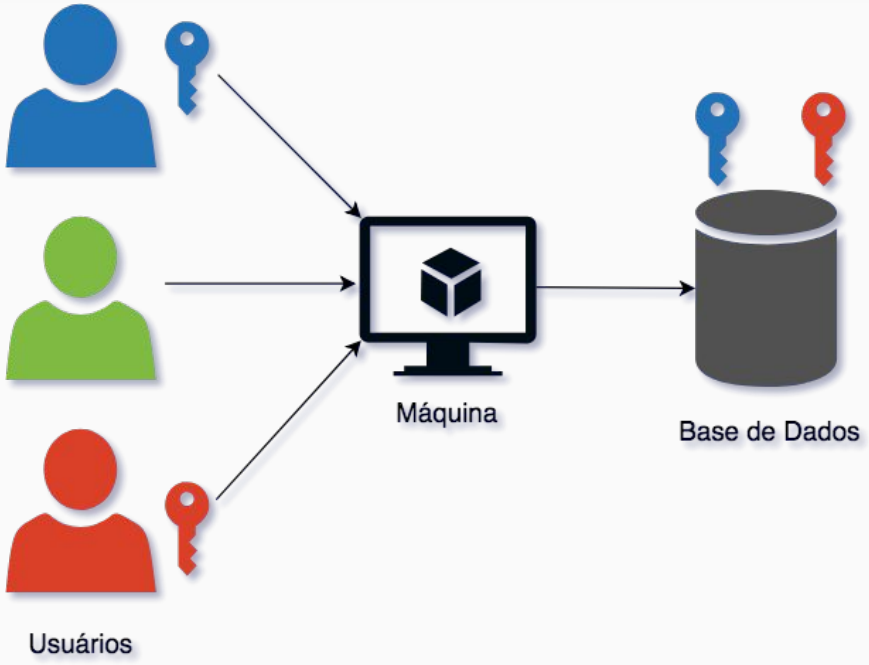
- Autenticação
- SSH e seus usos
- Alguns problemas
- GSH
- Próximos passos

Autenticação

SSH vs Web



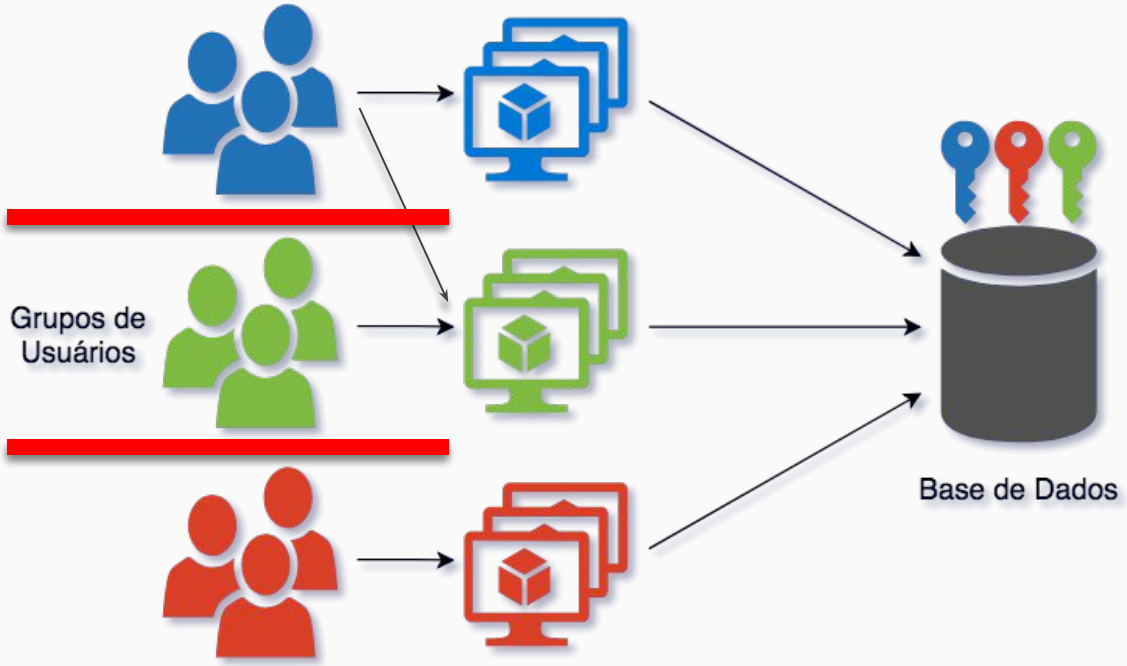
SSH como é hoje



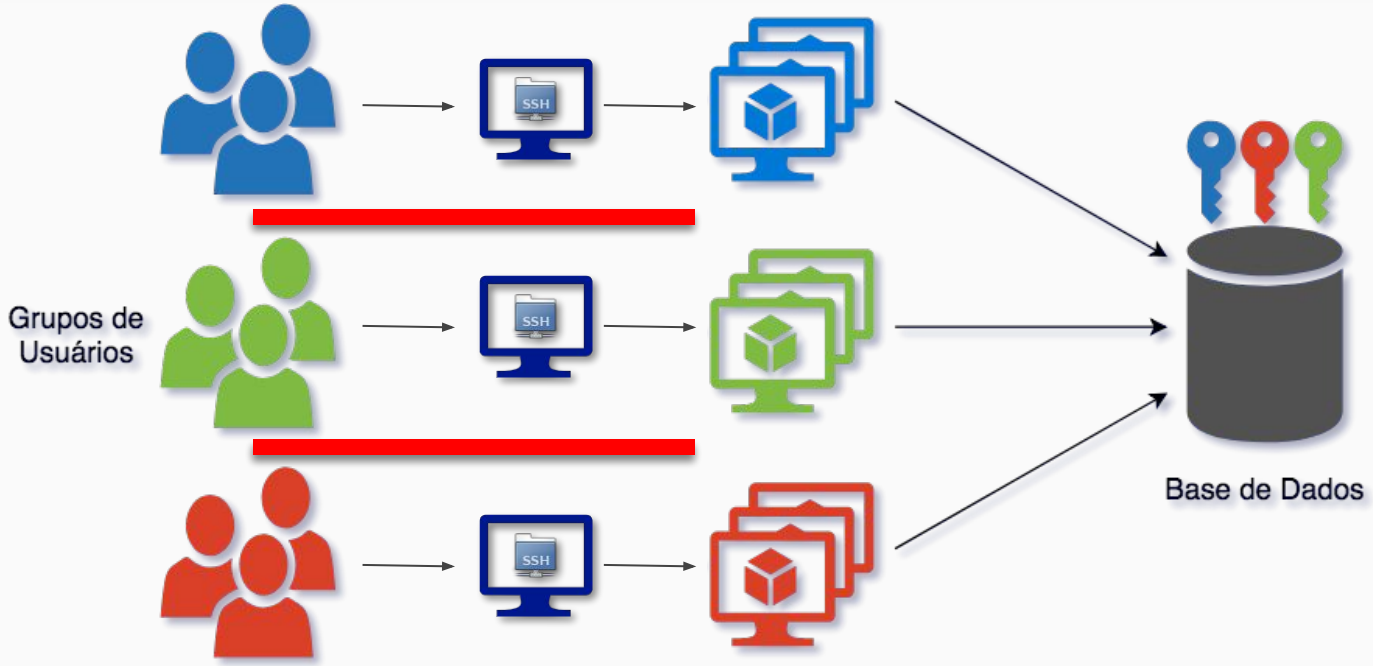
SSH como é hoje

SSH como é hoje

SSH como é hoje

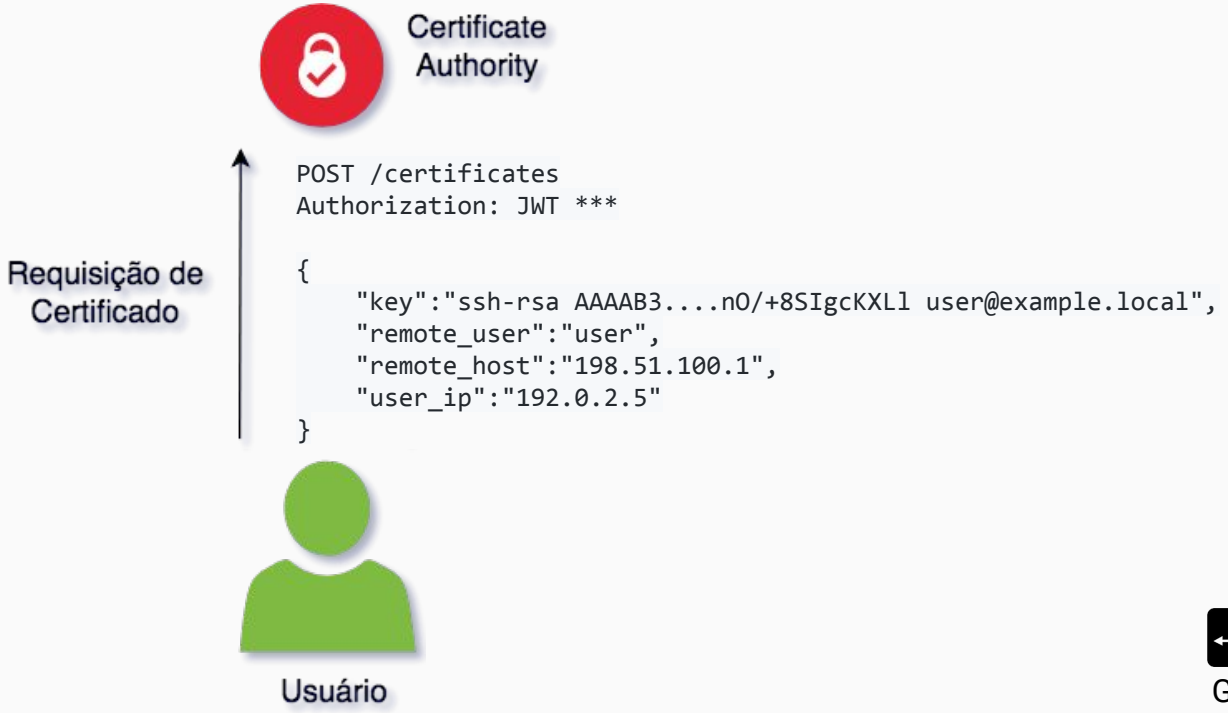


SSH como é hoje



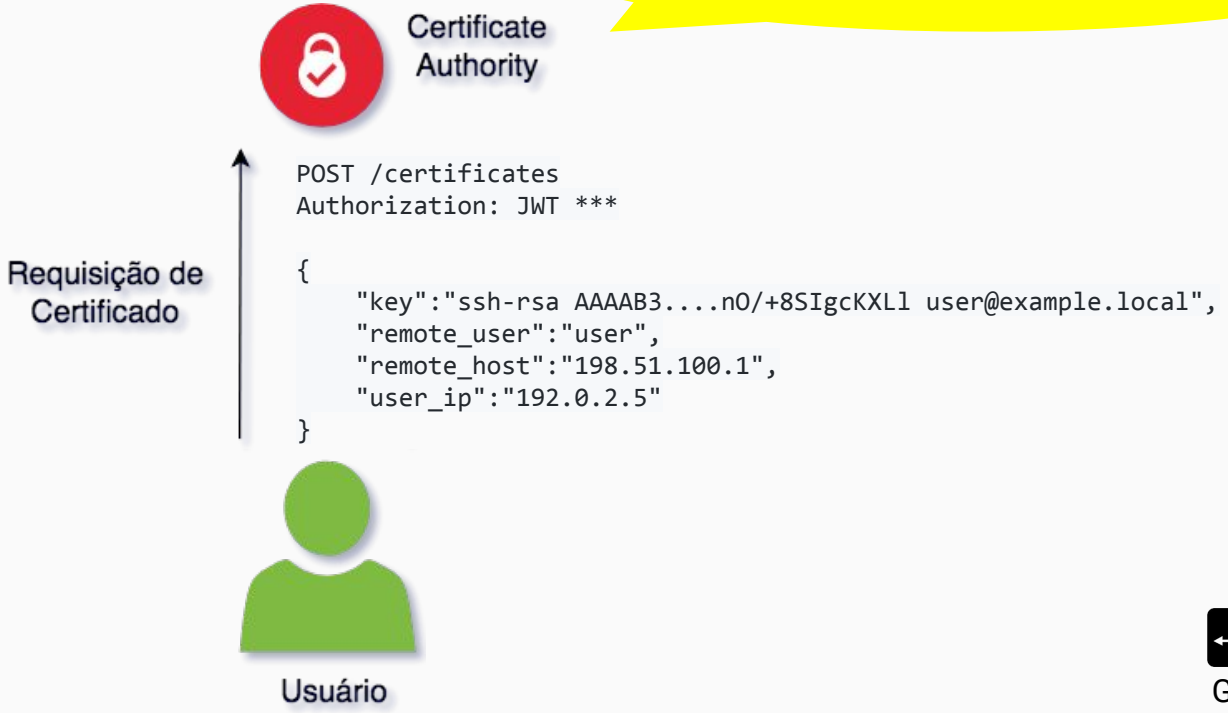
Possível solução

Possível solução



Possível solução

user pode acessar 198.51.100.1 a partir de 192.0.2.5?



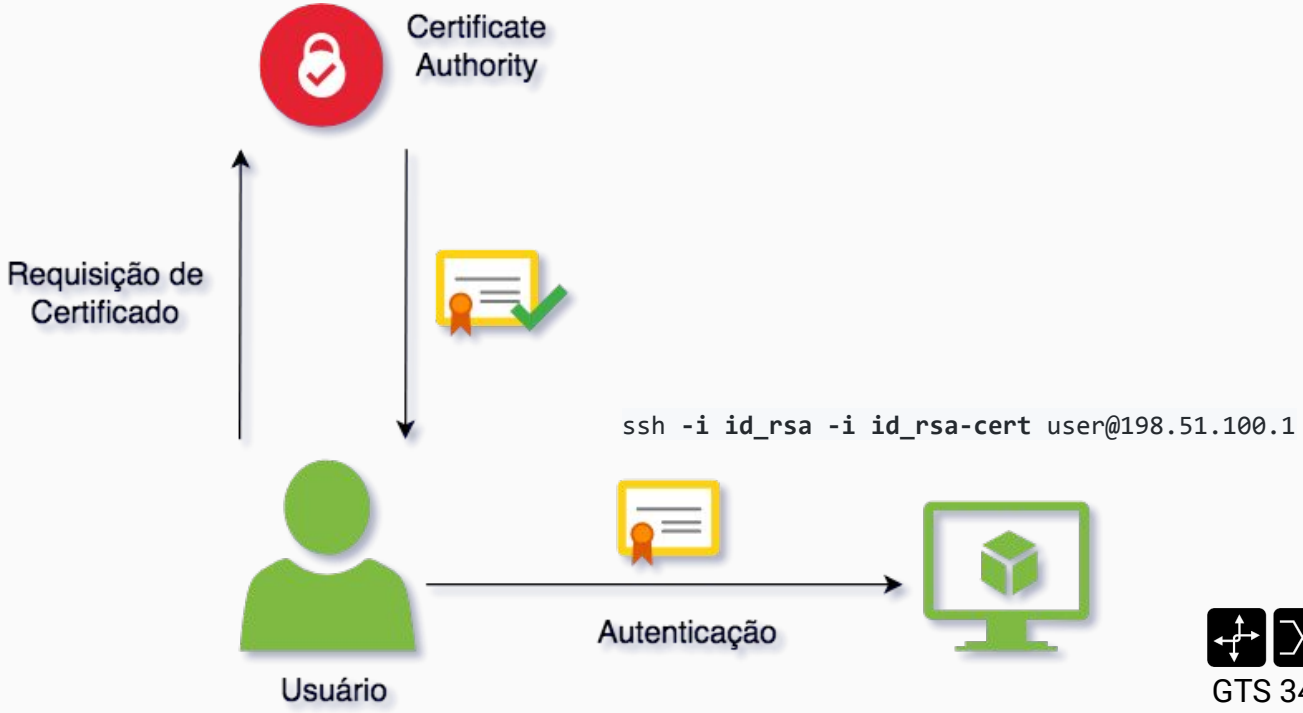
Possível solução


```
HTTP/1.1 200 OK

{
  "certificate": "ssh-rsa-cert-v01@openssh.com
AAAAHHNzaC1yc2EtY2VydC12MDFAb3BlbnNzaC5jb20AAAAgbR95jAgW
...u0/G1QHzUZWgGQzq2BnaeWs8uuYMCAel2NZnoMIqy5VldSDA\n",
  "result": "success"
}
```

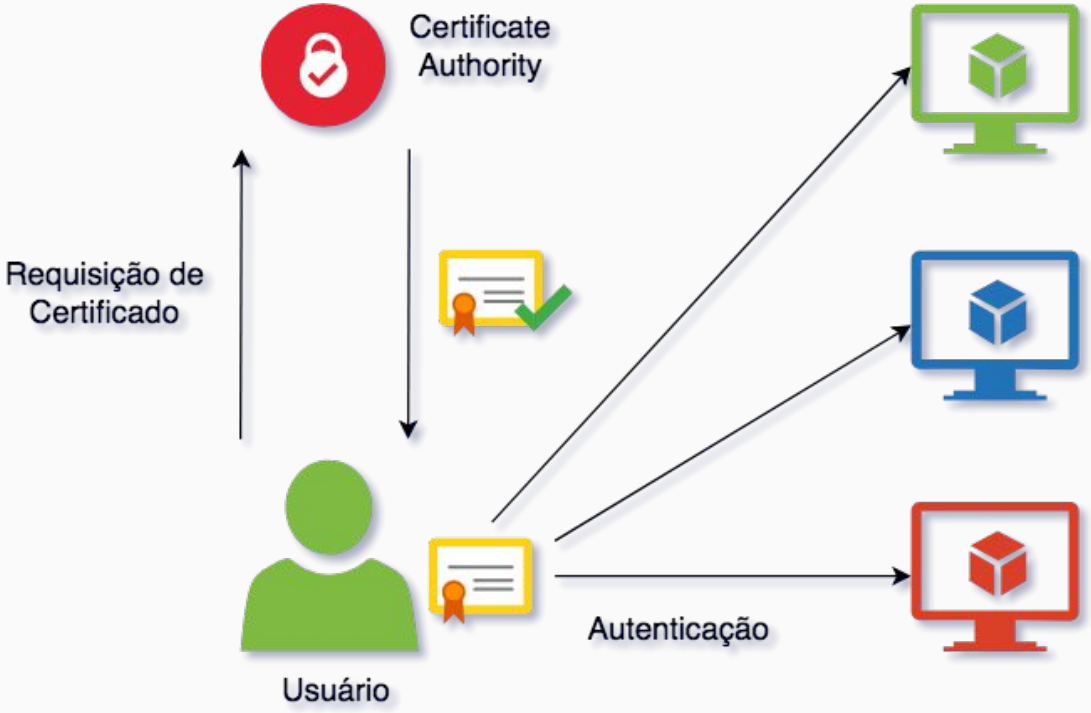
Possível solução

```
$ ssh-keygen -Lf id_rsa-cert.pub
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT
SHA256:1ChWGB1HsSvlVV8Od1WmyXLZLorkncIsoQ0boGmKDcE
        Signing CA: RSA SHA256:zJNiSEvSCvOvfWxieW1VGHo4D7Fk039F9E2CCeBfsjE
(using ssh-rsa)
        Key ID: "64e0c354-b92a-415b-9cf8-698f73ca7968"
        Serial: 0
        Valid: from 2019-12-12T14:34:28 to 2019-12-12T14:44:58
        Principals:
                user
        Critical Options:
                source-address 192.0.2.5
        Extensions:
                permit-pty
```

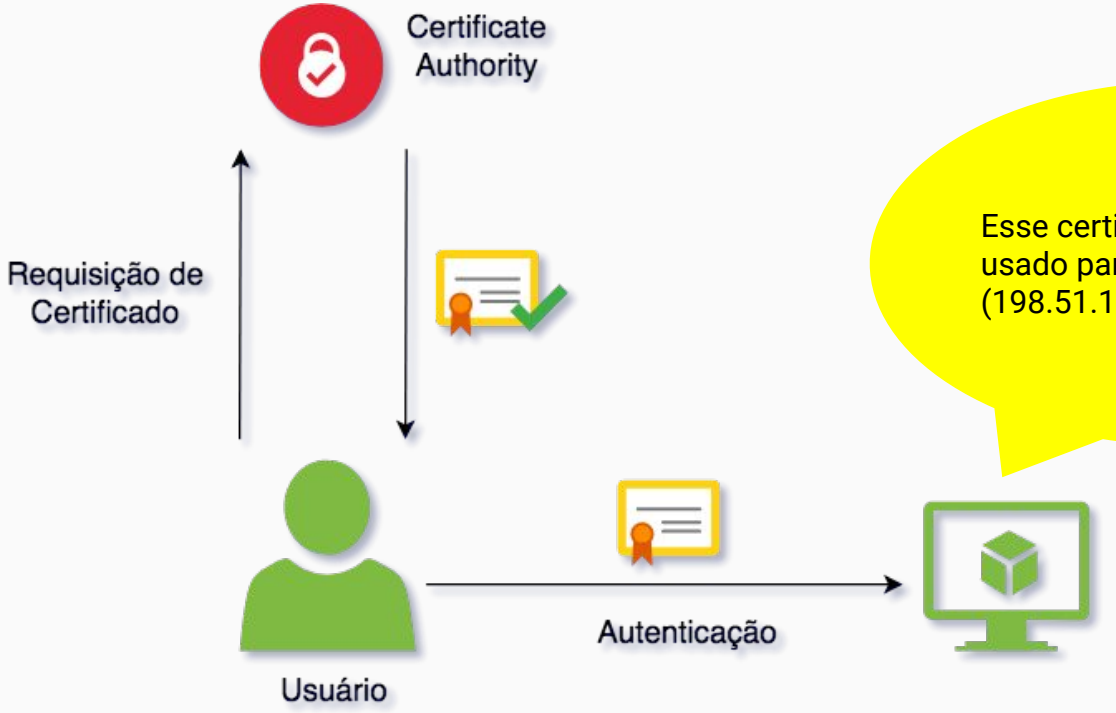
Possível solução



Porém...


Certificate Authority
Requisição de Certificado
Usuário
Autenticação

Possível solução



sshd_config(5) - OpenBSD ma

man.openbsd.org/sshd_config#AuthorizedPrincipalsCommand

Incognito (2)

AUTHORIZED_KEYS FILE FORMAT section of sshd(8). Arguments to **AuthorizedKeysFile** accept the tokens described in the TOKENS section. After expansion, **AuthorizedKeysFile** is taken to be an absolute path or one relative to the user's home directory. Multiple files may be listed, separated by whitespace. Alternately this option may be set to **none** to skip checking for user keys in files. The default is ".ssh/authorized_keys .ssh/authorized_keys2".

AuthorizedPrincipalsCommand

Specifies a program to be used to generate the list of allowed certificate principals as per **AuthorizedPrincipalsFile**. The program must be owned by root, not writable by group or others and specified by an absolute path. Arguments to **AuthorizedPrincipalsCommand** accept the tokens described in the TOKENS section. If no arguments are specified then the username of the target user is used.

The program should produce on standard output zero or more lines of **AuthorizedPrincipalsFile** output. If either **AuthorizedPrincipalsCommand** or **AuthorizedPrincipalsFile** is specified, then certificates offered by the client for authentication must contain a principal that is listed. By default, no **AuthorizedPrincipalsCommand** is run.

AuthorizedPrincipalsCommandUser

Specifies the user under whose account the **AuthorizedPrincipalsCommand** is run. It is recommended to use a dedicated user that has no other role on the host than running authorized principals commands. If **AuthorizedPrincipalsCommand** is specified but **AuthorizedPrincipalsCommandUser** is not, then sshd(8) will refuse to start.

AuthorizedPrincipalsFile

Specifies a file that lists principal names that are accepted for certificate authentication. When using certificates signed by a key listed in **TrustedUserCAKeys**, this file lists names, one of which must appear in the certificate for it to be accepted for authentication. Names are listed one per line preceded by key options (as described in AUTHORIZED_KEYS FILE FORMAT in sshd(8)). Empty lines and comments starting with '#' are ignored.

Usuário

sshd_config(5) - OpenBSD ma

man.openbsd.org/sshd_config#TOKENS

Incognito (2)

TOKENS

Arguments to some keywords can make use of tokens, which are expanded at runtime:

%%	A literal '%'.
%D	The routing domain in which the incoming connection was received.
%F	The fingerprint of the CA key.
%f	The fingerprint of the key or certificate.
%h	The home directory of the user.
%i	The key ID in the certificate.
%K	The base64-encoded CA key.
%k	The base64-encoded key or certificate for authentication.
%s	The serial number of the certificate.
%T	The type of the CA key.
%t	The key or certificate type.
%U	The numeric user ID of the target user.
%u	The username.

AuthorizedKeysCommand accepts the tokens %%, %f, %h, %k, %t, %U, and %u.

AuthorizedKeysFile accepts the tokens %%, %h, %U, and %u.

AuthorizedPrincipalsCommand accepts the tokens %%, %F, %f, %h, %i, %K, %k, %s, %T, %t, %U, and %u.

AuthorizedPrincipalsFile accepts the tokens %%, %h, %U, and %u.

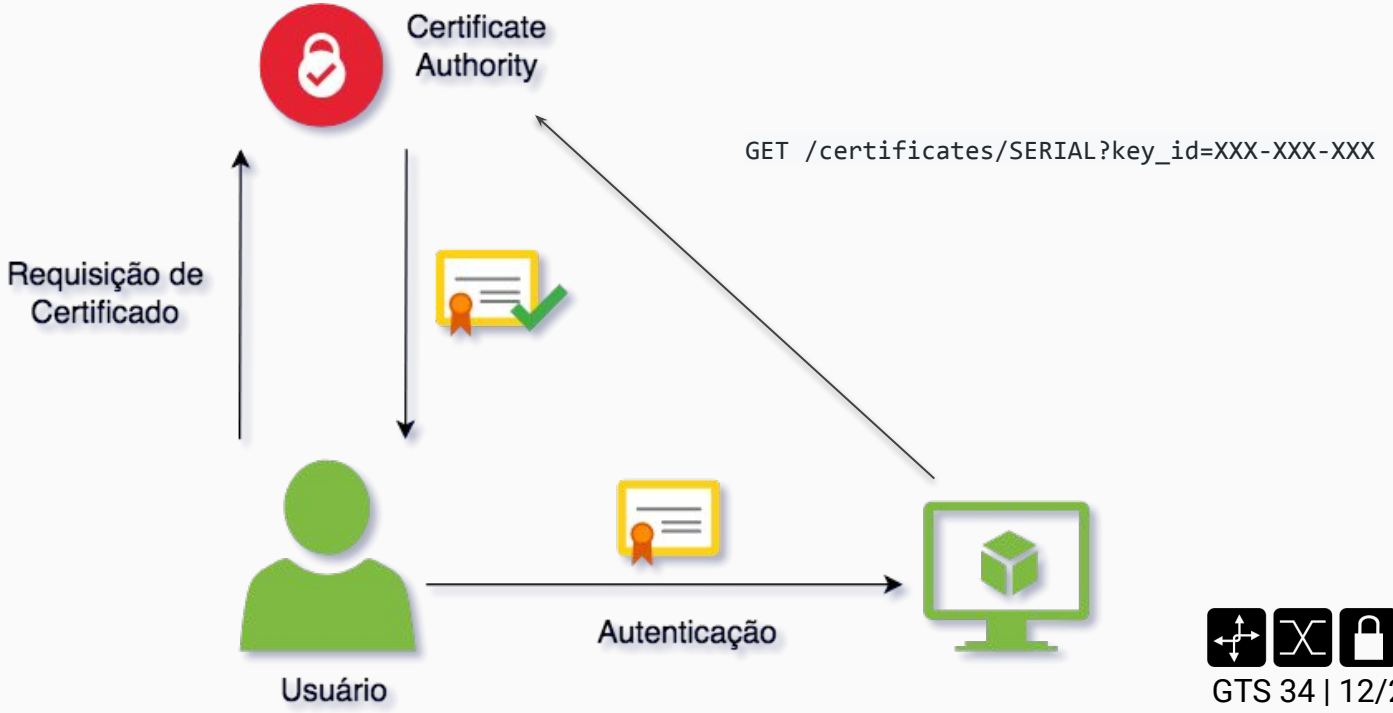
ChrootDirectory accepts the tokens %%, %h, %U, and %u.

RoutingDomain accepts the token %D.

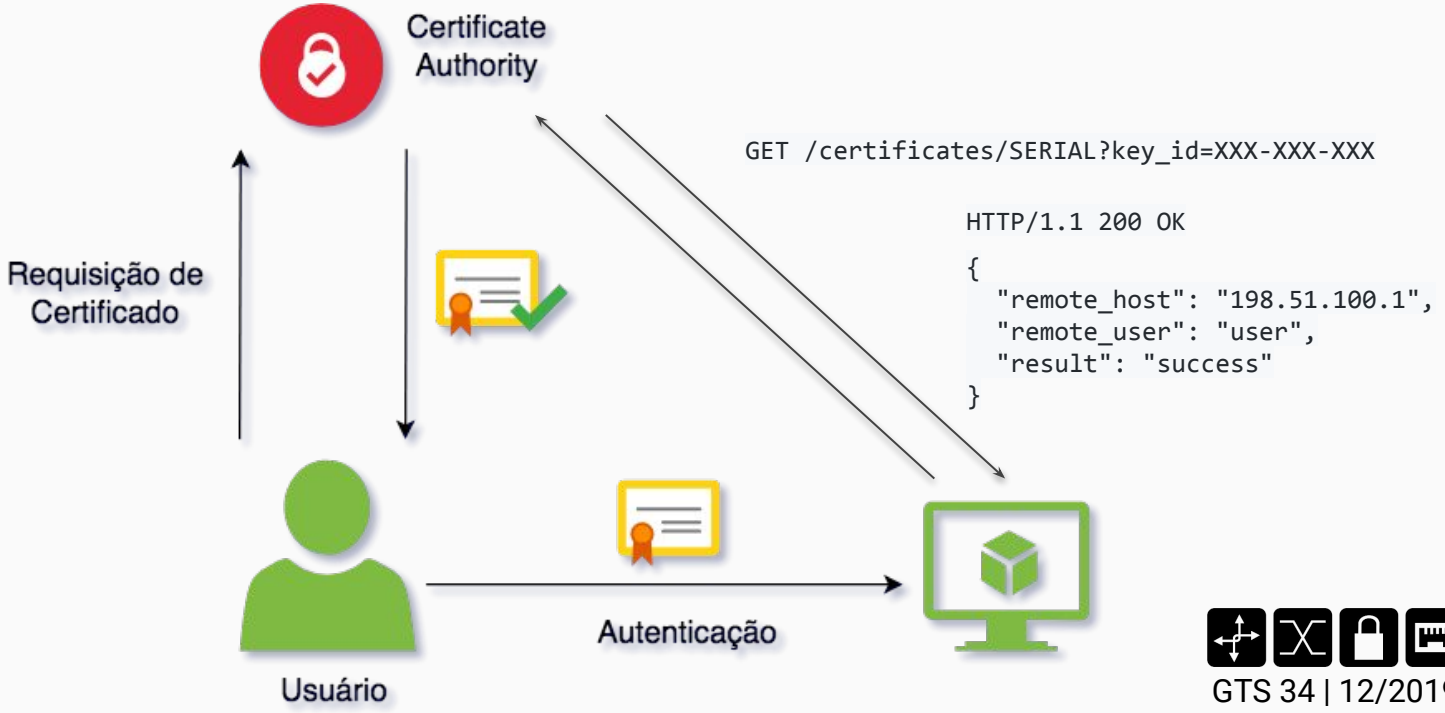
FILES

Usuário

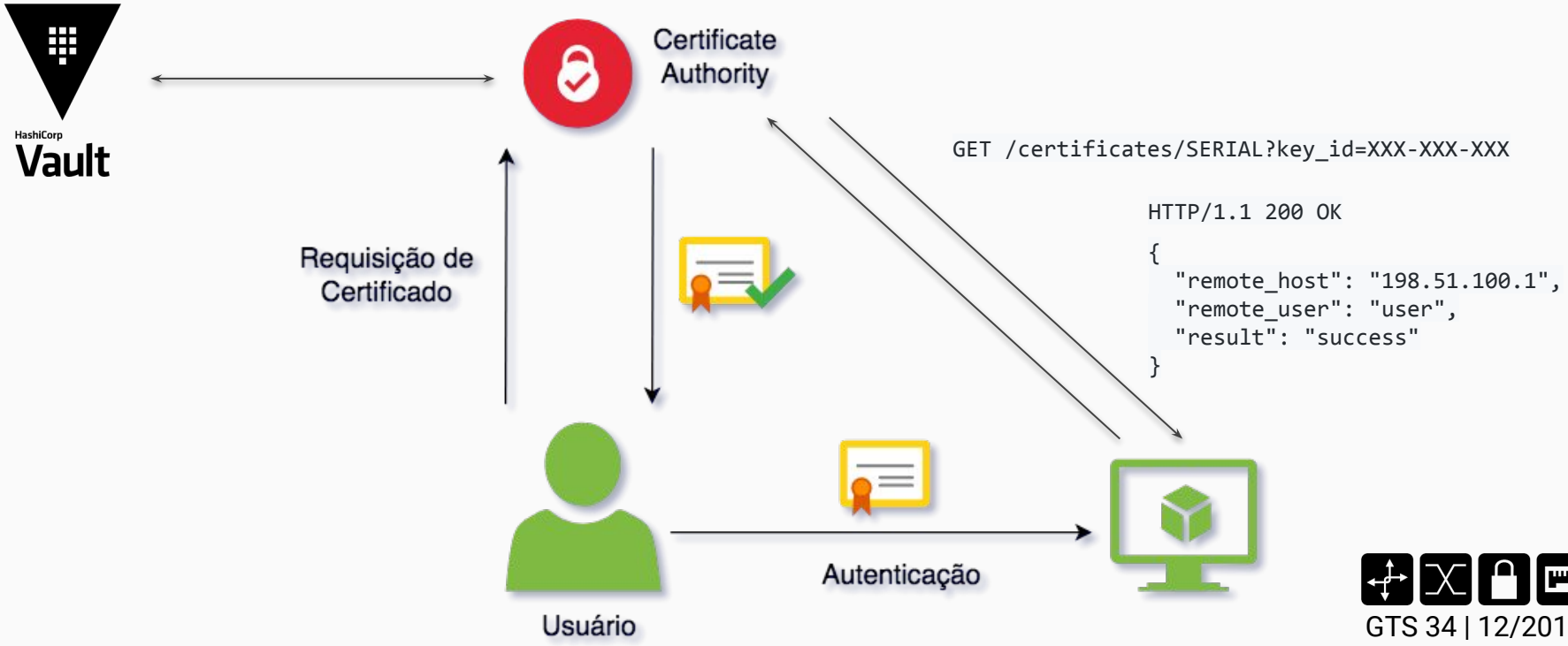
Possível solução



Possível solução



Possível solução



GSH

Mudança na configuração do OpenSSH (>=6.8):

```
AuthorizedPrincipalsCommand /usr/local/bin/gsh-agent check-permission
--api https://gsh-api.example.com --key-id %i --serial-number %s
--username %u
AuthorizedPrincipalsCommandUser root
TrustedUserCAKeys /etc/ssh/cas.pub
```

O comando chamado pelo OpenSSH deverá retornar um *principal* (username) válido com o certificado apresentado.

```
>#  /usr/local/bin/gsh-agent check-permission --api https://gsh-api.example.com --key-id
key-id-1234567890 --serial-number 0987654321 --username manoel.junior
> manoel.junior
```

https://man.openbsd.org/sshd_config#AuthorizedPrincipalsCommand

clear Clear all enabled permissions. This is useful for clearing the default set of permissions so permissions may be added individually.

critical:*name*[=*contents*]
extension:*name*[=*contents*]
Includes an arbitrary certificate critical option or extension. The specified *name* should include a domain suffix, e.g. “name@example.com”. If *contents* is specified then it is included as the contents of the extension/option encoded as a string, otherwise the extension/option is created with no contents (usually indicating a flag). Extensions may be ignored by a client or server that does not recognise them, whereas unknown critical options will cause the certificate to be refused.

force-command=*command*
Forces the execution of *command* instead of any shell or command specified by the user when the certificate is used for authentication.

no-agent-forwarding
Disable ssh-agent(1) forwarding (permitted by default).

no-port-forwarding
Disable port forwarding (permitted by default).

no-pty Disable PTY allocation (permitted by default).

no-user-rc Disable execution of *~/.ssh/rc* by sshd(8) (permitted by default).

no-x11-forwarding
Disable X11 forwarding (permitted by default).

permit-agent-forwarding
Allows ssh-agent(1) forwarding.

permit-port-forwarding
Allows port forwarding.

permit-pty Allows PTY allocation.

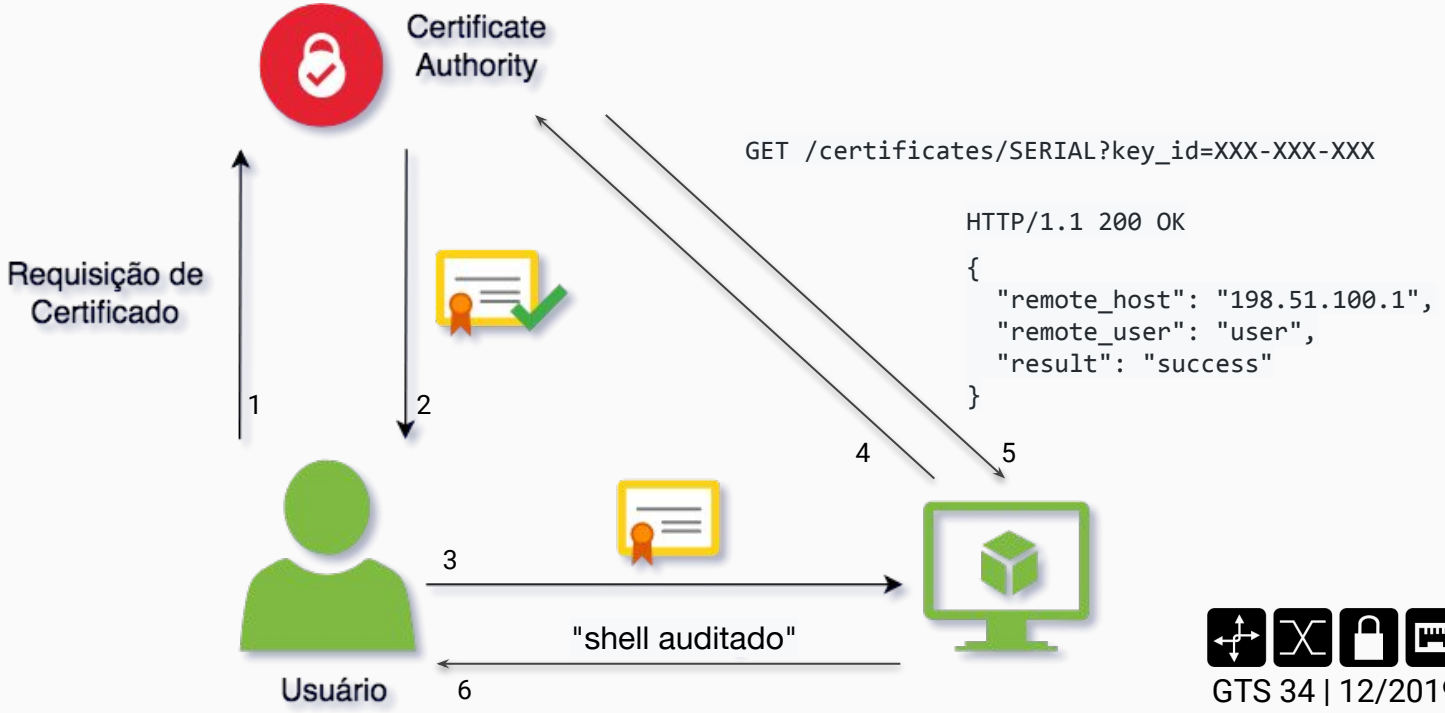
permit-user-rc
Allows execution of *~/.ssh/rc* by sshd(8).

permit-X11-forwarding
Allows X11 forwarding.

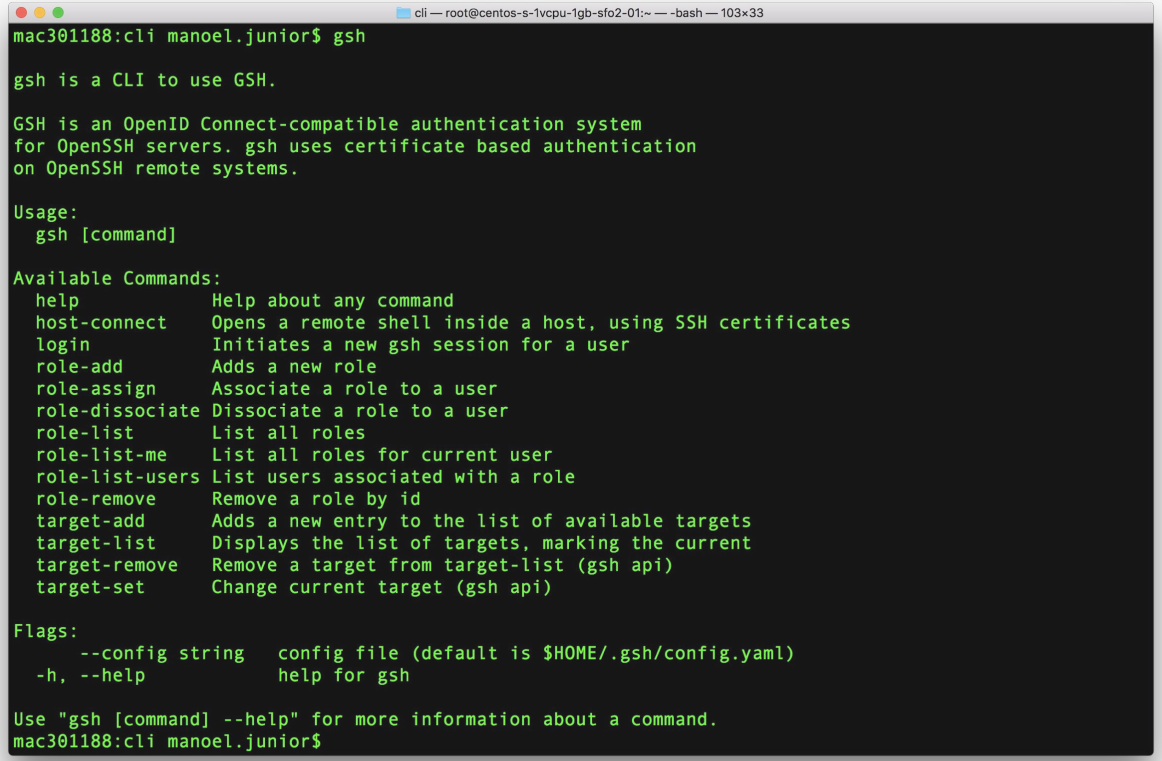
no-touch-required
Do not require signatures made using this key require demonstration of user presence (e.g. by having the user touch the key). This option only makes sense for the Security Key algorithms **ecdsa-sk** and **ed25519-sk**.

source-address=*address_list*
Restrict the source addresses from which the certificate is considered valid. The *address_list* is a comma-separated list of one or more address/netmask pairs in CIDR format.

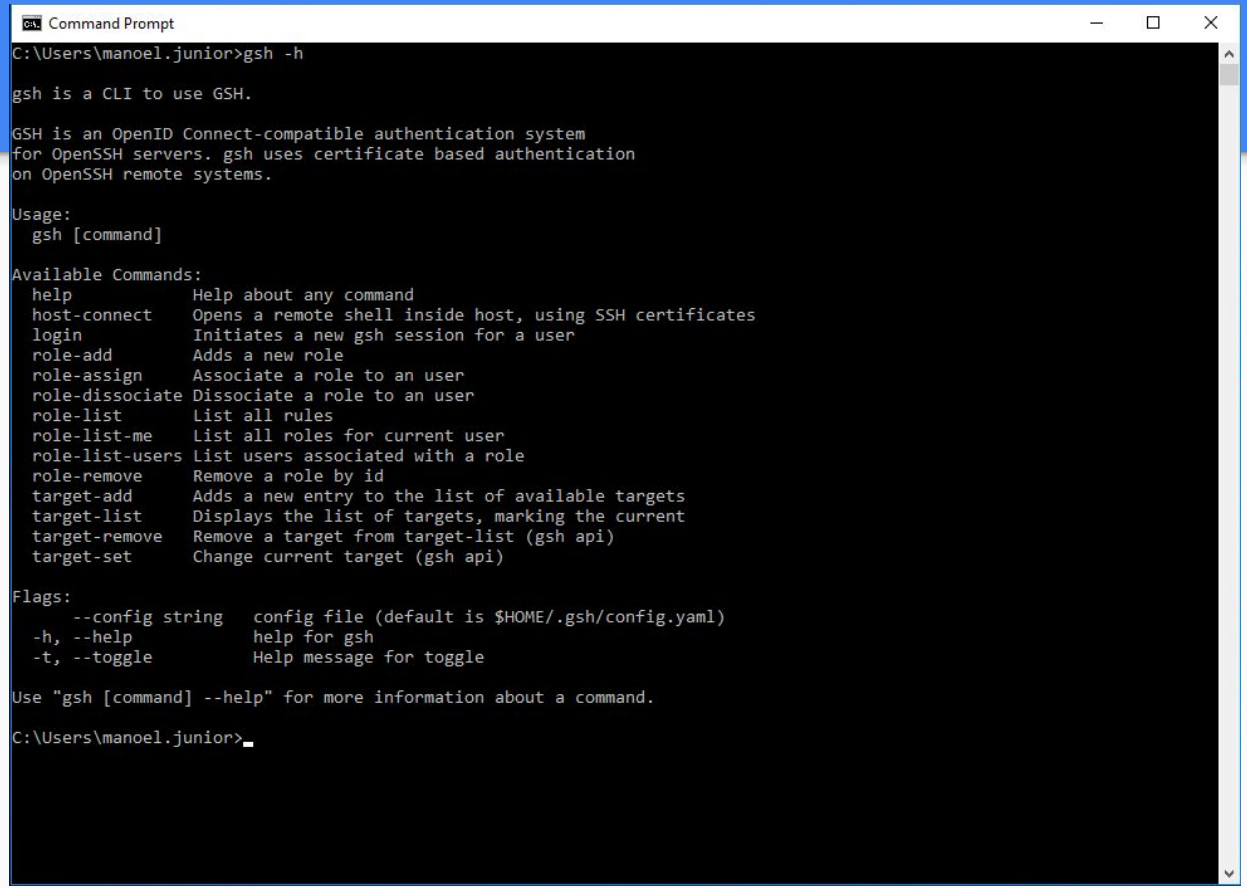
indo além...


Certificate Authority
GET /certificates/SERIAL?key_id=XXX-XXX-XXX
HTTP/1.1 200 OK
{
"remote_host": "198.51.100.1",
"remote_user": "user",
"result": "success"
}
Requisição de Certificado
1
2
3
4
5
6
"shell auditado"
Usuário

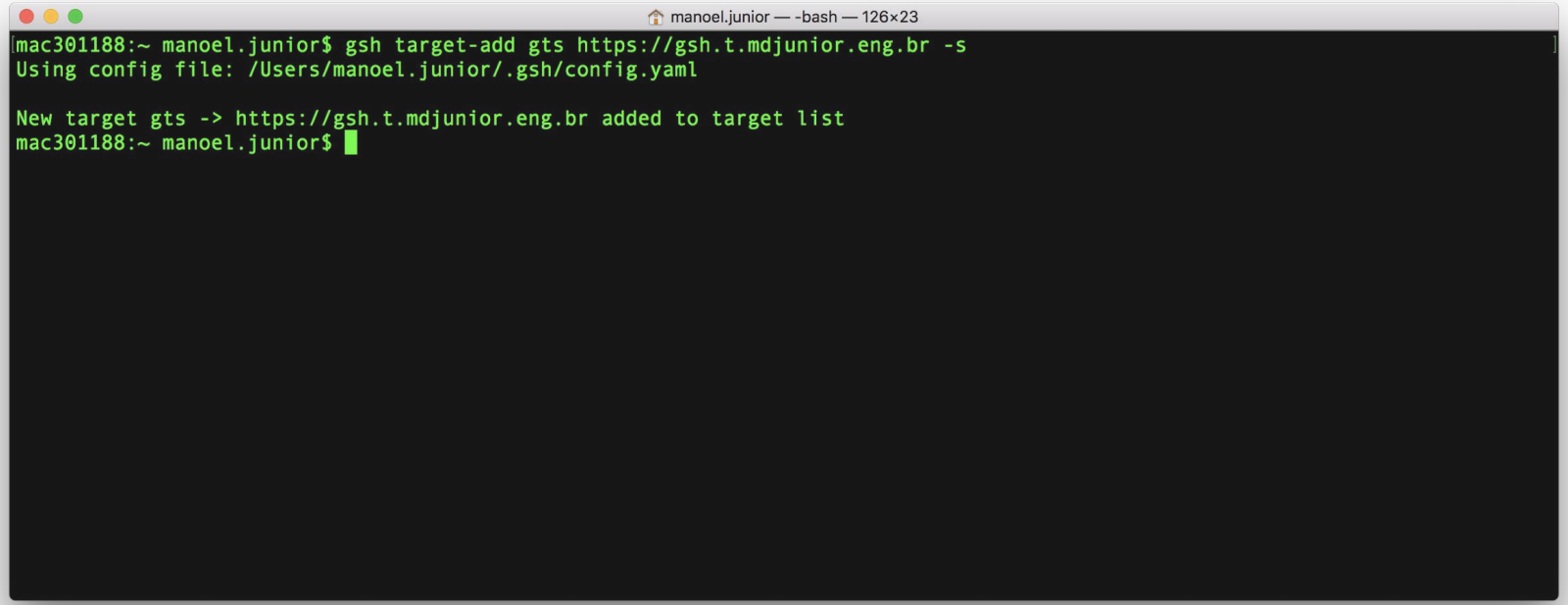
GSH


cli — root@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 103×33
mac301188:cli manoel.junior$ gsh
gsh is a CLI to use GSH.
GSH is an OpenID Connect-compatible authentication system
for OpenSSH servers. gsh uses certificate based authentication
on OpenSSH remote systems.
Usage:
gsh [command]
Available Commands:
help Help about any command
host-connect Opens a remote shell inside a host, using SSH certificates
login Initiates a new gsh session for a user
role-add Adds a new role
role-assign Associate a role to a user
role-dissociate Dissociate a role to a user
role-list List all roles
role-list-me List all roles for current user
role-list-users List users associated with a role
role-remove Remove a role by id
target-add Adds a new entry to the list of available targets
target-list Displays the list of targets, marking the current
target-remove Remove a target from target-list (gsh api)
target-set Change current target (gsh api)
Flags:
--config string config file (default is $HOME/.gsh/config.yaml)
-h, --help help for gsh
Use "gsh [command] --help" for more information about a command.
mac301188:cli manoel.junior$

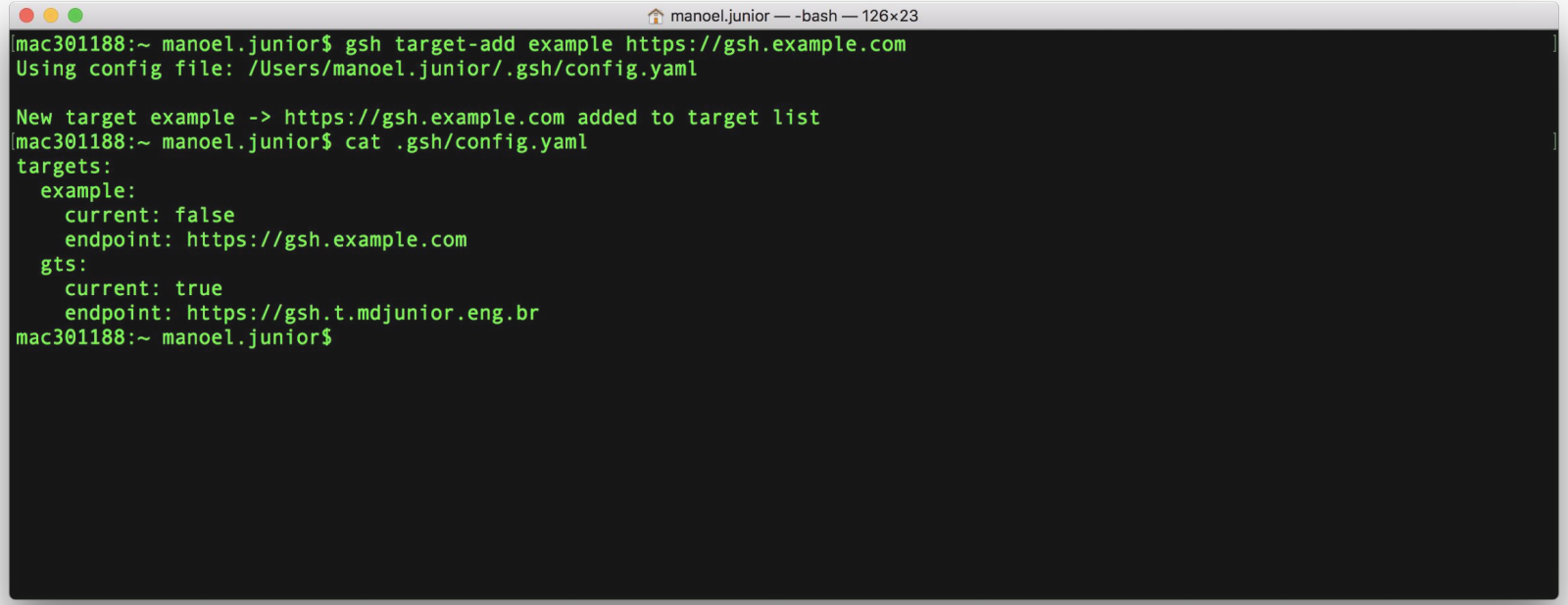
GSH


Command Prompt
C:\Users\manoel.junior>gsh -h
gsh is a CLI to use GSH.
GSH is an OpenID Connect-compatible authentication system
for OpenSSH servers. gsh uses certificate based authentication
on OpenSSH remote systems.
Usage:
gsh [command]
Available Commands:
help Help about any command
host-connect Opens a remote shell inside host, using SSH certificates
login Initiates a new gsh session for a user
role-add Adds a new role
role-assign Associate a role to an user
role-dissociate Dissociate a role to an user
role-list List all rules
role-list-me List all roles for current user
role-list-users List users associated with a role
role-remove Remove a role by id
target-add Adds a new entry to the list of available targets
target-list Displays the list of targets, marking the current
target-remove Remove a target from target-list (gsh api)
target-set Change current target (gsh api)
Flags:
--config string config file (default is $HOME/.gsh/config.yaml)
-h, --help help for gsh
-t, --toggle Help message for toggle
Use "gsh [command] --help" for more information about a command.
C:\Users\manoel.junior>

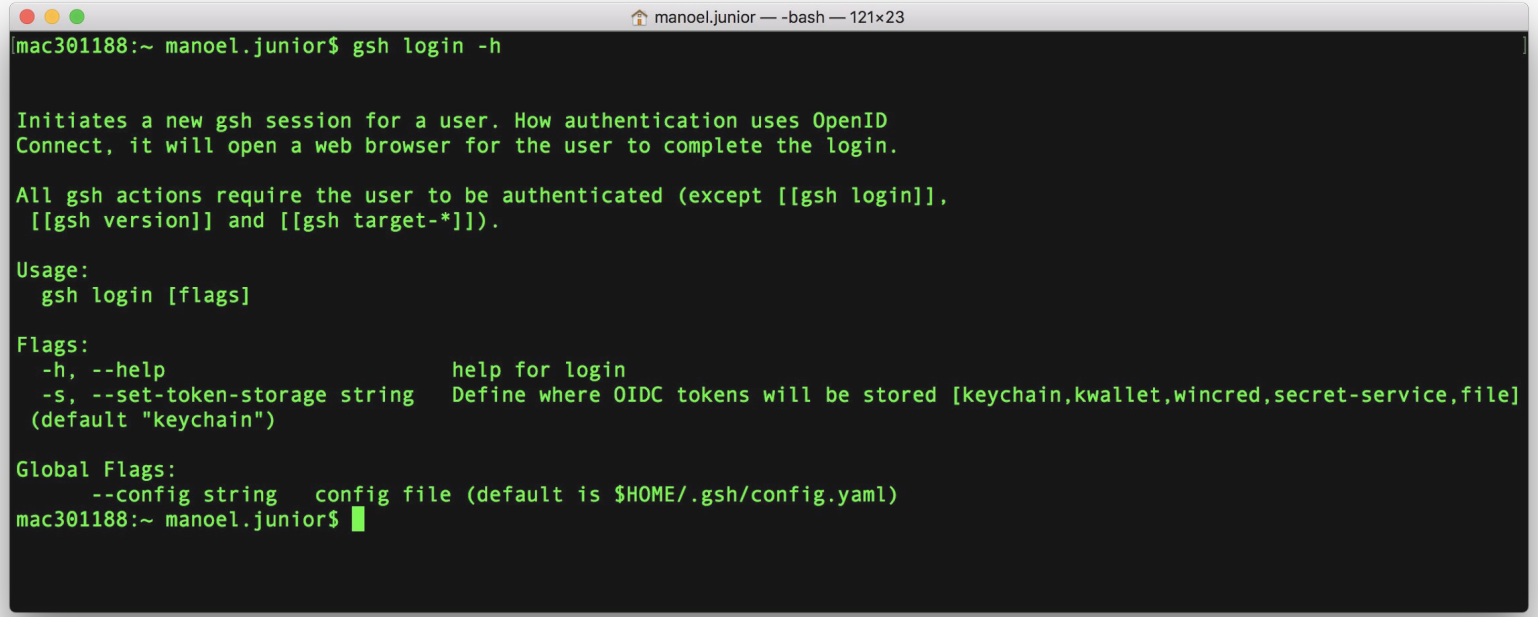
GSH


manoel.junior — -bash — 126×23
mac301188:~ manoel.junior$ gsh target-add gts https://gsh.t.mdjunior.eng.br -s
Using config file: /Users/manoel.junior/.gsh/config.yaml
New target gts -> https://gsh.t.mdjunior.eng.br added to target list
mac301188:~ manoel.junior$

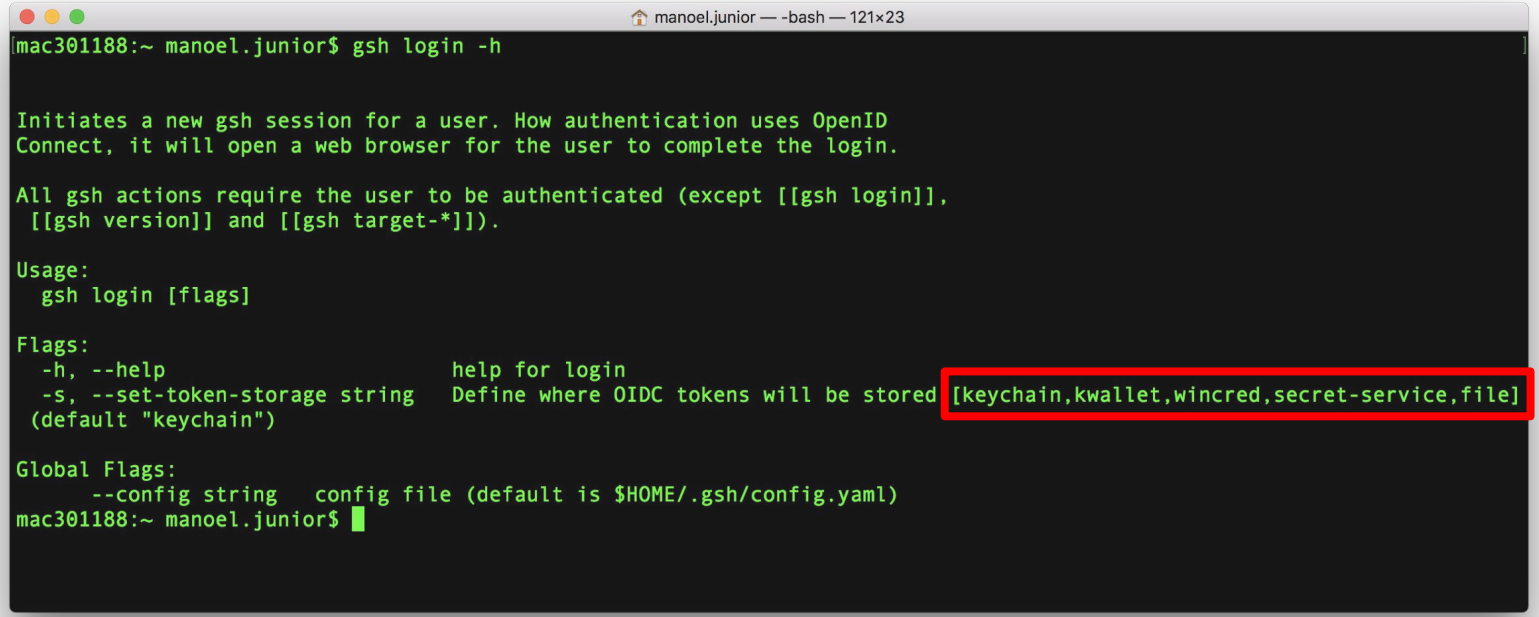
GSH


manoel.junior — -bash — 126×23
mac301188:~ manoel.junior$ gsh target-add example https://gsh.example.com
Using config file: /Users/manoel.junior/.gsh/config.yaml
New target example -> https://gsh.example.com added to target list
mac301188:~ manoel.junior$ cat .gsh/config.yaml
targets:
example:
current: false
endpoint: https://gsh.example.com
gts:
current: true
endpoint: https://gsh.t.mdjunior.eng.br
mac301188:~ manoel.junior$

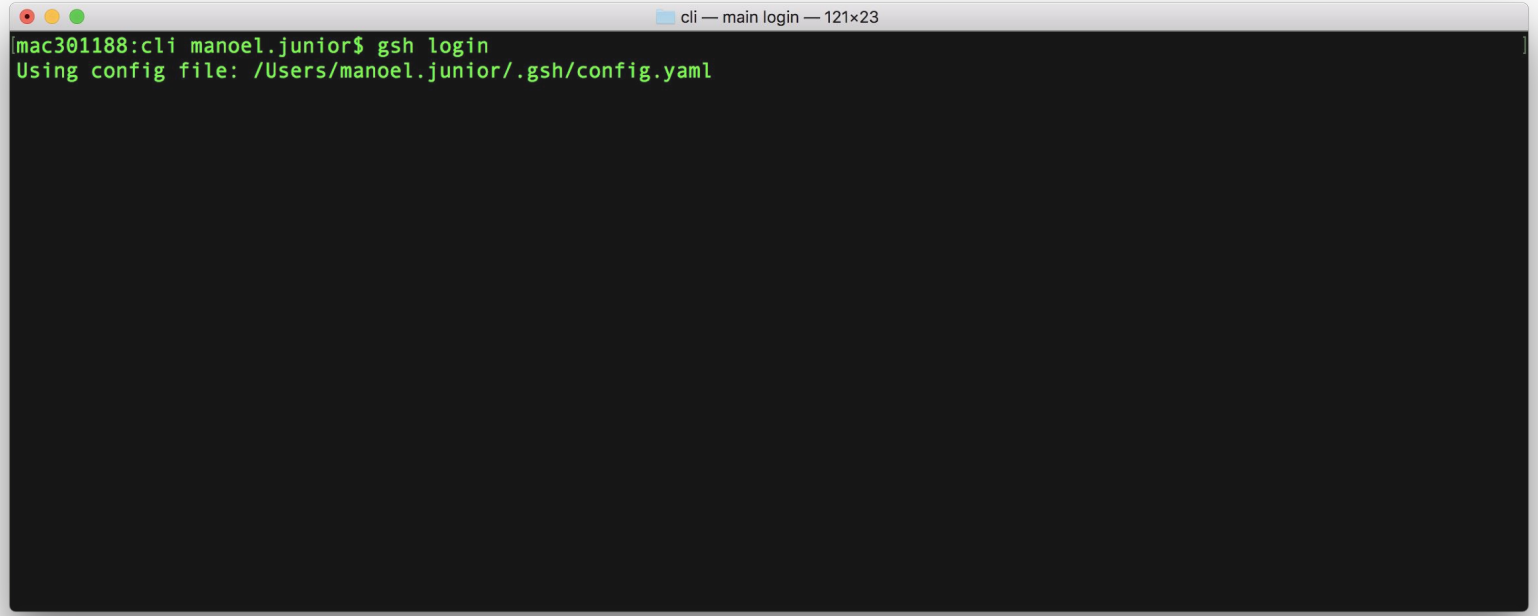
GSH


manoel.junior — -bash — 121×23
mac301188:~ manoel.junior$ gsh login -h
Initiates a new gsh session for a user. How authentication uses OpenID
Connect, it will open a web browser for the user to complete the login.
All gsh actions require the user to be authenticated (except [[gsh login]],
[[gsh version]] and [[gsh target-*]]).
Usage:
gsh login [flags]
Flags:
-h, --help help for login
-s, --set-token-storage string Define where OIDC tokens will be stored [keychain,kwallet,wincred,secret-service,file]
(default "keychain")
Global Flags:
--config string config file (default is $HOME/.gsh/config.yaml)
mac301188:~ manoel.junior$

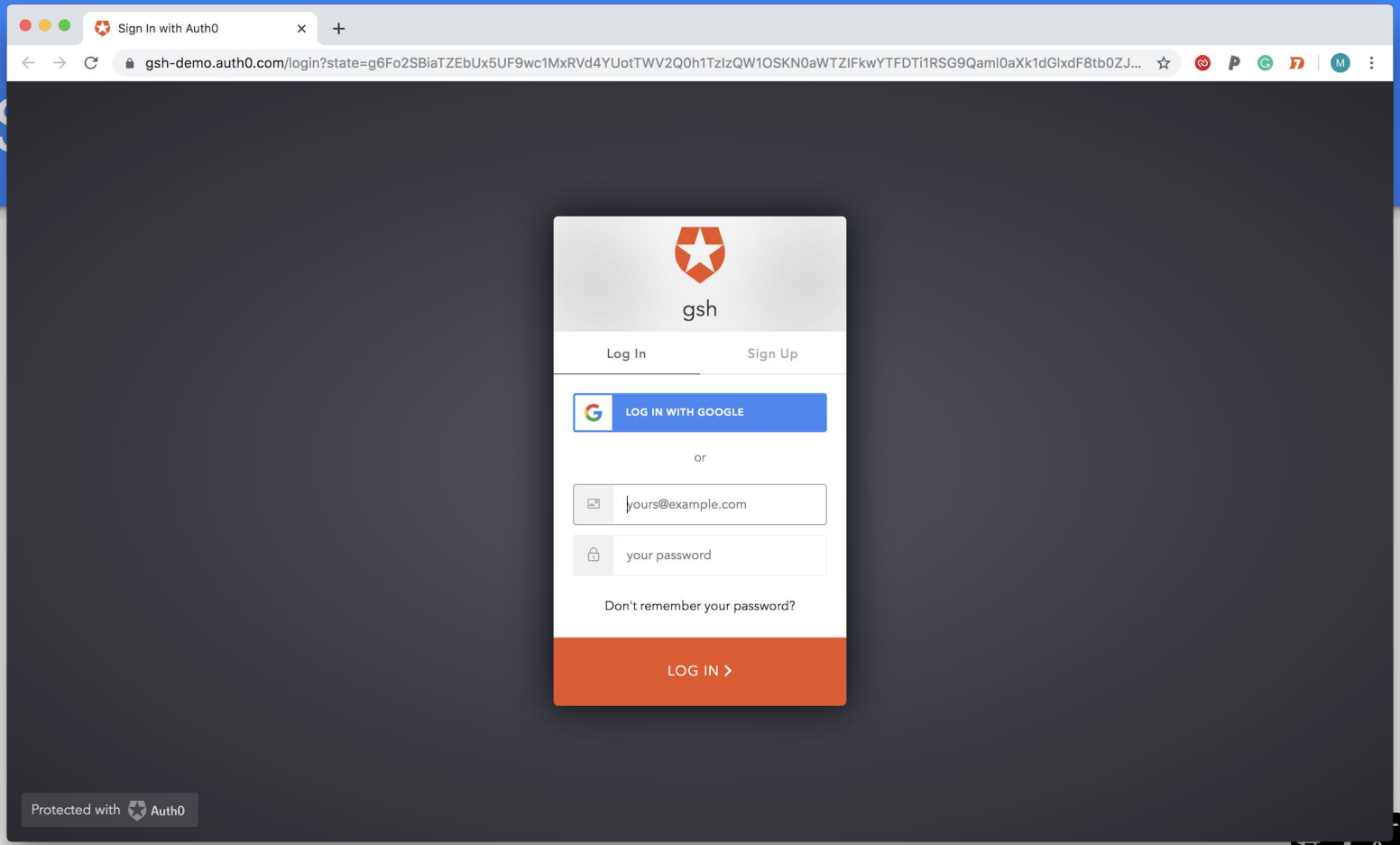
GSH


manoel.junior — -bash — 121×23
mac301188:~ manoel.junior$ gsh login -h
Initiates a new gsh session for a user. How authentication uses OpenID
Connect, it will open a web browser for the user to complete the login.
All gsh actions require the user to be authenticated (except [[gsh login]],
[[gsh version]] and [[gsh target-*]]).
Usage:
gsh login [flags]
Flags:
-h, --help help for login
-s, --set-token-storage string Define where OIDC tokens will be stored [keychain,kwallet,wincred,secret-service,file]
(default "keychain")
Global Flags:
--config string config file (default is $HOME/.gsh/config.yaml)
mac301188:~ manoel.junior$

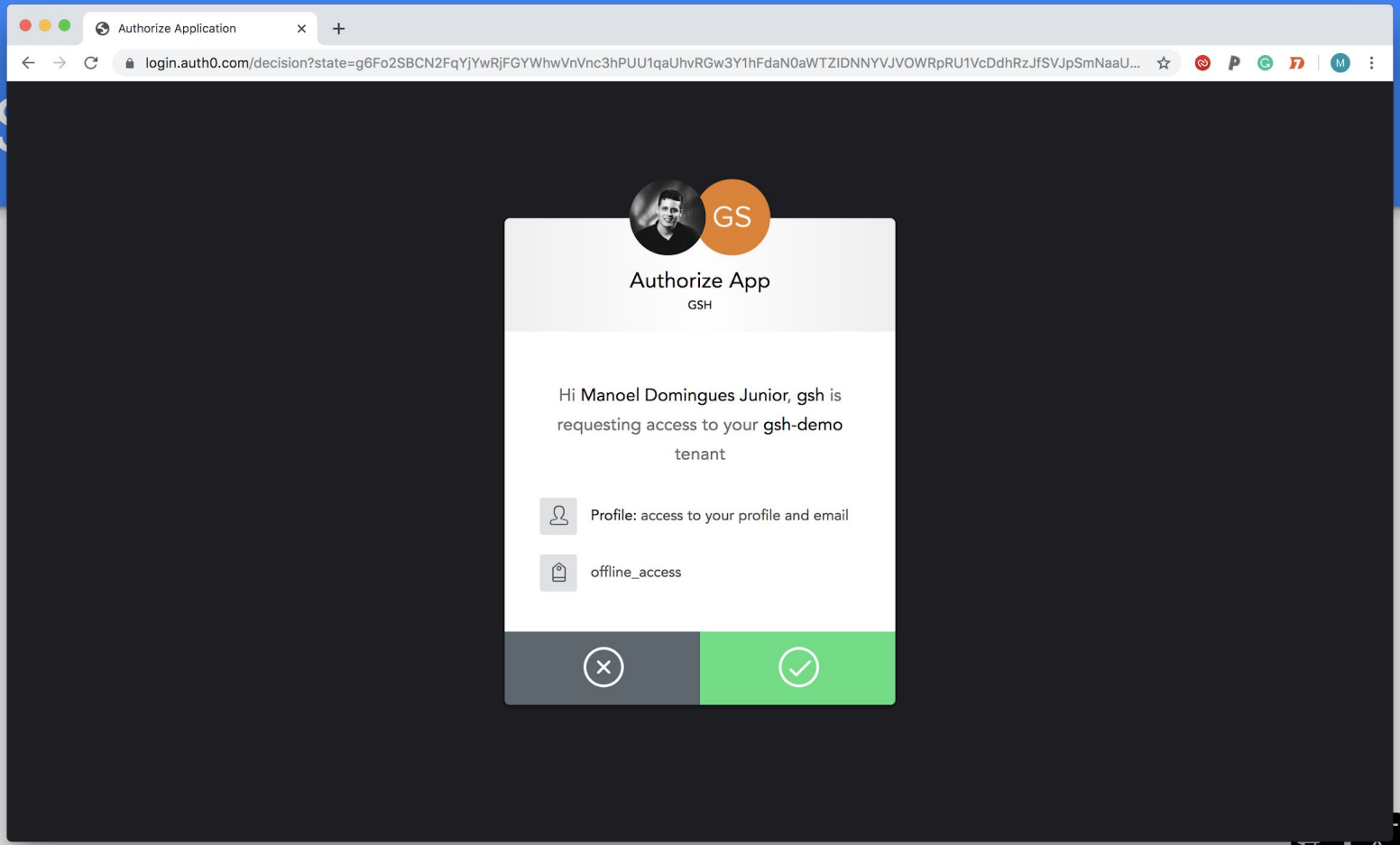
GSH

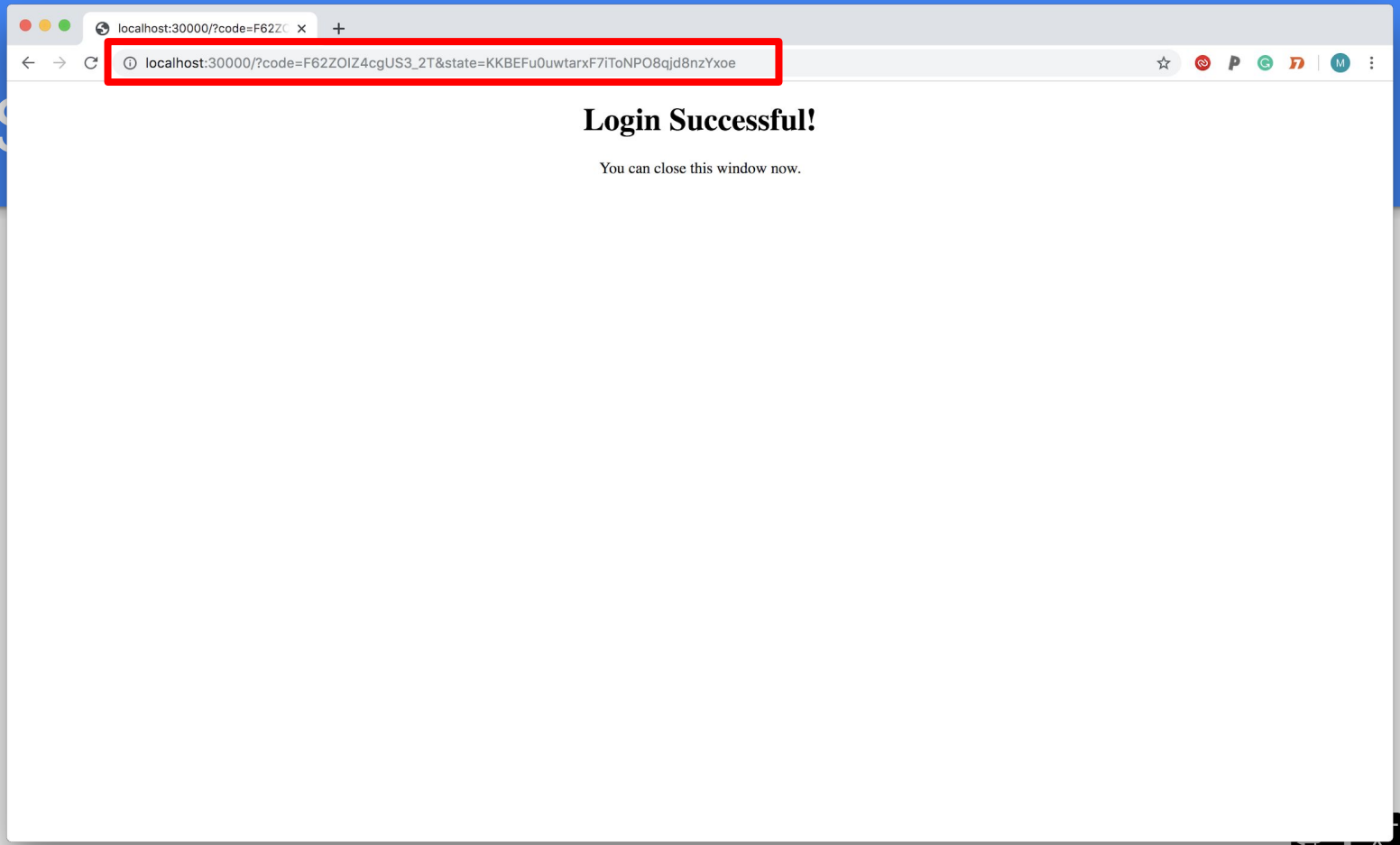

cli — main login — 121×23
mac301188:cli manoel.junior$ gsh login
Using config file: /Users/manoel.junior/.gsh/config.yaml

GS

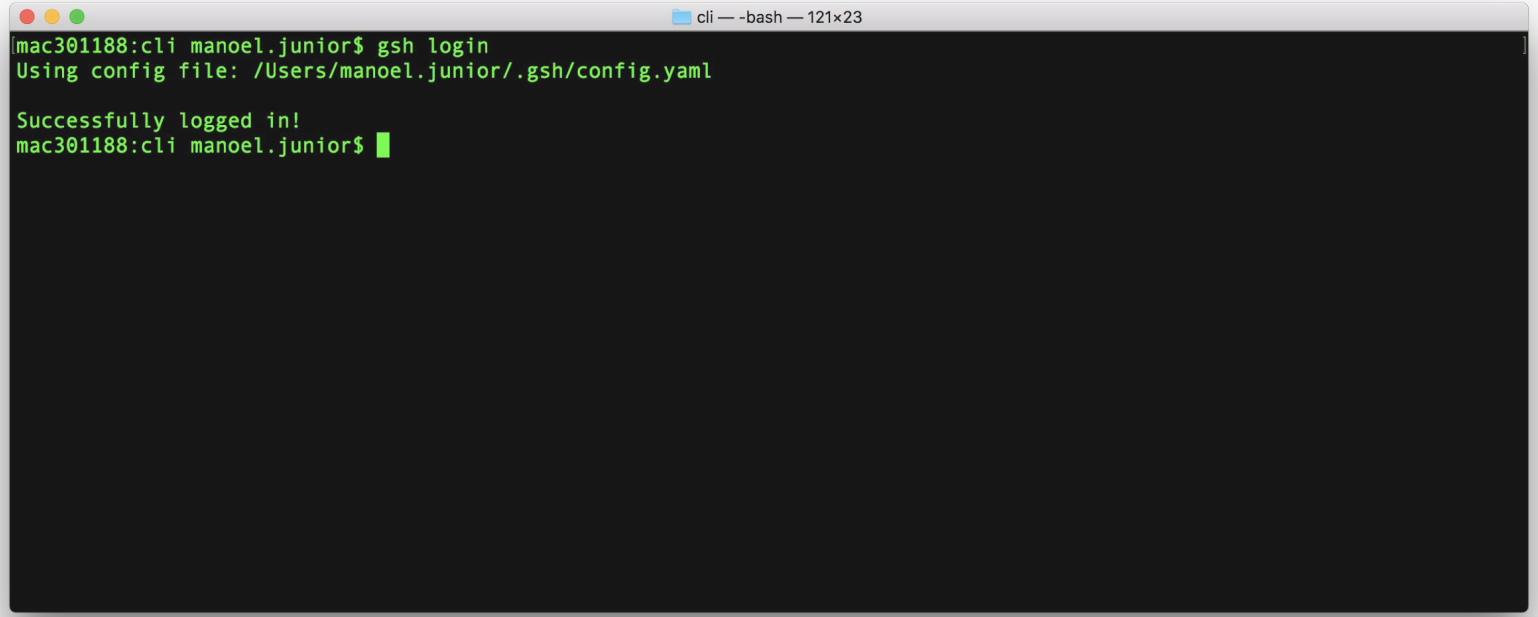

Sign In with Auth0
gsh-demo.auth0.com/login?state=g6Fo2SBiaTZEbUx5UF9wc1MxRVd4YUotTWV2Q0h1TzIzQW1OSKN0aWTZIFkwYTFDTi1RSG9Qaml0aXk1dGlxdF8tb0ZJ...
gsh
Log In
Sign Up
LOG IN WITH GOOGLE
or
yours@example.com
your password
Don't remember your password?
LOG IN
Protected with Auth0

GS


Authorize Application
login.auth0.com/decision?state=g6Fo2SBCN2FqYjYwRjFGYWhwVnVnc3hPUU1qaUhvRGw3Y1hFdaN0aWTZIDNNYVJVOWRpRU1VcDdhRzJfSVJpSmNaaU...
GS
Authorize App
GSH
Hi Manoel Domingues Junior, gsh is requesting access to your gsh-demo tenant
Profile: access to your profile and email
offline_access

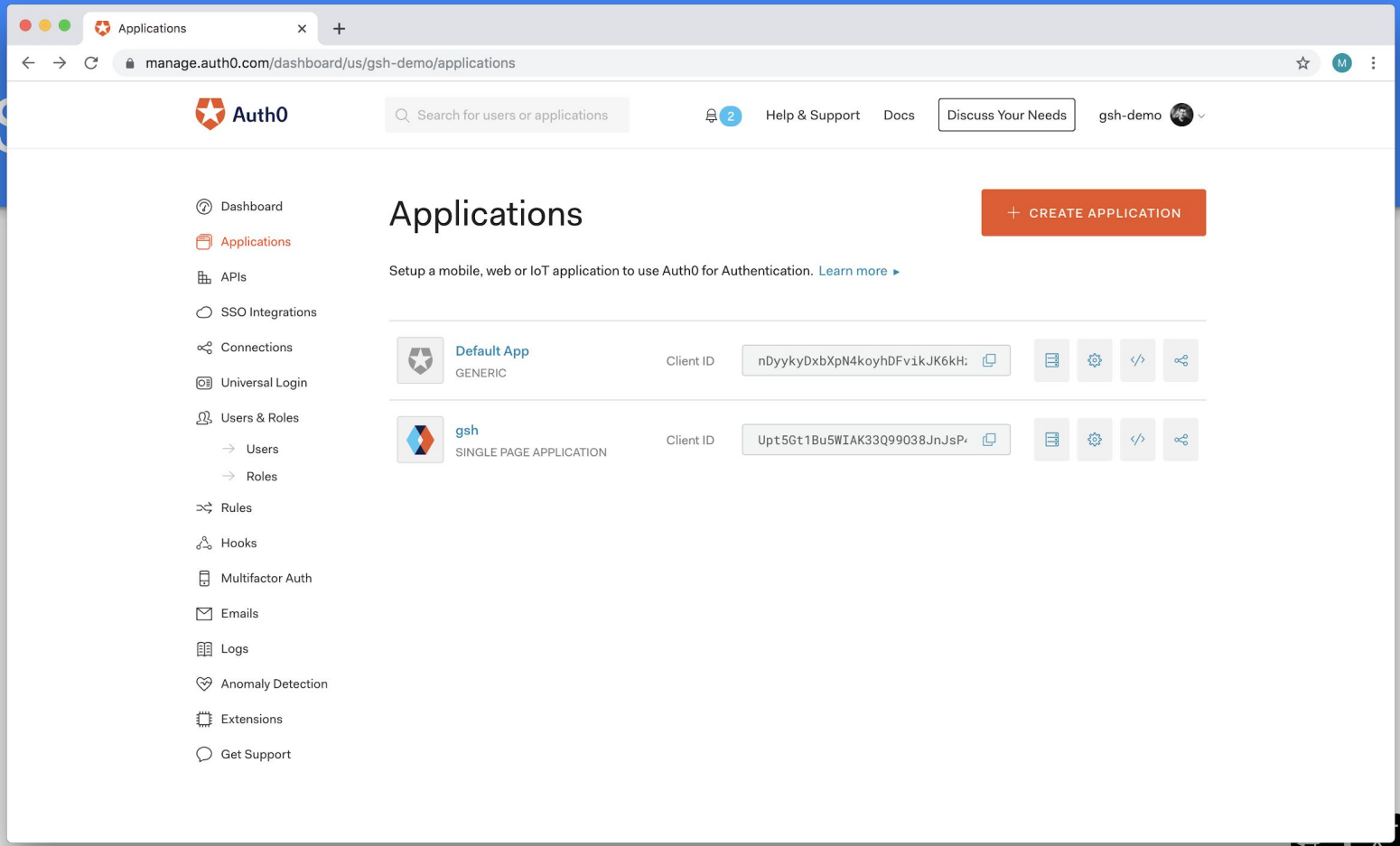

localhost:30000/?code=F62ZOIZ4cgUS3_2T&state=KKBEFu0uwtarxF7iTnPO8qjd8nzYxoe
Login Successful!
You can close this window now.

GSH

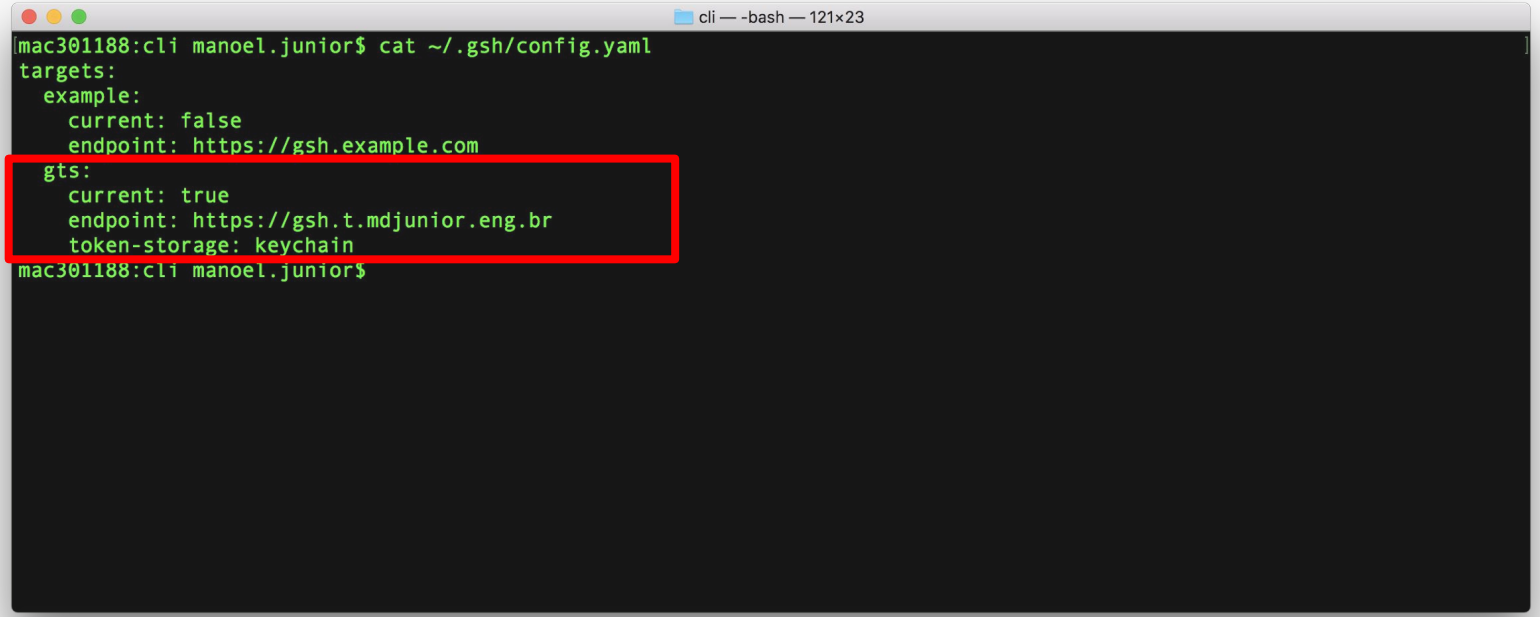

cli — -bash — 121×23
mac301188:cli manoel.junior$ gsh login
Using config file: /Users/manoel.junior/.gsh/config.yaml
Successfully logged in!
mac301188:cli manoel.junior$

GSH

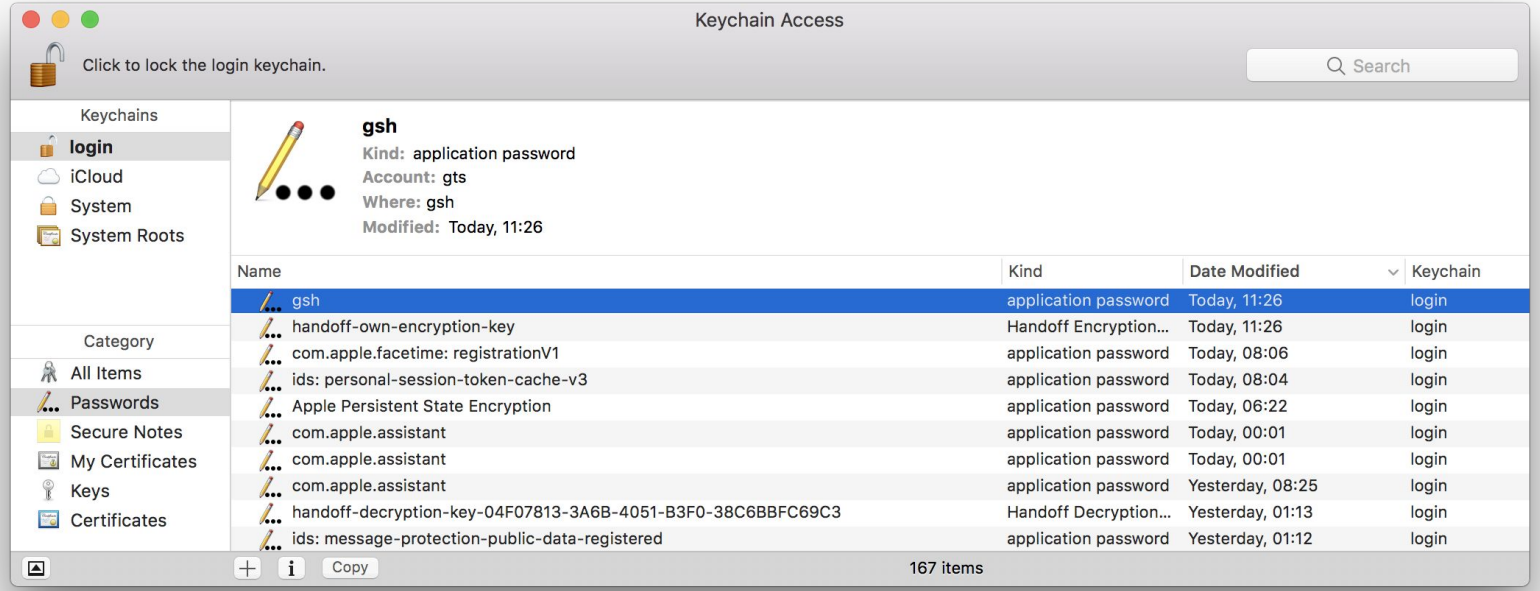
```
GET /status/config

HTTP/2 200
{
  "oidc_audience": "Upt5Gt1Bu5WIAK33Q99O38JnJsP4DDHk",
  "oidc_base_url": "https://gsh-demo.auth0.com",
  "oidc_callback_port": "30000",
  "oidc_certs": "https://gsh-demo.auth0.com/.well-known/jwks.json",
  "oidc_claim_name": "nickname",
  "oidc_issuer": "https://gsh-demo.auth0.com/"
}
```


Applications
manage.auth0.com/dashboard/us/gsh-demo/applications
Auth0
Search for users or applications
2
Help & Support
Docs
Discuss Your Needs
gsh-demo
Dashboard
Applications
APIs
SSO Integrations
Connections
Universal Login
Users & Roles
Users
Roles
Rules
Hooks
Multifactor Auth
Emails
Logs
Anomaly Detection
Extensions
Get Support
Applications
+ CREATE APPLICATION
Setup a mobile, web or IoT application to use Auth0 for Authentication. Learn more ▸
Default App
GENERIC
Client ID
nDyykyDxbXpN4koyhDFvikJK6kH
gsh
SINGLE PAGE APPLICATION
Client ID
Upt5Gt1Bu5WIAK33Q99O38JnJsP

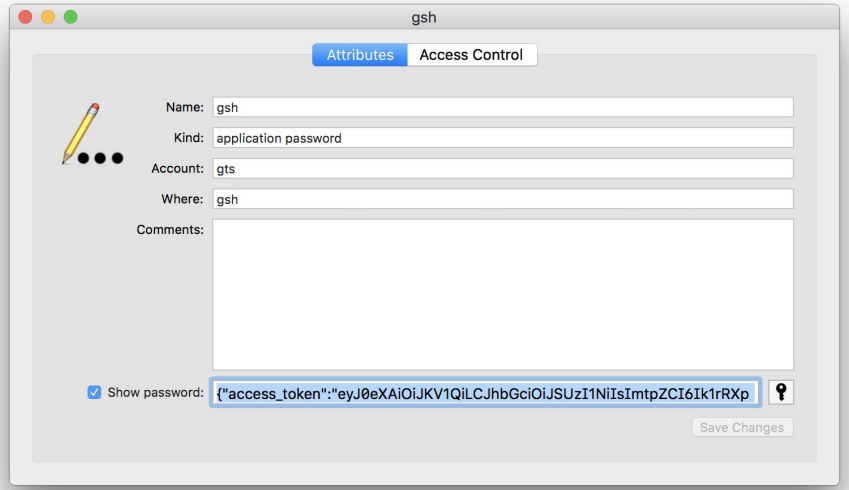
GSH

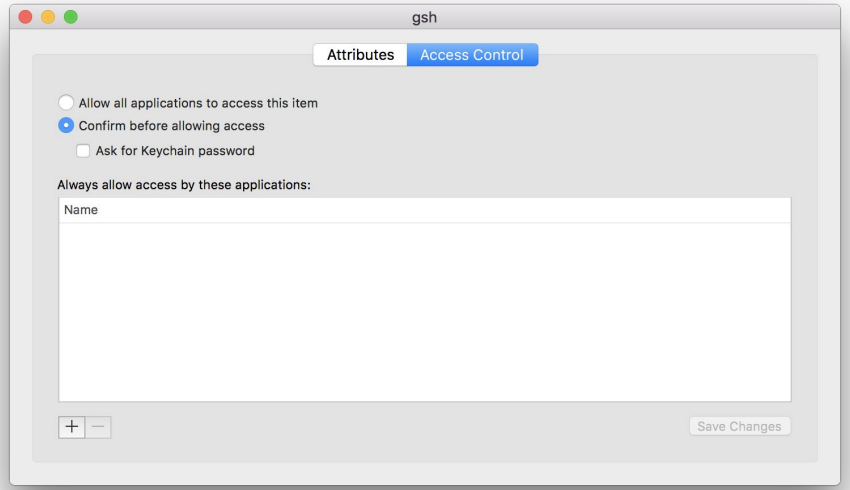

cli — -bash — 121×23
mac301188:cli manoel.junior$ cat ~/.gsh/config.yaml
targets:
  example:
    current: false
    endpoint: https://gsh.example.com
  gts:
    current: true
    endpoint: https://gsh.t.mdjunior.eng.br
    token-storage: keychain
mac301188:cli manoel.junior$

GSH

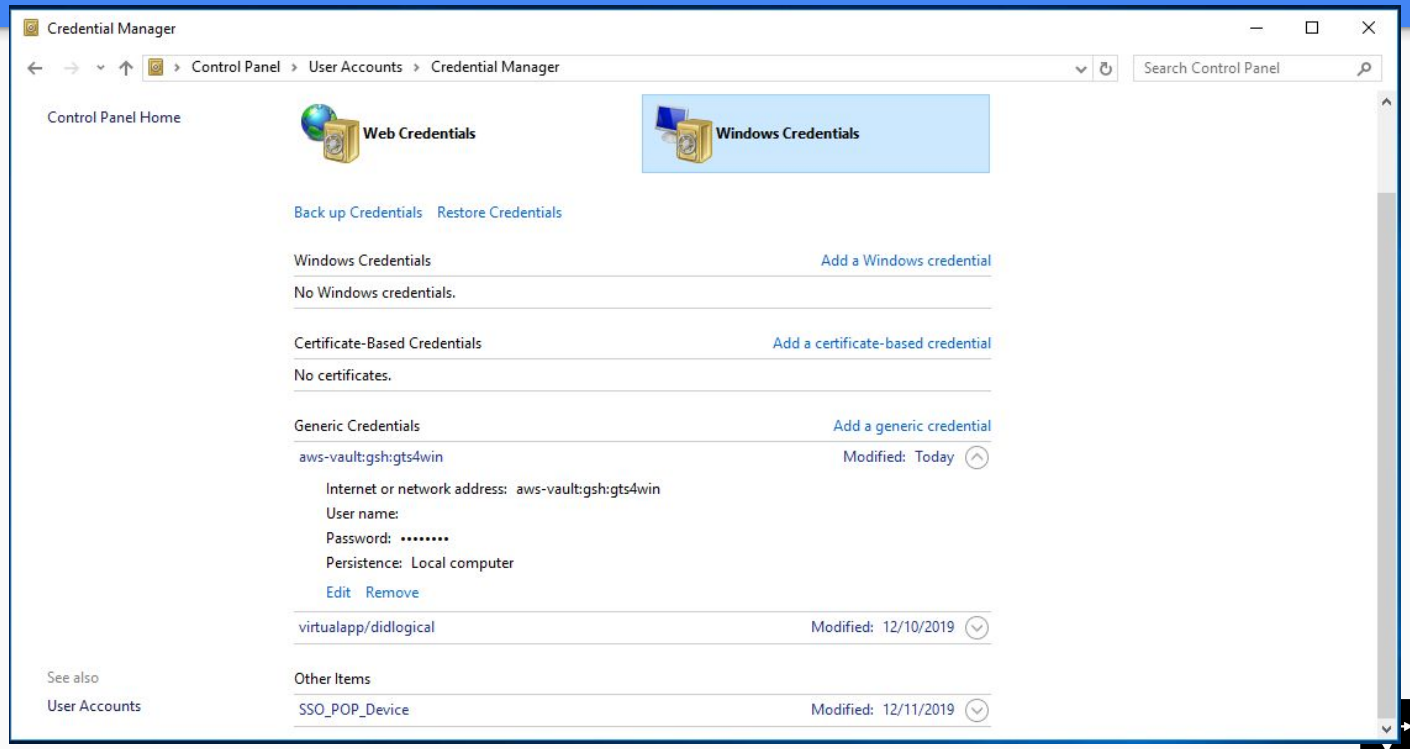

Keychain Access
Click to lock the login keychain.
Search
Keychains
login
iCloud
System
System Roots
Category
All Items
Passwords
Secure Notes
My Certificates
Keys
Certificates
gsh
Kind: application password
Account: gts
Where: gsh
Modified: Today, 11:26
Name
Kind
Date Modified
Keychain
gsh application password Today, 11:26 login
handoff-own-encryption-key Handoff Encryption... Today, 11:26 login
com.apple.facetime: registrationV1 application password Today, 08:06 login
ids: personal-session-token-cache-v3 application password Today, 08:04 login
Apple Persistent State Encryption application password Today, 06:22 login
com.apple.assistant application password Today, 00:01 login
com.apple.assistant application password Today, 00:01 login
com.apple.assistant application password Yesterday, 08:25 login
handoff-decryption-key-04F07813-3A6B-4051-B3F0-38C6BBFC69C3 Handoff Decryption... Yesterday, 01:13 login
ids: message-protection-public-data-registered application password Yesterday, 01:12 login
Copy
167 items

GSH

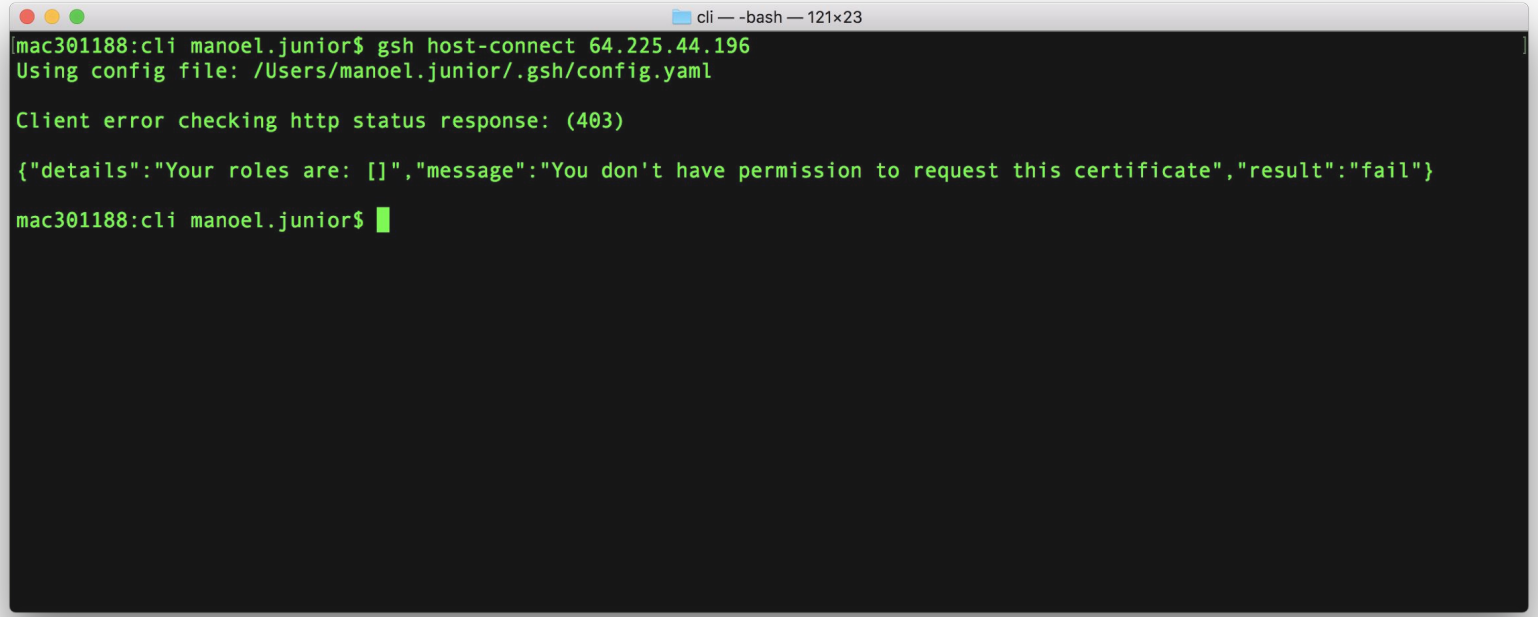

gsh
Attributes
Access Control
Name: gsh
Kind: application password
Account: gts
Where: gsh
Comments:
Show password:
{"access_token":"eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1NiIsImtpZCI6Ik1rRXp
Save Changes


gsh
Attributes
Access Control
Allow all applications to access this item
Confirm before allowing access
Ask for Keychain password
Always allow access by these applications:
Name
Save Changes

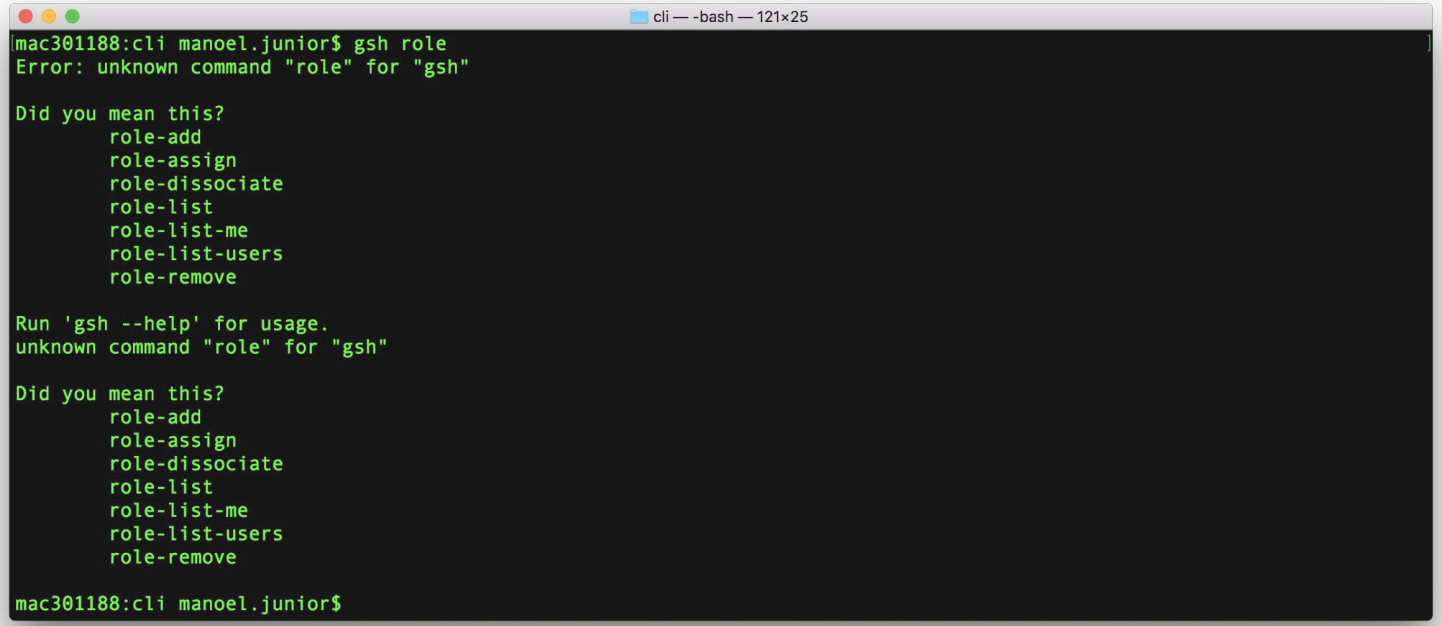
GSH


Credential Manager
Control Panel › User Accounts › Credential Manager
Search Control Panel
Control Panel Home
Web Credentials
Windows Credentials
Back up Credentials
Restore Credentials
Windows Credentials
Add a Windows credential
No Windows credentials.
Certificate-Based Credentials
Add a certificate-based credential
No certificates.
Generic Credentials
Add a generic credential
aws-vault:gsh:gts4win
Modified: Today
Internet or network address: aws-vault:gsh:gts4win
User name:
Password: ••••••••
Persistence: Local computer
Edit
Remove
virtualapp/didlogical
Modified: 12/10/2019
See also
User Accounts
Other Items
SSO_POP_Device
Modified: 12/11/2019

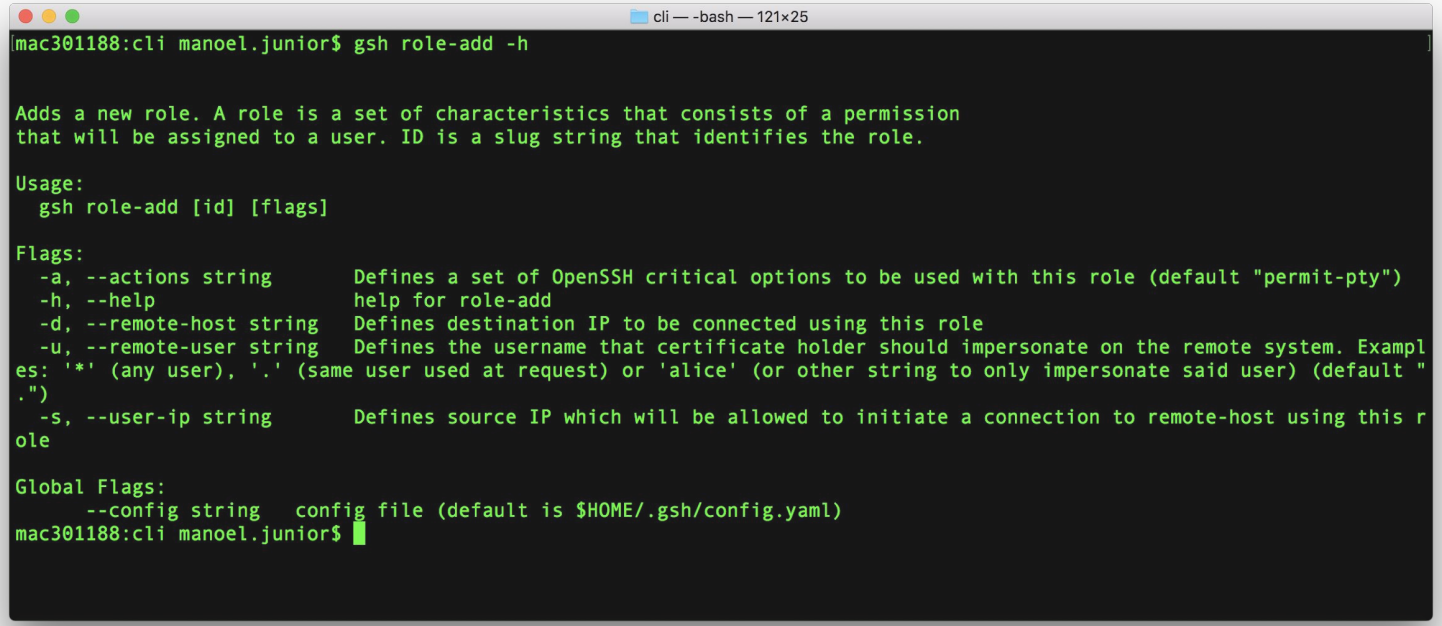
GSH


cli — -bash — 121×23
mac301188:cli manoel.junior$ gsh host-connect 64.225.44.196
Using config file: /Users/manoel.junior/.gsh/config.yaml
Client error checking http status response: (403)
{"details":"Your roles are: []","message":"You don't have permission to request this certificate","result":"fail"}
mac301188:cli manoel.junior$

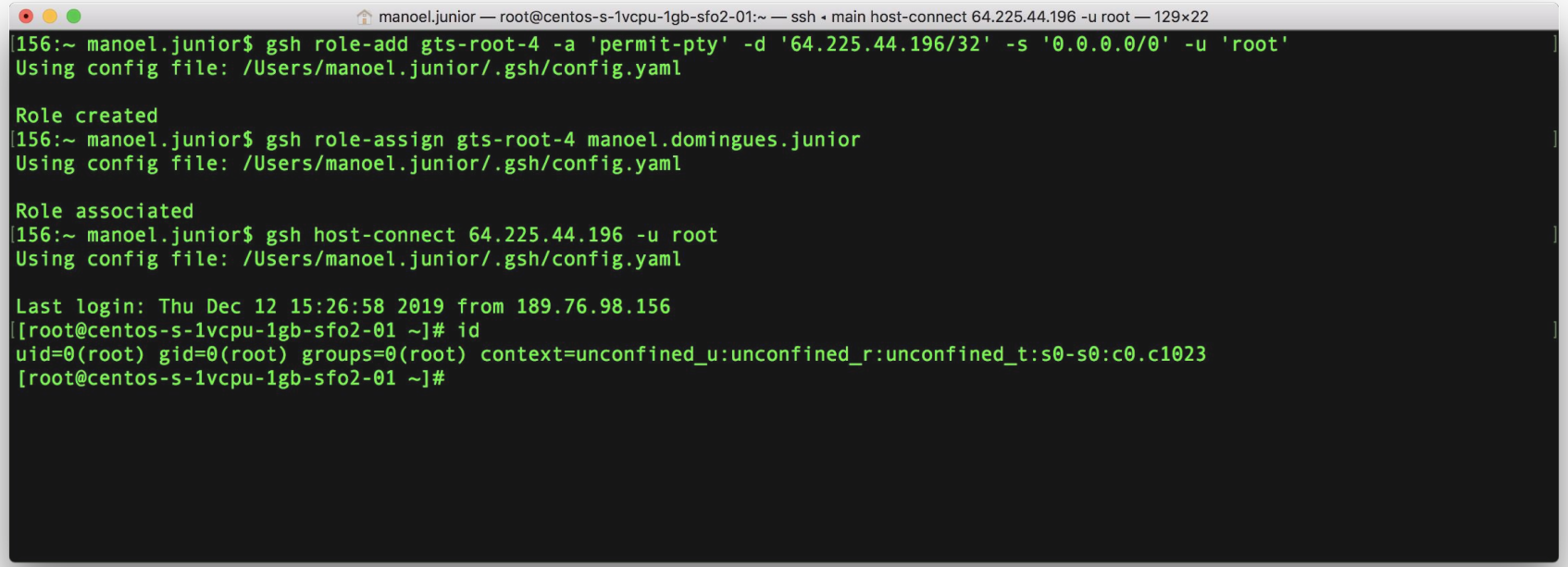
GSH


cli — -bash — 121×25
mac301188:cli manoel.junior$ gsh role
Error: unknown command "role" for "gsh"
Did you mean this?
role-add
role-assign
role-dissociate
role-list
role-list-me
role-list-users
role-remove
Run 'gsh --help' for usage.
unknown command "role" for "gsh"
Did you mean this?
role-add
role-assign
role-dissociate
role-list
role-list-me
role-list-users
role-remove
mac301188:cli manoel.junior$

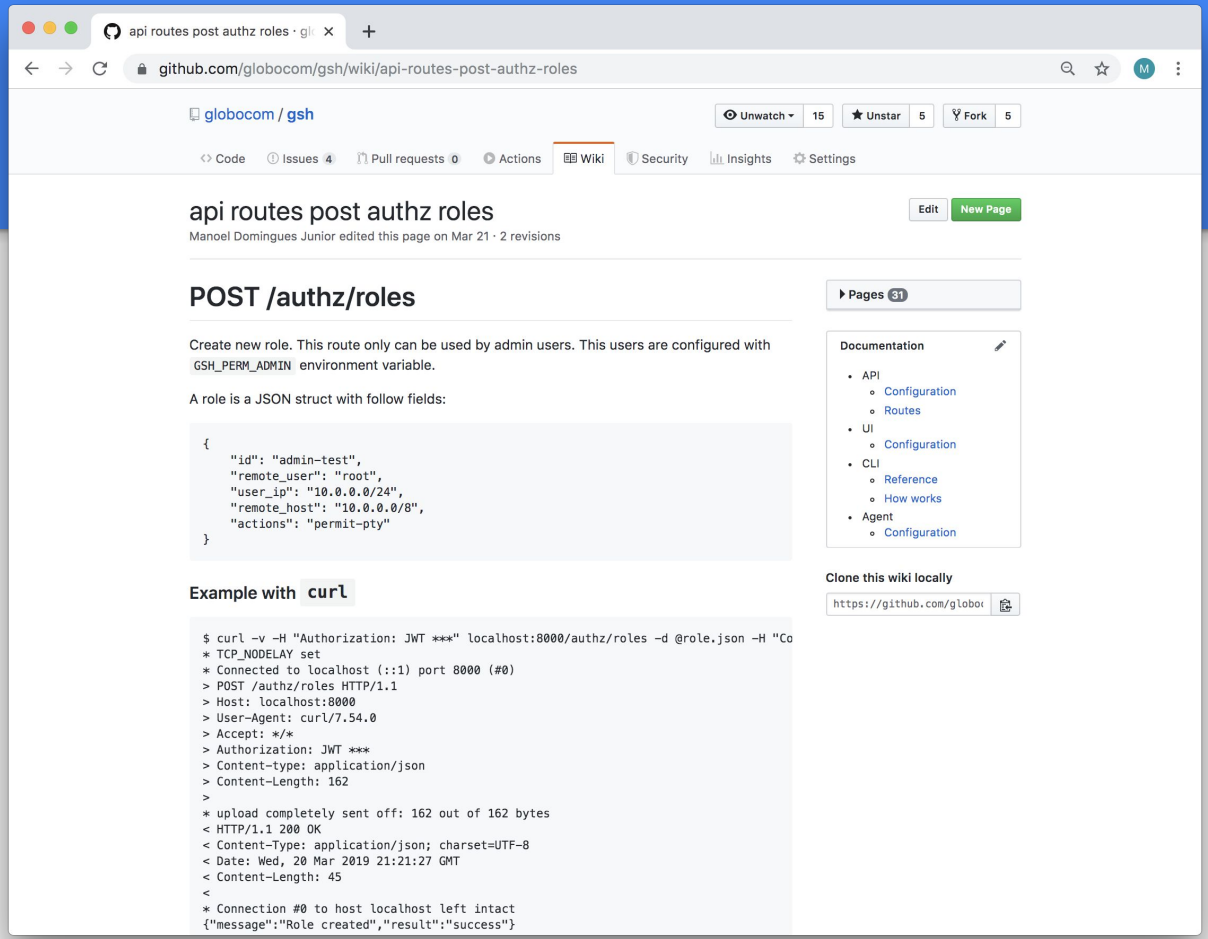
GSH


cli — -bash — 121×25
mac301188:cli manoel.junior$ gsh role-add -h
Adds a new role. A role is a set of characteristics that consists of a permission
that will be assigned to a user. ID is a slug string that identifies the role.
Usage:
gsh role-add [id] [flags]
Flags:
-a, --actions string Defines a set of OpenSSH critical options to be used with this role (default "permit-pty")
-h, --help help for role-add
-d, --remote-host string Defines destination IP to be connected using this role
-u, --remote-user string Defines the username that certificate holder should impersonate on the remote system. Exampl
es: '*' (any user), '.' (same user used at request) or 'alice' (or other string to only impersonate said user) (default "
.")
-s, --user-ip string Defines source IP which will be allowed to initiate a connection to remote-host using this r
ole
Global Flags:
--config string config file (default is $HOME/.gsh/config.yaml)
mac301188:cli manoel.junior$

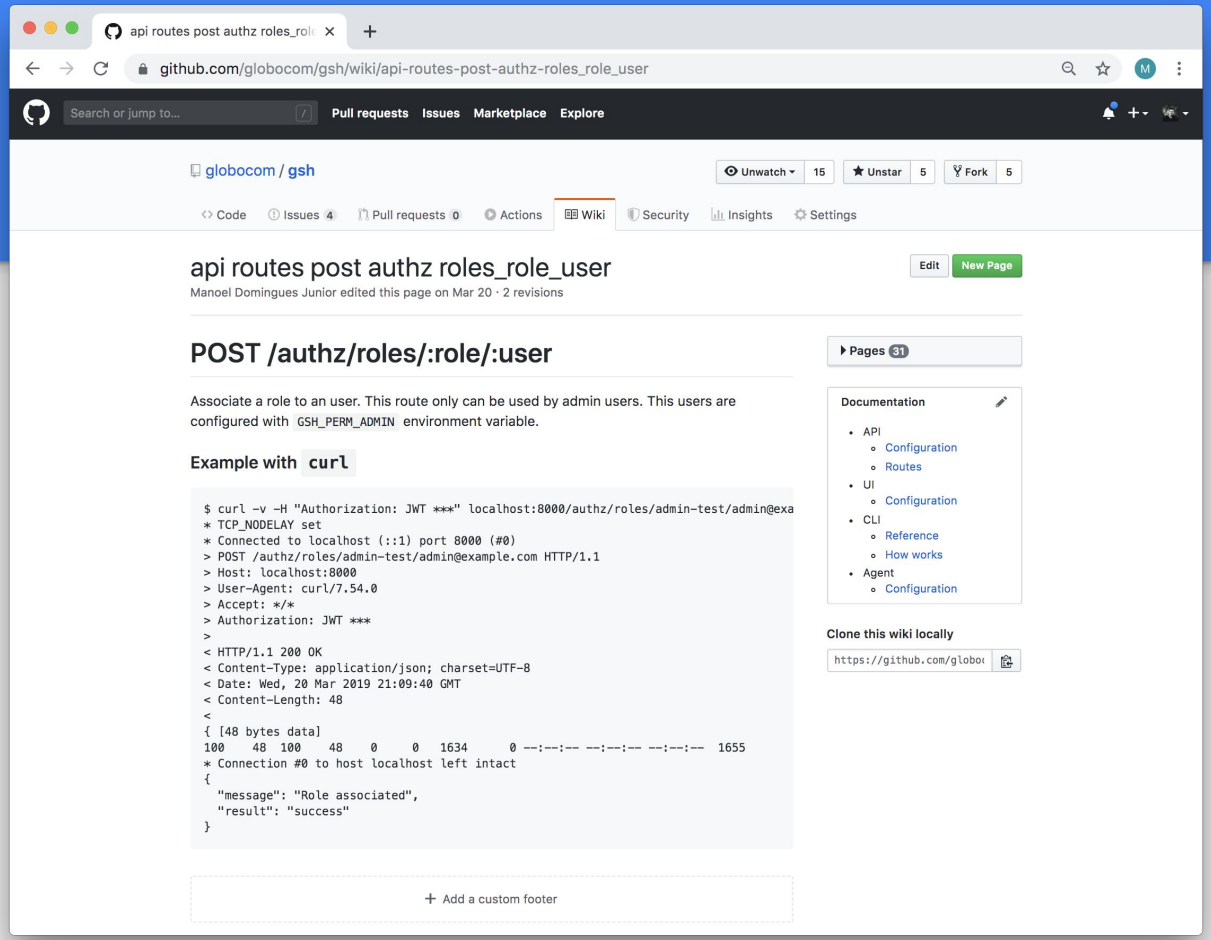
GSH


manoel.junior — root@centos-s-1vcpu-1gb-sfo2-01:~ — ssh • main host-connect 64.225.44.196 -u root — 129×22
156:~ manoel.junior$ gsh role-add gts-root-4 -a 'permit-pty' -d '64.225.44.196/32' -s '0.0.0.0/0' -u 'root'
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role created
156:~ manoel.junior$ gsh role-assign gts-root-4 manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role associated
156:~ manoel.junior$ gsh host-connect 64.225.44.196 -u root
Using config file: /Users/manoel.junior/.gsh/config.yaml
Last login: Thu Dec 12 15:26:58 2019 from 189.76.98.156
[root@centos-s-1vcpu-1gb-sfo2-01 ~]# id
uid=0(root) gid=0(root) groups=0(root) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[root@centos-s-1vcpu-1gb-sfo2-01 ~]#

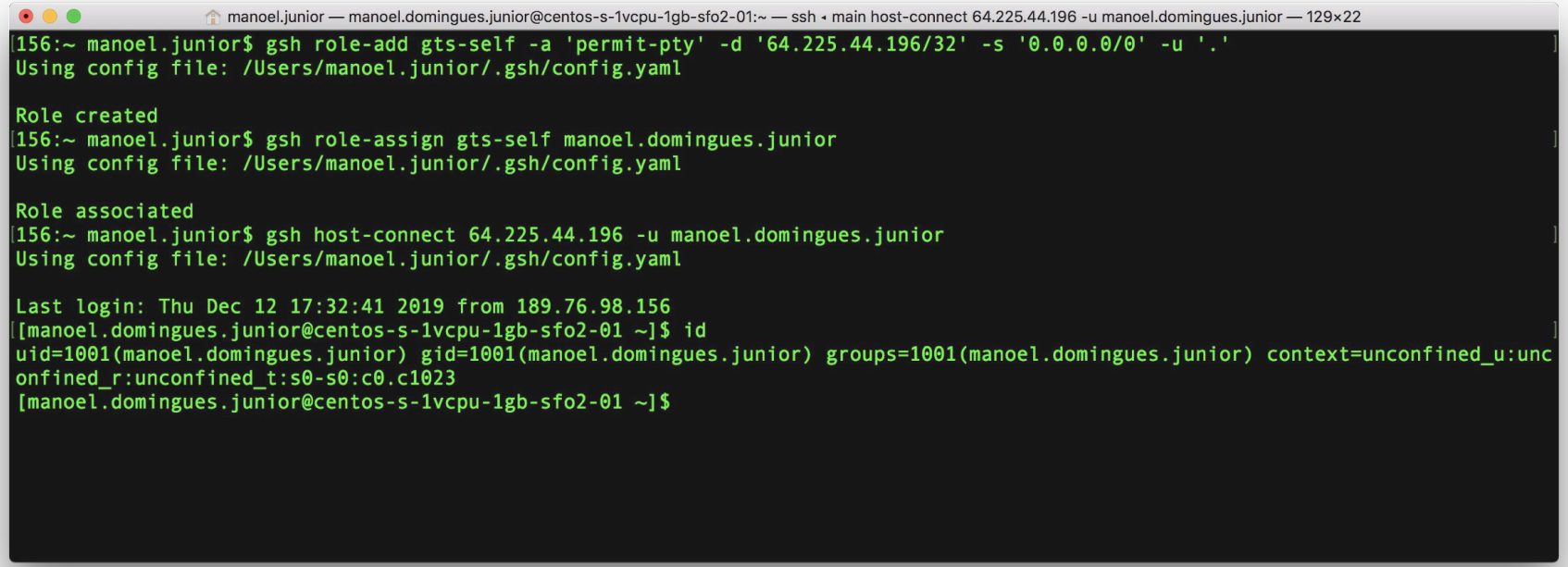
GSH


api routes post authz roles · gl
github.com/globocom/gsh/wiki/api-routes-post-authz-roles
globocom / gsh
Unwatch 15
Unstar 5
Fork 5
Code
Issues 4
Pull requests 0
Actions
Wiki
Security
Insights
Settings
api routes post authz roles
Manoel Domingues Junior edited this page on Mar 21 · 2 revisions
Edit
New Page
POST /authz/roles
Create new role. This route only can be used by admin users. This users are configured with GSH_PERM_ADMIN environment variable.
A role is a JSON struct with follow fields:
{
"id": "admin-test",
"remote_user": "root",
"user_ip": "10.0.0.0/24",
"remote_host": "10.0.0.0/8",
"actions": "permit-pty"
}
Example with curl
$ curl -v -H "Authorization: JWT ***" localhost:8000/authz/roles -d @role.json -H "Co
* TCP_NODELAY set
* Connected to localhost (::1) port 8000 (#0)
> POST /authz/roles HTTP/1.1
> Host: localhost:8000
> User-Agent: curl/7.54.0
> Accept: */*
> Authorization: JWT ***
> Content-type: application/json
> Content-Length: 162
>
* upload completely sent off: 162 out of 162 bytes
< HTTP/1.1 200 OK
< Content-Type: application/json; charset=UTF-8
< Date: Wed, 20 Mar 2019 21:21:27 GMT
< Content-Length: 45
<
* Connection #0 to host localhost left intact
{"message":"Role created","result":"success"}
Pages 31
Documentation
API
Configuration
Routes
UI
Configuration
CLI
Reference
How works
Agent
Configuration
Clone this wiki locally
https://github.com/globoc

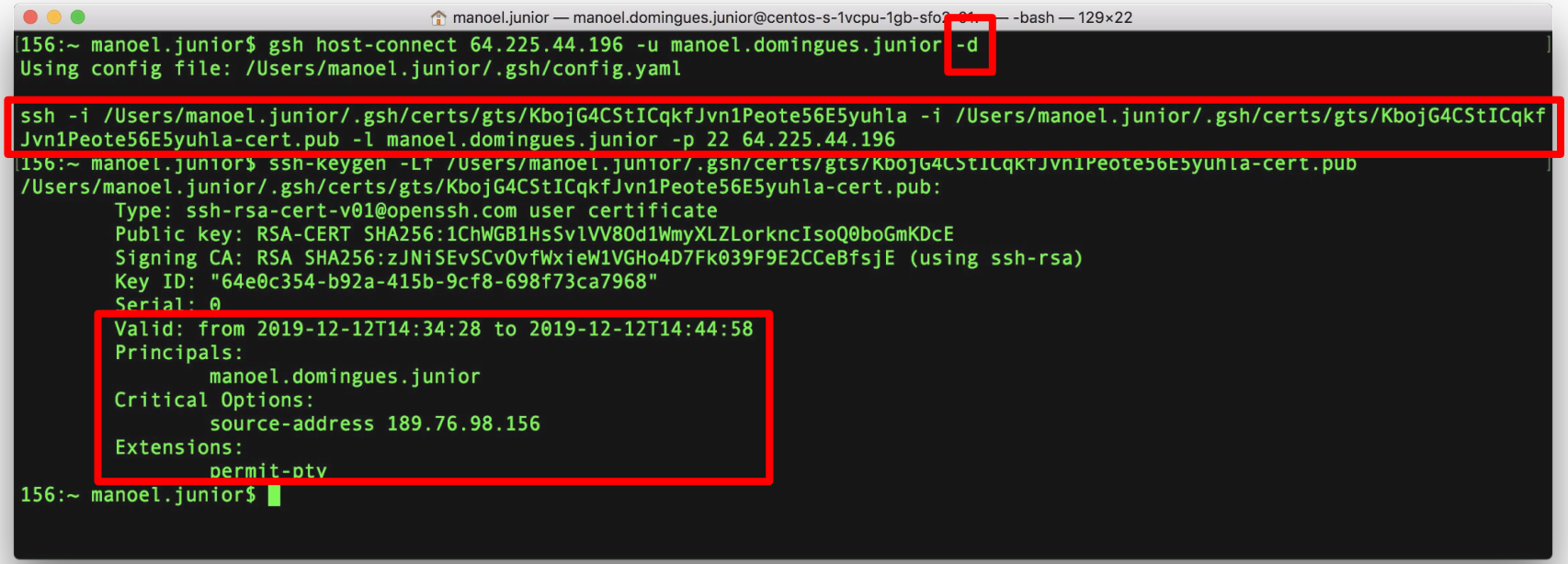
GSH


api routes post authz roles_role_user
github.com/globocom/gsh/wiki/api-routes-post-authz-roles_role_user
Search or jump to...
Pull requests
Issues
Marketplace
Explore
globocom / gsh
Unwatch 15
Unstar 5
Fork 5
Code
Issues 4
Pull requests 0
Actions
Wiki
Security
Insights
Settings
api routes post authz roles_role_user
Edit
New Page
Manoel Domingues Junior edited this page on Mar 20 · 2 revisions
POST /authz/roles/:role/:user
Associate a role to an user. This route only can be used by admin users. This users are configured with GSH_PERM_ADMIN environment variable.
Example with curl
$ curl -v -H "Authorization: JWT ***" localhost:8000/authz/roles/admin-test/admin@exa
* TCP_NODELAY set
* Connected to localhost (::1) port 8000 (#0)
> POST /authz/roles/admin-test/admin@example.com HTTP/1.1
> Host: localhost:8000
> User-Agent: curl/7.54.0
> Accept: */*
> Authorization: JWT ***
>
< HTTP/1.1 200 OK
< Content-Type: application/json; charset=UTF-8
< Date: Wed, 20 Mar 2019 21:09:40 GMT
< Content-Length: 48
<
{ [48 bytes data]
100 48 100 48 0 0 1634 0 --:--:-- --:--:-- --:--:-- 1655
* Connection #0 to host localhost left intact
{
"message": "Role associated",
"result": "success"
}
Add a custom footer
Pages 31
Documentation
API
Configuration
Routes
UI
Configuration
CLI
Reference
How works
Agent
Configuration
Clone this wiki locally
https://github.com/globoc

GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — ssh ◂ main host-connect 64.225.44.196 -u manoel.domingues.junior — 129×22
156:~ manoel.junior$ gsh role-add gts-self -a 'permit-pty' -d '64.225.44.196/32' -s '0.0.0.0/0' -u '.'
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role created
156:~ manoel.junior$ gsh role-assign gts-self manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role associated
156:~ manoel.junior$ gsh host-connect 64.225.44.196 -u manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
Last login: Thu Dec 12 17:32:41 2019 from 189.76.98.156
[manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01 ~]$ id
uid=1001(manoel.domingues.junior) gid=1001(manoel.domingues.junior) groups=1001(manoel.domingues.junior) context=unconfined_u:unconfined_r:unconfined_t:s0-s0:c0.c1023
[manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01 ~]$

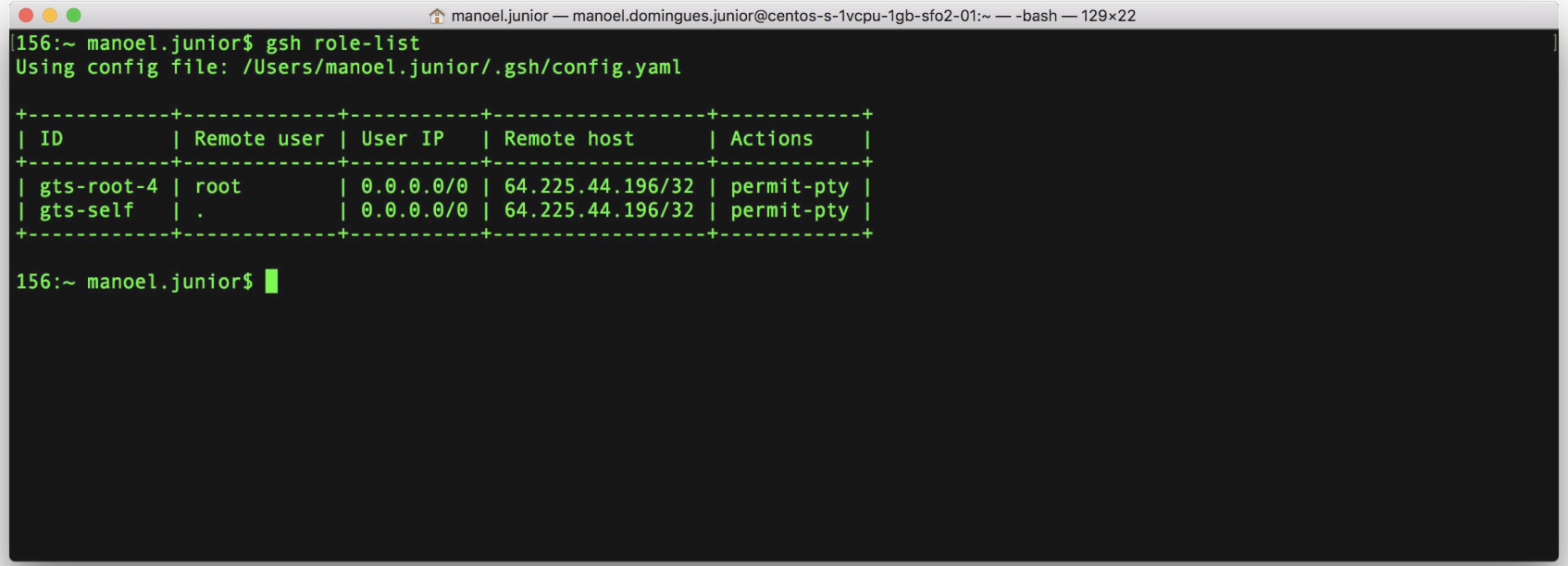
GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01: — -bash — 129×22
156:~ manoel.junior$ gsh host-connect 64.225.44.196 -u manoel.domingues.junior -d
Using config file: /Users/manoel.junior/.gsh/config.yaml
ssh -i /Users/manoel.junior/.gsh/certs/gts/KbojG4CStICqkfJvn1Peote56E5yuhla -i /Users/manoel.junior/.gsh/certs/gts/KbojG4CStICqkfJvn1Peote56E5yuhla-cert.pub -l manoel.domingues.junior -p 22 64.225.44.196
156:~ manoel.junior$ ssh-keygen -Lf /Users/manoel.junior/.gsh/certs/gts/KbojG4CStICqkfJvn1Peote56E5yuhla-cert.pub
/Users/manoel.junior/.gsh/certs/gts/KbojG4CStICqkfJvn1Peote56E5yuhla-cert.pub:
Type: ssh-rsa-cert-v01@openssh.com user certificate
Public key: RSA-CERT SHA256:1ChWGB1HsSvlVV8Od1WmyXLZLorkncIsoQ0boGmKDcE
Signing CA: RSA SHA256:zJNiSEvSCvOvfWxieW1VGHo4D7Fk039F9E2CCeBfsjE (using ssh-rsa)
Key ID: "64e0c354-b92a-415b-9cf8-698f73ca7968"
Serial: 0
Valid: from 2019-12-12T14:34:28 to 2019-12-12T14:44:58
Principals:
manoel.domingues.junior
Critical Options:
source-address 189.76.98.156
Extensions:
permit-pty
156:~ manoel.junior$

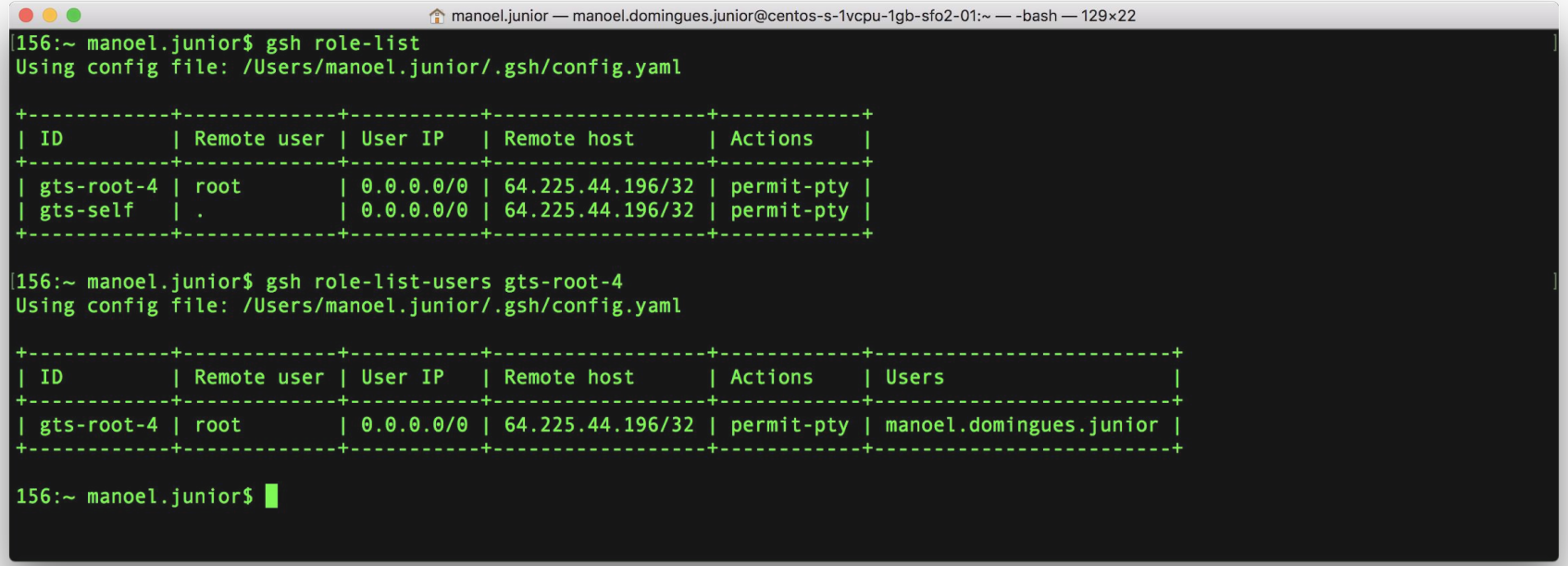
GSH

```
Dec 12 17:21:54 centos-s-1vcpu-1gb-sfo2-01 sshd[9602]: reverse mapping checking getaddrinfo for
186-192-87-8.prt.globo.com [186.192.87.8] failed - POSSIBLE BREAK-IN ATTEMPT!
Dec 12 17:21:55 centos-s-1vcpu-1gb-sfo2-01 sshd[9602]: Authentication tried for manoel.domingues.junior with
valid certificate but not from a permitted host (ip=186.192.87.8).
Dec 12 17:21:55 centos-s-1vcpu-1gb-sfo2-01 sshd[9602]: error: invalid certificate options
Dec 12 17:21:55 centos-s-1vcpu-1gb-sfo2-01 sshd[9602]: Connection closed by 186.192.87.8 port 20302 [preauth]
```

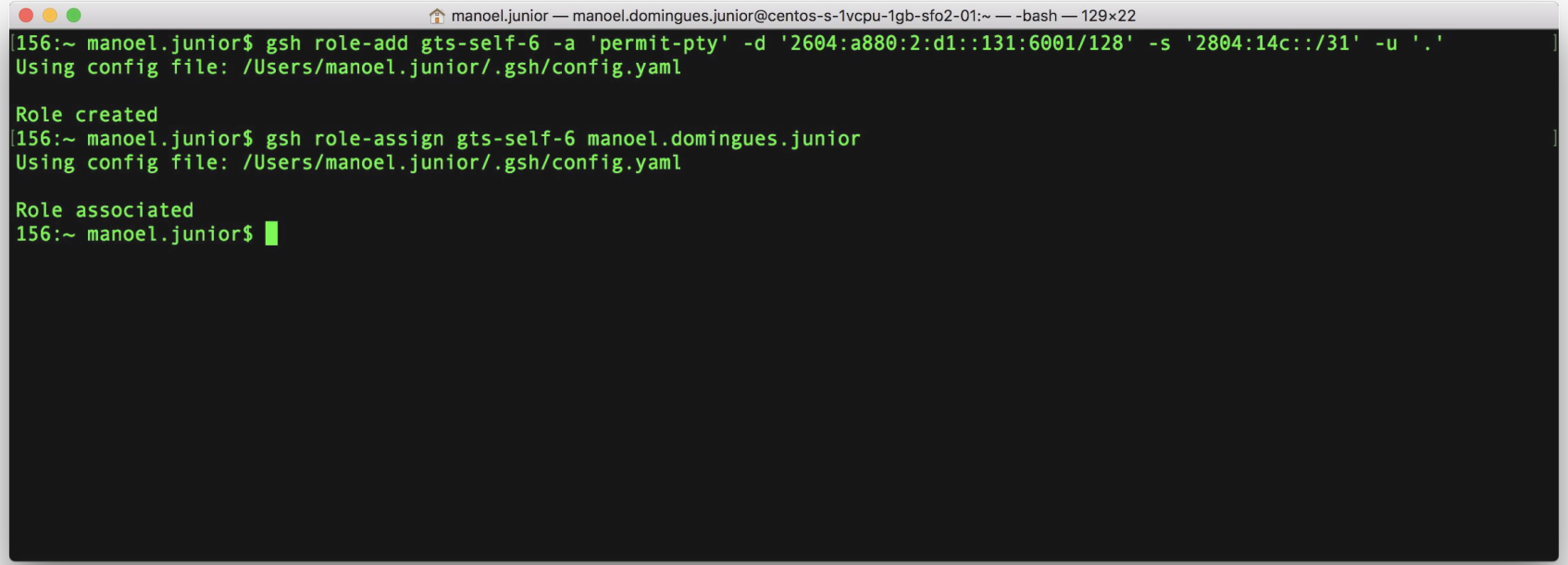
GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 129×22
156:~ manoel.junior$ gsh role-list
Using config file: /Users/manoel.junior/.gsh/config.yaml
+------------+-------------+-----------+------------------+------------+
| ID | Remote user | User IP | Remote host | Actions |
+------------+-------------+-----------+------------------+------------+
| gts-root-4 | root | 0.0.0.0/0 | 64.225.44.196/32 | permit-pty |
| gts-self | . | 0.0.0.0/0 | 64.225.44.196/32 | permit-pty |
+------------+-------------+-----------+------------------+------------+
156:~ manoel.junior$

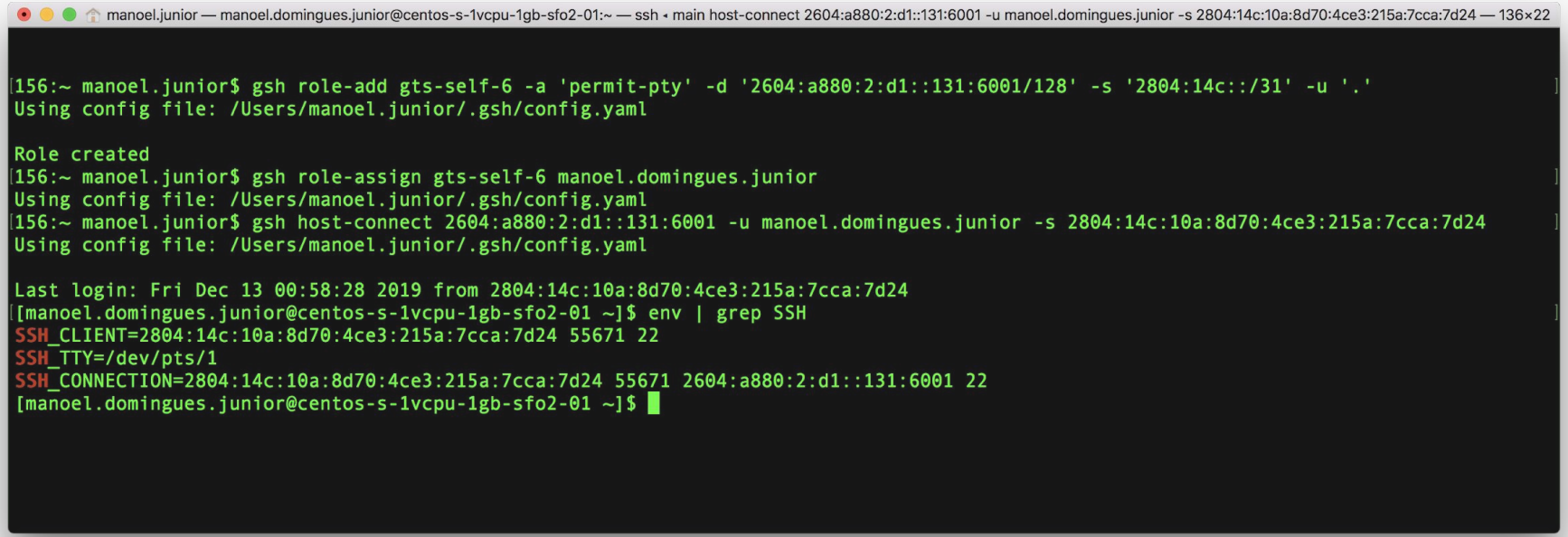
GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 129×22
156:~ manoel.junior$ gsh role-list
Using config file: /Users/manoel.junior/.gsh/config.yaml
ID	Remote user	User IP	Remote host	Actions
gts-root-4	root	0.0.0.0/0	64.225.44.196/32	permit-pty
gts-self	.	0.0.0.0/0	64.225.44.196/32	permit-pty
156:~ manoel.junior$ gsh role-list-users gts-root-4
Using config file: /Users/manoel.junior/.gsh/config.yaml
ID	Remote user	User IP	Remote host	Actions	Users
gts-root-4	root	0.0.0.0/0	64.225.44.196/32	permit-pty	manoel.domingues.junior
156:~ manoel.junior$

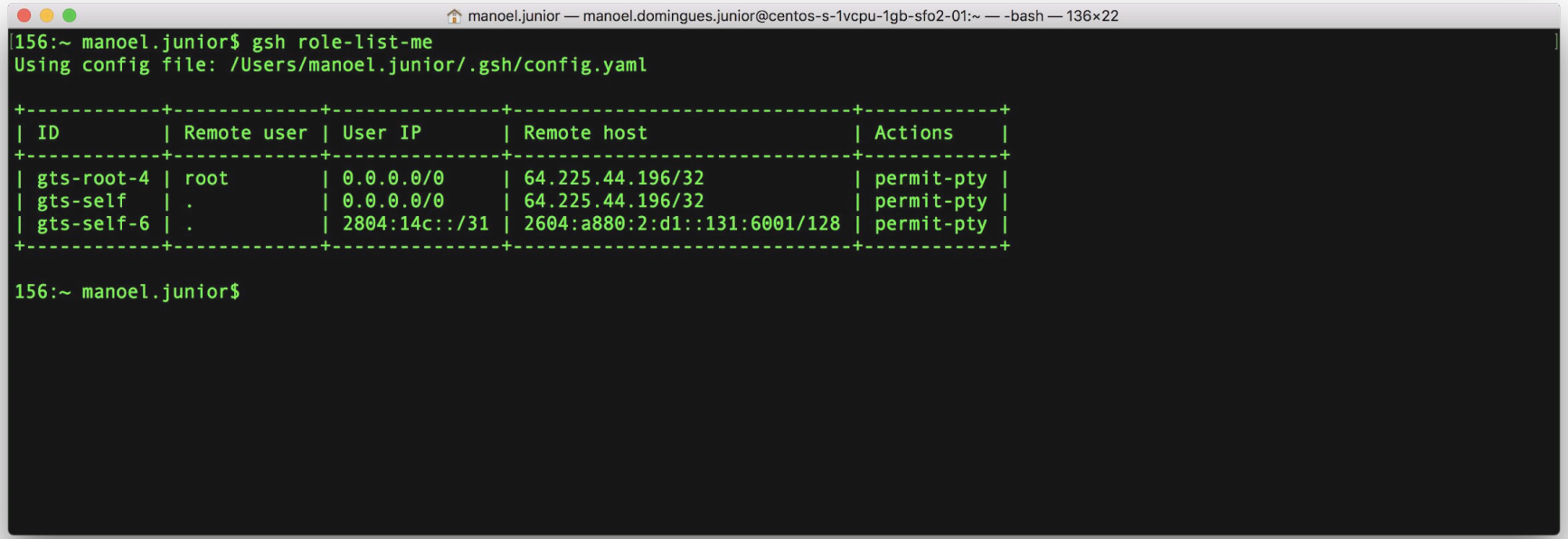
GSH - ipv6?


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 129×22
156:~ manoel.junior$ gsh role-add gts-self-6 -a 'permit-pty' -d '2604:a880:2:d1::131:6001/128' -s '2804:14c::/31' -u '.'
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role created
156:~ manoel.junior$ gsh role-assign gts-self-6 manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role associated
156:~ manoel.junior$

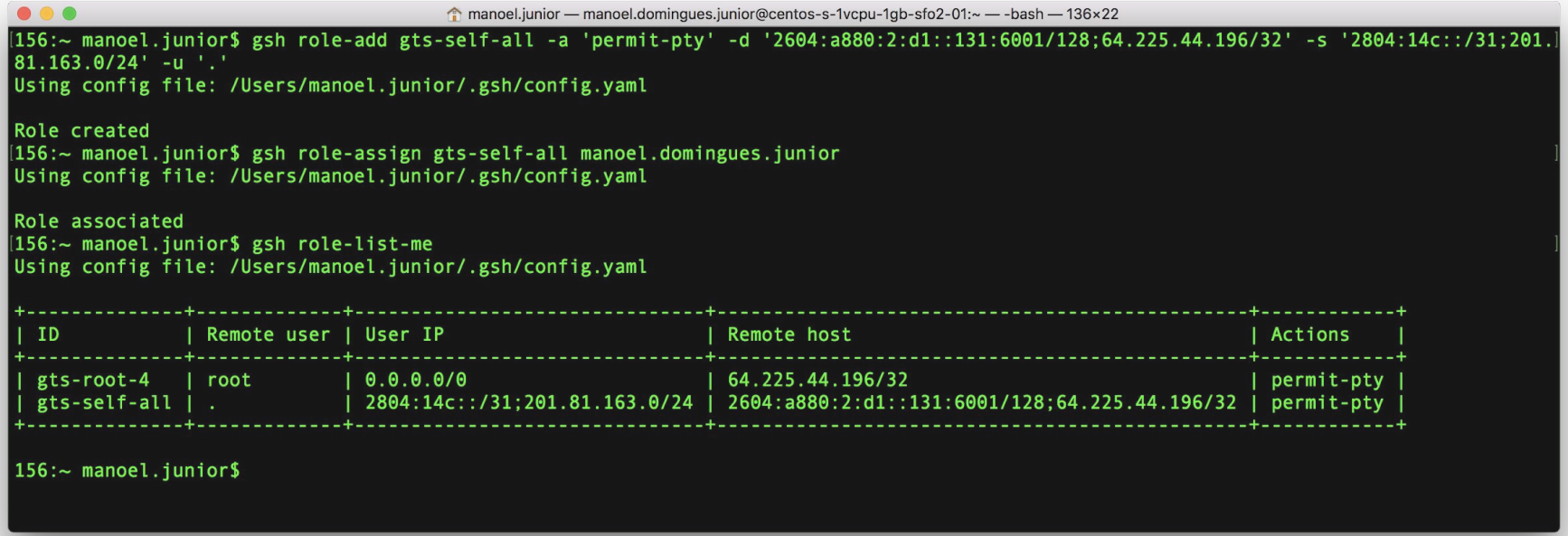
GSH - ipv6?


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — ssh ◂ main host-connect 2604:a880:2:d1::131:6001 -u manoel.domingues.junior -s 2804:14c:10a:8d70:4ce3:215a:7cca:7d24 — 136×22
156:~ manoel.junior$ gsh role-add gts-self-6 -a 'permit-pty' -d '2604:a880:2:d1::131:6001/128' -s '2804:14c::/31' -u '.'
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role created
156:~ manoel.junior$ gsh role-assign gts-self-6 manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
156:~ manoel.junior$ gsh host-connect 2604:a880:2:d1::131:6001 -u manoel.domingues.junior -s 2804:14c:10a:8d70:4ce3:215a:7cca:7d24
Using config file: /Users/manoel.junior/.gsh/config.yaml
Last login: Fri Dec 13 00:58:28 2019 from 2804:14c:10a:8d70:4ce3:215a:7cca:7d24
[manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01 ~]$ env | grep SSH
SSH_CLIENT=2804:14c:10a:8d70:4ce3:215a:7cca:7d24 55671 22
SSH_TTY=/dev/pts/1
SSH_CONNECTION=2804:14c:10a:8d70:4ce3:215a:7cca:7d24 55671 2604:a880:2:d1::131:6001 22
[manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01 ~]$

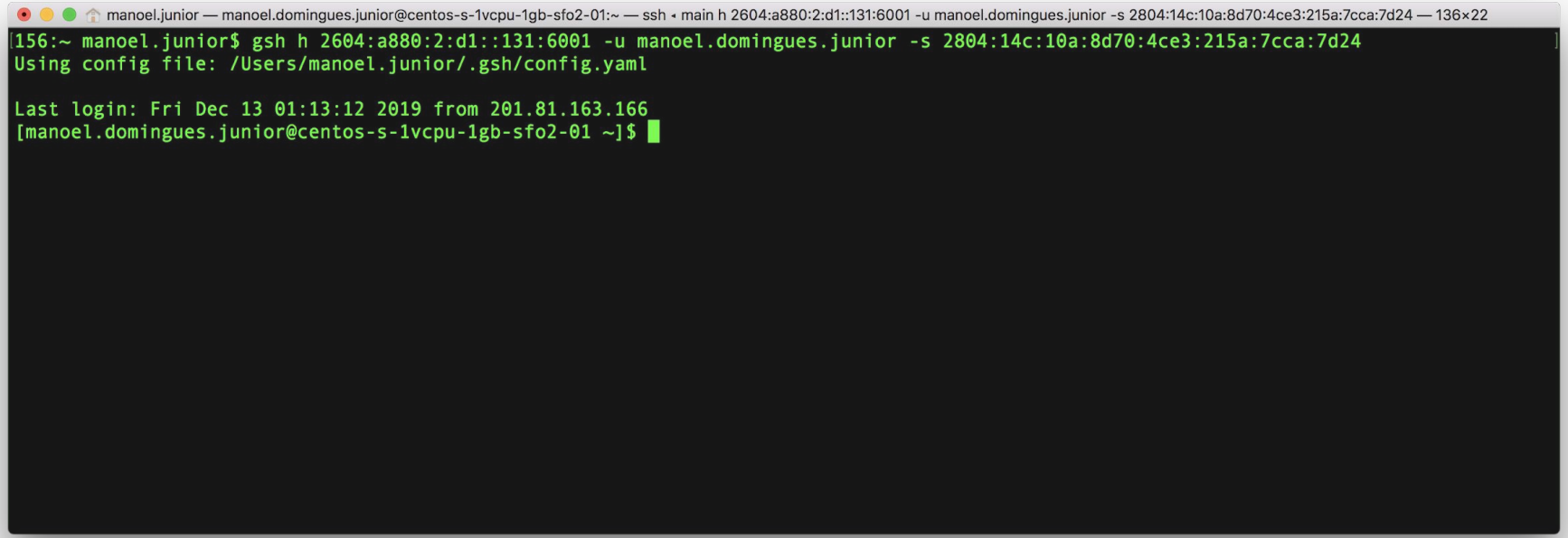
GSH - ipv6?


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 136×22
156:~ manoel.junior$ gsh role-list-me
Using config file: /Users/manoel.junior/.gsh/config.yaml
+------------+-------------+--------------+-----------------------------+------------+
| ID | Remote user | User IP | Remote host | Actions |
+------------+-------------+--------------+-----------------------------+------------+
gts-root-4	root	0.0.0.0/0	64.225.44.196/32	permit-pty
gts-self	.	0.0.0.0/0	64.225.44.196/32	permit-pty
gts-self-6	.	2804:14c::/31	2604:a880:2:d1::131:6001/128	permit-pty
+------------+-------------+--------------+-----------------------------+------------+
156:~ manoel.junior$

GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — -bash — 136×22
156:~ manoel.junior$ gsh role-add gts-self-all -a 'permit-pty' -d '2604:a880:2:d1::131:6001/128;64.225.44.196/32' -s '2804:14c::/31;201.81.163.0/24' -u '.'
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role created
156:~ manoel.junior$ gsh role-assign gts-self-all manoel.domingues.junior
Using config file: /Users/manoel.junior/.gsh/config.yaml
Role associated
156:~ manoel.junior$ gsh role-list-me
Using config file: /Users/manoel.junior/.gsh/config.yaml
ID	Remote user	User IP	Remote host	Actions
gts-root-4	root	0.0.0.0/0	64.225.44.196/32	permit-pty
gts-self-all	.	2804:14c::/31;201.81.163.0/24	2604:a880:2:d1::131:6001/128;64.225.44.196/32	permit-pty
156:~ manoel.junior$

GSH


manoel.junior — manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01:~ — ssh ◂ main h 2604:a880:2:d1::131:6001 -u manoel.domingues.junior -s 2804:14c:10a:8d70:4ce3:215a:7cca:7d24 — 136×22
[156:~ manoel.junior$ gsh h 2604:a880:2:d1::131:6001 -u manoel.domingues.junior -s 2804:14c:10a:8d70:4ce3:215a:7cca:7d24
Using config file: /Users/manoel.junior/.gsh/config.yaml
Last login: Fri Dec 13 01:13:12 2019 from 201.81.163.166
[manoel.domingues.junior@centos-s-1vcpu-1gb-sfo2-01 ~]$

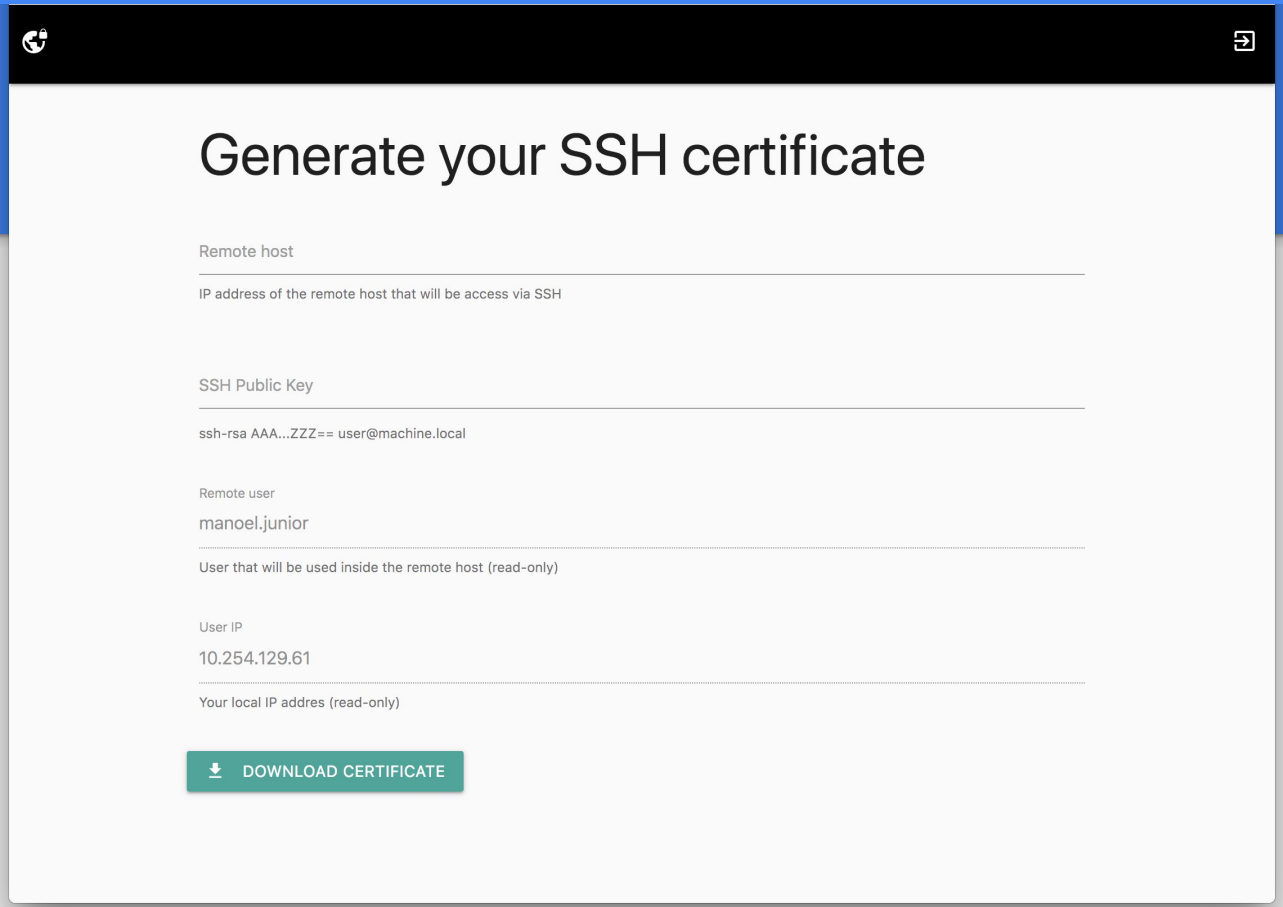
GSH

*$ ssh-keygen -Lf /Users/manoel.junior/.**gsh/certs/gts**/KbojG4CStICqkfJvn1Peote56E5yuhla-cert.pub*

```
/Users/manoel.junior/.gsh/certs/gts/KbojG4CStICqkfJvn1Peote56E5yuhla-cert.pub:
        Type: ssh-rsa-cert-v01@openssh.com user certificate
        Public key: RSA-CERT
SHA256:1ChWGB1HsSvlVV8Od1WmyXLZLorkncIsoQ0boGmKDcE
        Signing CA: RSA SHA256:zJNiSEvSCvOvfWxieW1VGHo4D7Fk039F9E2CCeBfsjE
(using ssh-rsa)
        Key ID: "64e0c354-b92a-415b-9cf8-698f73ca7968"
        Serial: 0
        Valid: from 2019-12-12T14:34:28 to 2019-12-12T14:44:58
        Principals:
                manoel.domingues.junior
        Critical Options:
                source-address 189.76.98.156
        Extensions:
                permit-pty
```

GSH - meus usuários não usam a CLI...

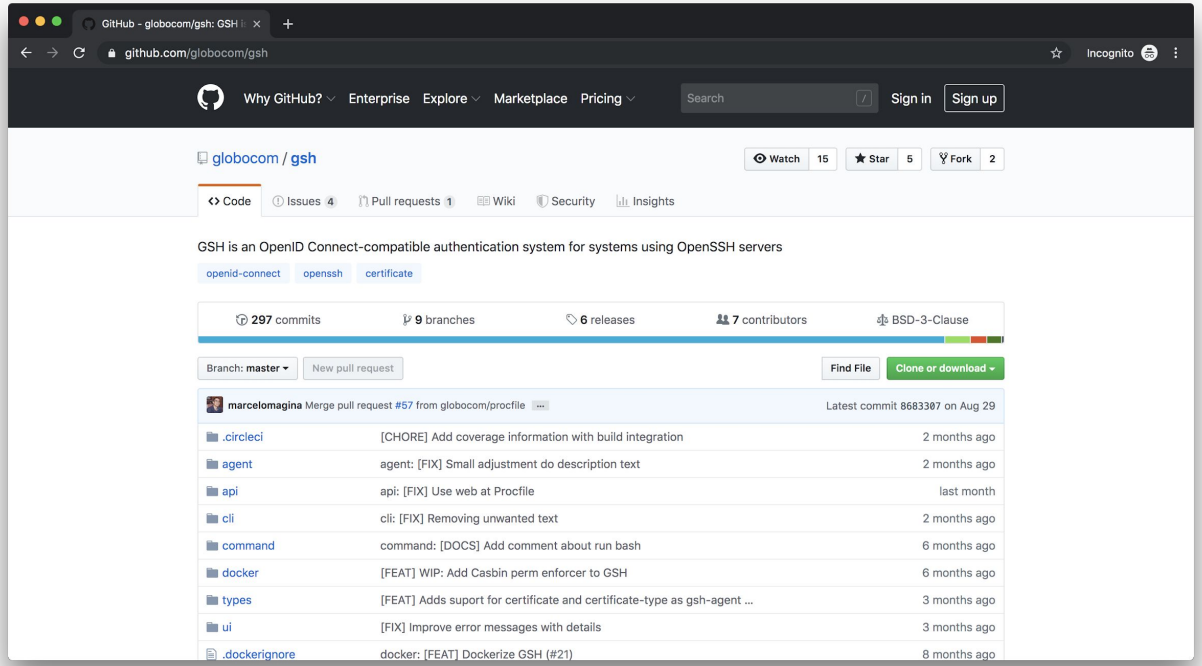
GSH


Generate your SSH certificate
Remote host
IP address of the remote host that will be access via SSH
SSH Public Key
ssh-rsa AAA...ZZZ== user@machine.local
Remote user
manoel.junior
User that will be used inside the remote host (read-only)
User IP
10.254.129.61
Your local IP addres (read-only)
DOWNLOAD CERTIFICATE

GSH - Próximos passos

- Integração com outros provedores OpenID Connect
- Extensão no certificado para verificação de destino offline
- Suporte para múltiplas origens/destinos nos certificados
- Edição de roles
- Suporte para chaves com curvas elípticas

Mais informações



https://github.com/globocom/gsh

Ma

compatibility matrix · globocom

github.com/globocom/gsh/wiki/compatibility-matrix

Incognito (2)

GSH Compatibility Matrix

GSH needs an OpenSSH version >= 6.8. This is because GSH uses `AuthorizedPrincipalsCommand` feature.

Operational System	OpenSSH version	Compatible?	Alternative?
Centos/Red-Hat/Oracle Linux 5	4.3	No	compile your RPM
Centos/Red-Hat/Oracle Linux 6	5.3	No	compile your RPM
Centos/Red-Hat/Oracle Linux 7	7.4	Yes	-
Centos/Red-Hat/Oracle Linux 8	7.8	Yes	-
Fedora 29	7.9	Yes	-
Fedora 30	8.0	Yes	-
Fedora 31	8.0	Yes	-
Fedora 32	8.1	Yes	-
Debian 10 (buster)	7.9	Yes	-
Debian 9 (stretch)	7.4	Yes	-
Debian 8 (jessie)	6.7	No	compile your DEB
Ubuntu 19.04 (disco)	7.9	Yes	-
Ubuntu 18.04 (bionic)	7.6	Yes	-
Ubuntu 16.04 (xenial)	7.2	Yes	-
ArchLinux	8.0	Yes (since 2015)	-
openSUSE Tumbleweed	7.9	Yes	-
openSUSE Leap 15.1	7.9	Yes	-
openSUSE Leap 15.0	7.6	Yes	-

Pages 31

Documentation

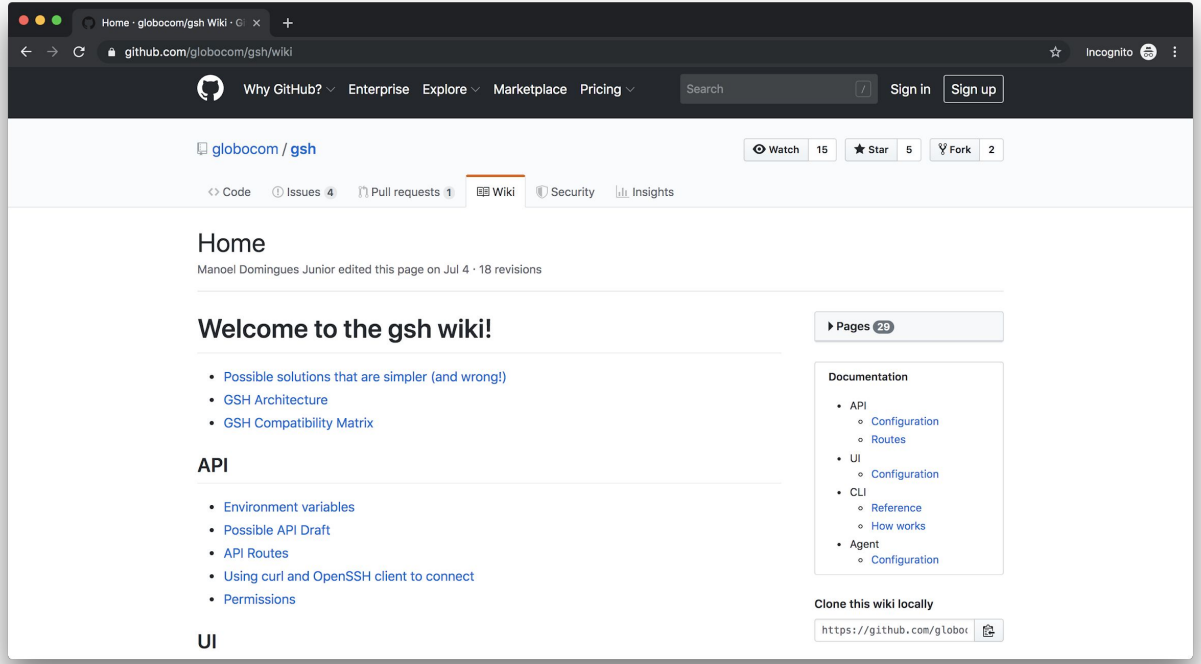
- API
  - Configuration
  - Routes
- UI
  - Configuration
- CLI
  - Reference
  - How works
- Agent
  - Configuration

Clone this wiki locally

https://github.com/globo

https://github.com/globocom/gsh

Mais informações



https://github.com/globocom/gsh

GTER 48 | GTS 34

Perguntas?

manoel.junior@corp.globo.com

Estamos contratando!

https://talentos.globo.com