Access via Teleport

Introduction to ECMWF computing services Training Week October 2025

Daniel Varela

ECMWF - User Services - Computing and Software Support team

ECMWF

What is Teleport?

- **Teleport**: A modern SSH Jump Host solution.
  - Role-based access control with single sign-on.
  - Used to access key ECMWF services like Atos HPCF and ECS/ECGATE.
- **Features**:
  - Direct SSH to internal ECMWF servers (e.g., HPC).
  - Re-authenticate only once per 12 hours.
  - Compatible with OpenSSH tools: ssh, scp, and ssh-agent.
  - Supports X11 and Port forwarding.
- **Usage**:
  - Initial sign-on with "tsh" application.
  - Post sign-on: use standard ssh or scp for internal ECMWF connections.

What is Teleport?

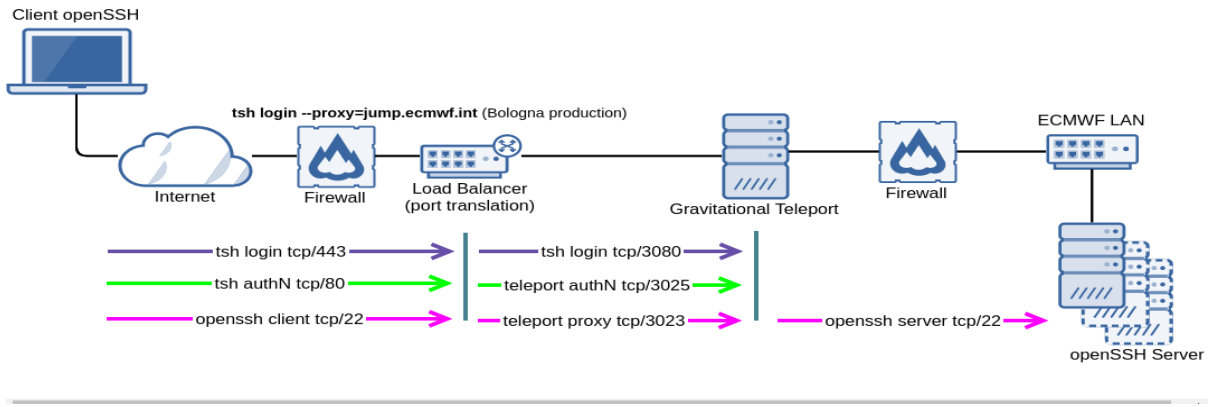
- **Advantages :**
  - Open source, very portable, and has minimal dependencies.
- **Installation:**
  - Available for Linux, Mac and Windows
  - As a static installation or a standalone client (if you don't have administrator privileges or are using Windows).
  - Must use a version of "tsh" equal to or one lower than the server version.
- **Authentication:**
  - Once every 12 hours, using ECMWF's Teleport gateway:
    - tsh login --proxy=jump-17.ecmwf.int
  - Once you have logged in at least once, tsh will save your proxy settings and you only need to run 'tsh login'.

tsh login –proxy=jump-17.ecmwf.int

- The tsh login step utilizes ports 80 and 443 for service login and obtaining the client certificate.
- It first contacts jump.ecmwf.int on port 443.
- *Tip: View these steps using the tsh login --debug option.*
- Subsequently, it initializes a local HTTP client on a high port 64xxx, generating a localhost URL for user access (e.g., http://127.0.0.1:64068/...), awaiting a callback from jump.ecmwf.int.
- This localhost URL redirects users for OIDC authentication at https://accounts.ecmwf.int (port 443), integrating with Keycloak associated with ActiveDirectory user accounts and the TOTP (Time-based One Time Password) security token.

tsh login –proxy=jump-17.ecmwf.int

- After successful authentication, tsh gets a callback from jump-17.ecmwf.int, obtaining the client certificate and concluding the login process.
- With the 12-hour valid client certificate, users gain authorization to access hosts behind the Teleport proxy using either tsh ssh or OpenSSH processes.
- Standard port 22 is employed by your SSH client for server access.
- Teleport's web shell service operates on port 443 on the same host.



Accessing ECMWF's HPCF/ ECS

If authenticating is successful, you will see an output similar to this:

```
> Profile URL:       https://jump.ecmwf.int:443
  Logged in as:      user.address@somewhere.com
  Cluster:           jump.ecmwf.int
  Roles:
  Logins:            ecmwfusername
  Kubernetes:        disabled
  Valid until:       2022-12-13 20:54:18 +0000 GMT [valid for 4h37m0s]
  Extensions:        permit-X11-forwarding, permit-agent-forwarding, permit-port-forwarding, permit-pty
```

- **SSH config:**
  - Strongly suggested to set up the options in it instead of passing them to the command line:

```
Host jump.ecmwf.int a?-* a??-* hpc-* hpc2020-* ecs-*
  User ecmwfusername
  IdentityFile ~/.tsh/keys/jump.ecmwf.int/user.address@somewhere.com
  CertificateFile ~/.tsh/keys/jump.ecmwf.int/user.address@somewhere.com-ssh/jump.ecmwf.int-cert.pub
  HostKeyAlgorithms +ssh-rsa*,rsa-sha2-512
  PubkeyAcceptedKeyTypes +ssh-rsa*
  ServerAliveInterval 60
  TCPKeepAlive yes

Host a?-* a??-* hpc-* hpc2020-* ecs-*
  ProxyJump jump.ecmwf.int
```

  - Replace ecmwfusername by your registered ECMWF user and user.address@somewhere.com by your registered email address at ECMWF.
  - Do please remember to use the right host name, as it will change with upgrades, eg jump-17.ecmwf.int, jump-18.ecmwf.int, etc

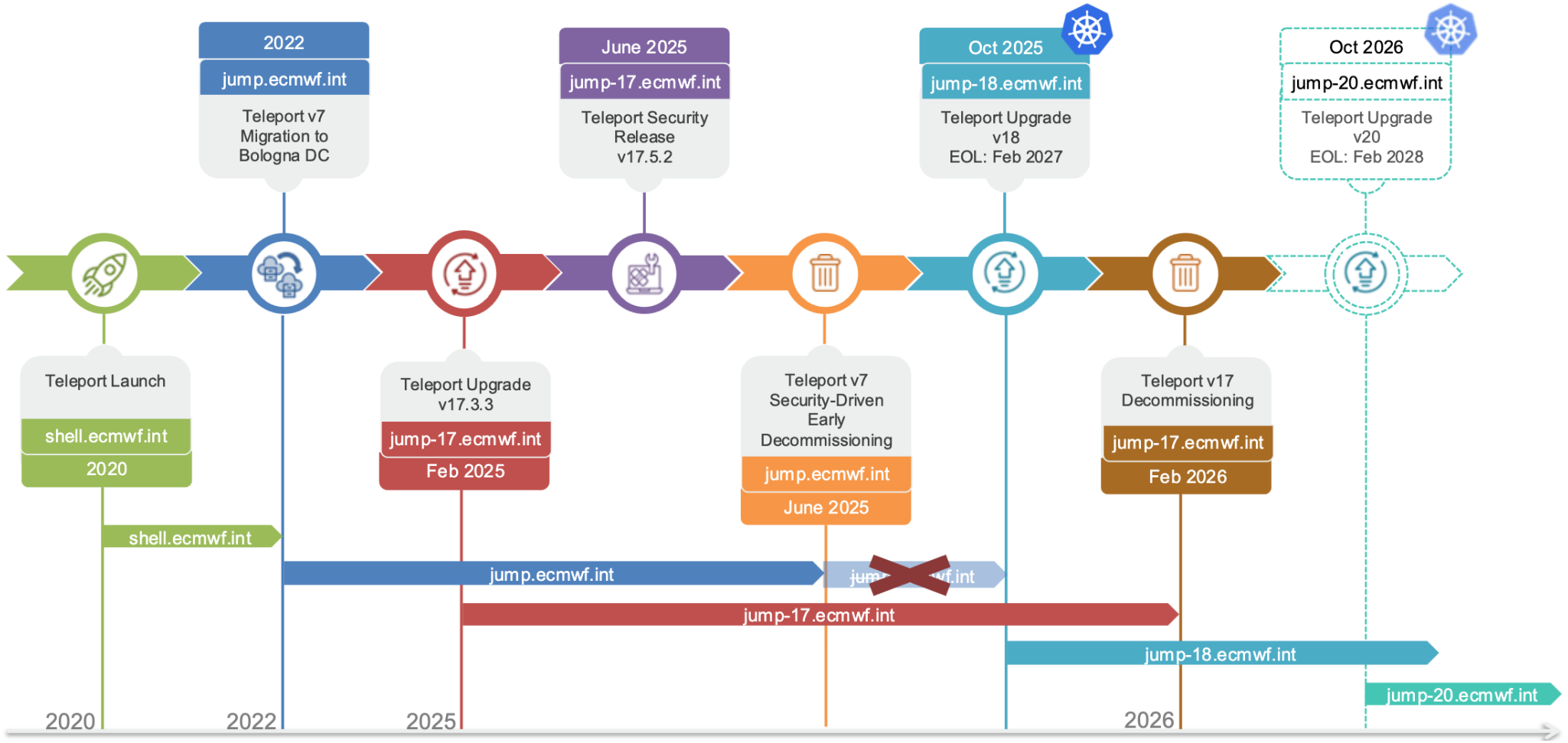
Accessing ECMWF's HPCF/ ECS

Once you have configured the appropriate settings, any SSH-based tools such as ssh, scp or rsync should work out of the box without any additional options.

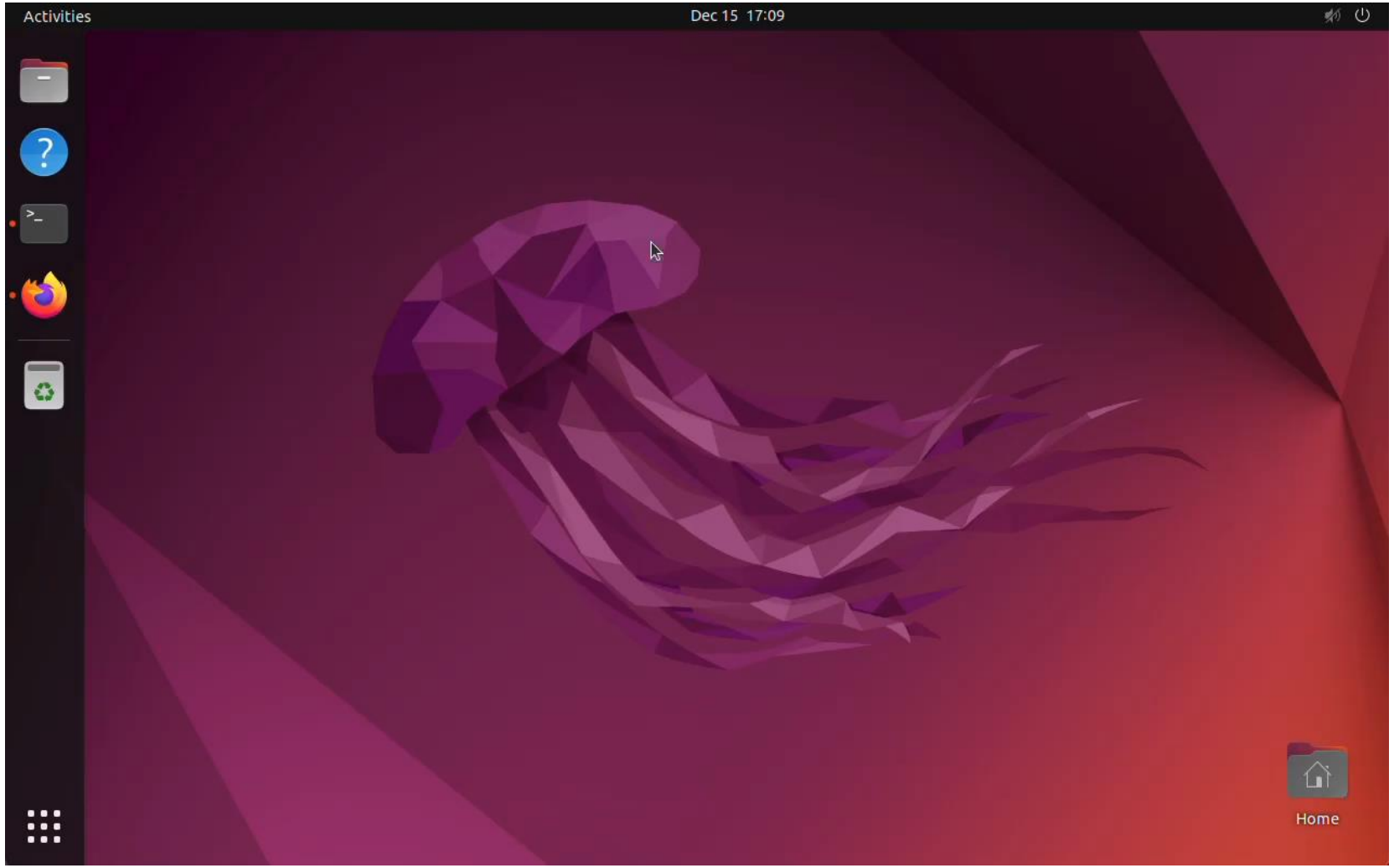
- ssh hpc-login – for access to HPCF
- ssh ecs-login – for access to ECS
- If you didn't set up your config file you'll have to specify the jump host with the –J option

  ssh -J user@jump-17.ecmwf.int user@hpc-login

Teleport roadmap

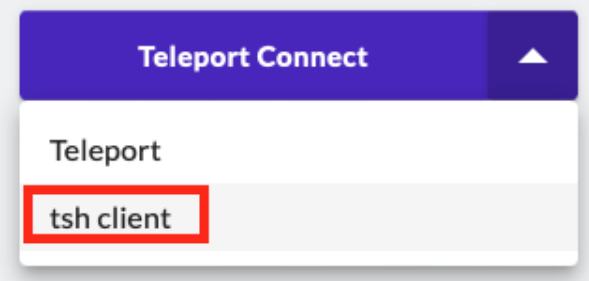


Teleport demo – Installation and access from Linux



Teleport installation under Windows

Make sure you download the “tsh client” instead of “Teleport Connect” for Windows

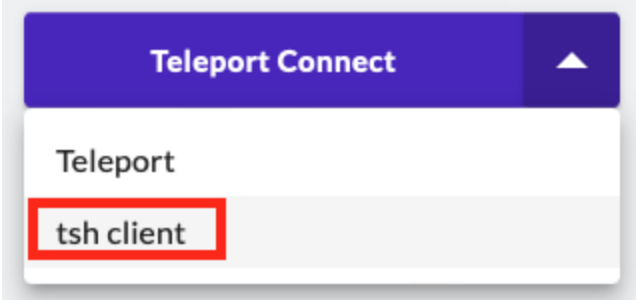


- Open the zip file in your file browser
- Drag the teleport folder inside the file and drop into the directory of your choice (the main directory for your user, for example)
- Open a Powershell and add to the PATH variable the location of the teleport directory. For example, if you dropped it on your main user directory (C:\Users\yourusername):
    - setx PATH "%USERPROFILE%\teleport;%PATH%"

Teleport demo – Installation and access from Windows

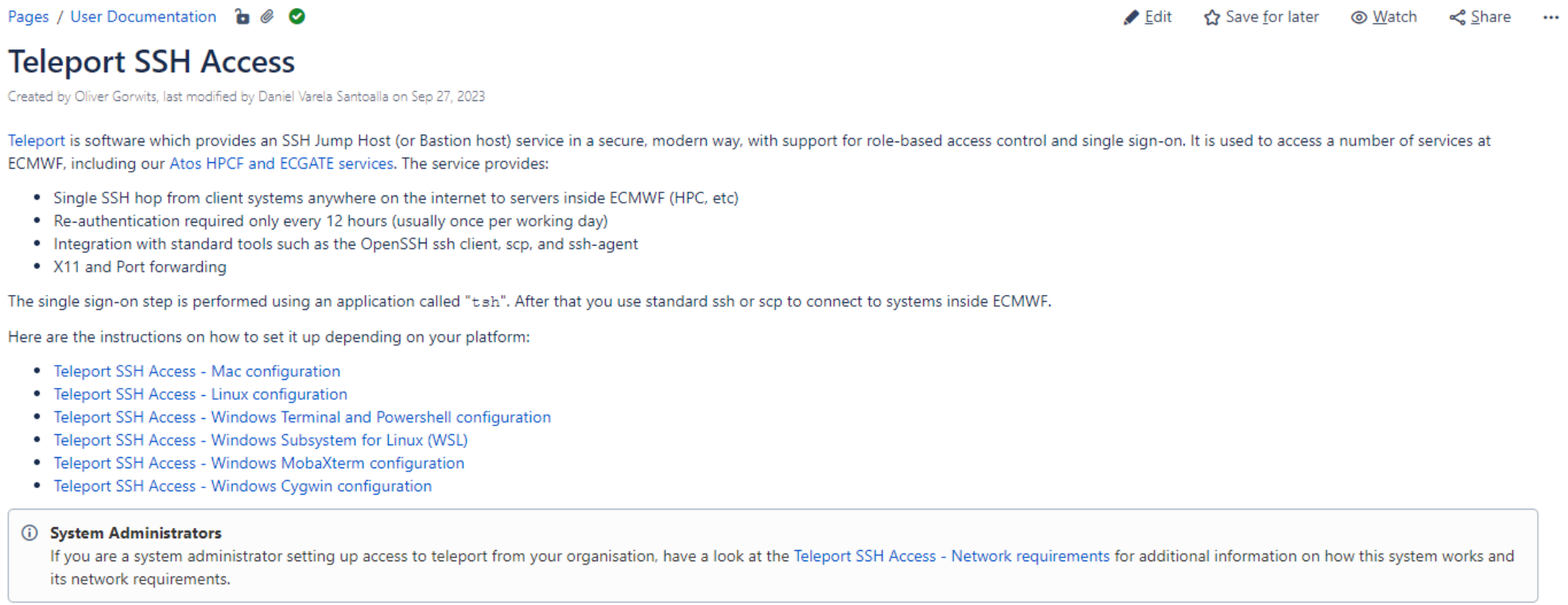
Teleport installation under Mac

- Either with brew or tsh client via Teleport website
- Teleport website recommended (brew doesn't have version 13.0)
  - With brew: brew install teleport
  - tsh client via Teleport website:



Teleport demo – Installation and access from Mac

Read more: User Documentation



Pages / User Documentation

Edit | Save for later | Watch | Share

Teleport SSH Access

Created by Oliver Gorwits, last modified by Daniel Varela Santoalla on Sep 27, 2023

Teleport is software which provides an SSH Jump Host (or Bastion host) service in a secure, modern way, with support for role-based access control and single sign-on. It is used to access a number of services at ECMWF, including our Atos HPCF and ECGATE services. The service provides:

- Single SSH hop from client systems anywhere on the internet to servers inside ECMWF (HPC, etc)
- Re-authentication required only every 12 hours (usually once per working day)
- Integration with standard tools such as the OpenSSH ssh client, scp, and ssh-agent
- X11 and Port forwarding

The single sign-on step is performed using an application called "`tsh`". After that you use standard ssh or scp to connect to systems inside ECMWF.

Here are the instructions on how to set it up depending on your platform:

- Teleport SSH Access - Mac configuration
- Teleport SSH Access - Linux configuration
- Teleport SSH Access - Windows Terminal and Powershell configuration
- Teleport SSH Access - Windows Subsystem for Linux (WSL)
- Teleport SSH Access - Windows MobaXterm configuration
- Teleport SSH Access - Windows Cygwin configuration

System Administrators
If you are a system administrator setting up access to teleport from your organisation, have a look at the Teleport SSH Access - Network requirements for additional information on how this system works and its network requirements.

https://confluence.ecmwf.int/display/UDOC/Teleport+SSH+Access

Questions?