Teleport

Teleport est une solution open source qui permet de sécuriser et unifier les accès aux serveurs, clusters Kubernetes, bases de données, applications web internes et postes de travail via un portail d’accès centralisé (bastion).

- Présentation
- Installation
- Enroler des resources

Présentation



Qu’est-ce que Teleport ?

Teleport est un outil open source qui permet de sécuriser l’accès à des ressources informatiques comme des serveurs, des bases de données, des applications internes ou encore des environnements Kubernetes. On peut le voir comme une **porte d’entrée centrale** que les administrateurs et les utilisateurs techniques empruntent pour se connecter aux systèmes sensibles.

Au lieu d’autoriser des connexions directes sur chaque machine, comme on le ferait avec SSH ou un VPN, on installe un serveur Teleport. Ce serveur devient le **point de passage obligatoire** pour accéder à l’infrastructure. C’est pour cela qu’on parle parfois de **bastion** : une sorte de rempart sécurisé qui protège l’accès à vos serveurs.

Pourquoi utiliser un bastion comme Teleport ?

L’un des premiers avantages de Teleport est qu’il permet de **centraliser tous les accès**, qu’ils soient à destination de serveurs Linux, de bases PostgreSQL, ou même d’applications web internes. Plus besoin de jongler avec des dizaines de connexions SSH, des VPN instables ou des mots de passe éparpillés.

Teleport vous permet aussi d’ajouter une **authentification forte**, par exemple via Google, GitHub, Azure AD, OpenLDAP ou même un annuaire interne. Cela signifie que l’accès à vos systèmes peut se faire avec un compte centralisé, et éventuellement avec une double authentification. C’est plus simple pour l’utilisateur, et bien plus sécurisé.

Autre point fort : **tout est enregistré**. Chaque connexion, chaque commande tapée dans un terminal, chaque accès à une base de données ou à une application peut être journalisé, voire enregistré sous forme de session vidéo. Cela permet aux administrateurs d’avoir une **traçabilité complète** des accès, très utile en cas d’audit ou d’incident.

Enfin, grâce à son interface web, Teleport rend l’accès à vos systèmes plus fluide, surtout pour les utilisateurs non techniques. On peut se connecter directement à un serveur ou à une application depuis un simple navigateur web, sans installer quoi que ce soit.

Comment ça fonctionne concrètement ?

Lorsqu’un utilisateur souhaite se connecter à un serveur, il ne se connecte pas directement à ce serveur. Il passe d’abord par le portail web ou par le proxy SSH de Teleport. Ce proxy vérifie son identité grâce au système d’authentification mis en place, puis vérifie s’il a les **droits nécessaires** pour accéder à la ressource demandée.

Si tout est en règle, la connexion est établie de manière sécurisée. Sinon, elle est bloquée. Ce fonctionnement permet de **contrôler précisément** qui a accès à quoi, à quel moment, et selon quelles conditions.

Il est également possible de **limiter la durée d’un accès**. Par exemple, un prestataire peut recevoir une autorisation valable uniquement pendant deux heures, ou un employé peut accéder à une base de données uniquement pendant la journée.

À qui s’adresse Teleport ?

Teleport est particulièrement utile dans les environnements où plusieurs personnes doivent se connecter à des machines sensibles. Cela peut être le cas dans une entreprise avec une équipe informatique, dans une ESN qui gère des serveurs pour ses clients, ou dans un centre de formation

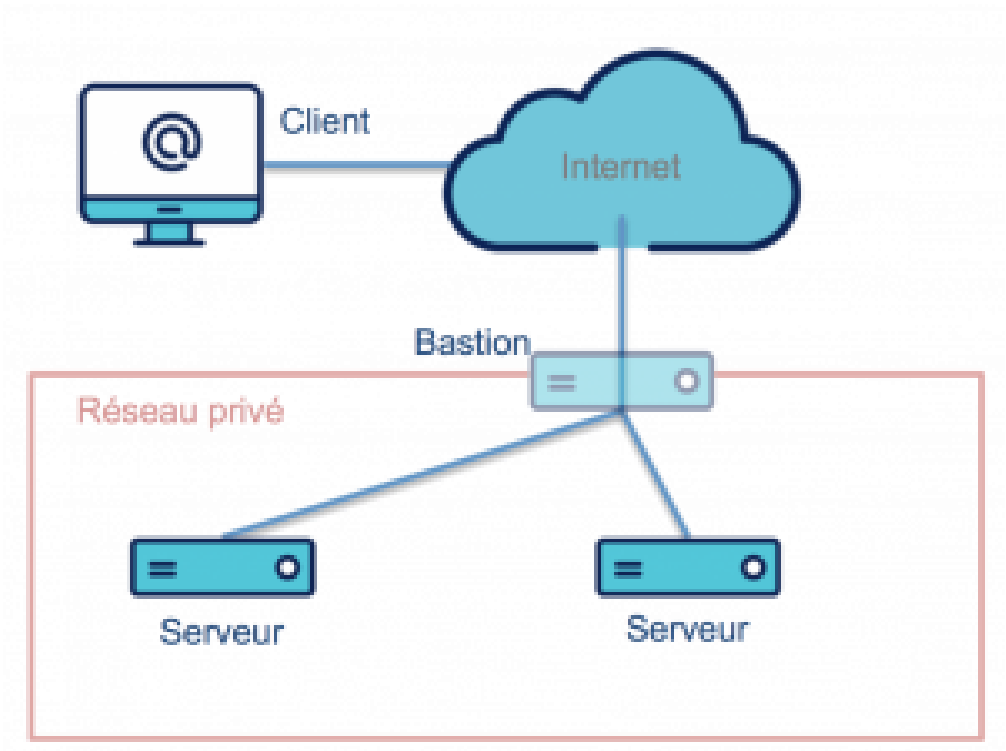
qui donne un accès temporaire à des machines virtuelles.

Mais Teleport n’est pas réservé aux grandes structures. Il peut très bien être utilisé à plus petite échelle, pour **simplifier l’administration d’un parc de serveurs**, tout en gardant un haut niveau de sécurité.

Un exemple pour mieux comprendre

Imaginons que vous ayez plusieurs serveurs Linux, un cluster Kubernetes, et une base PostgreSQL. Au lieu de devoir ouvrir des ports sur chaque machine, distribuer des clés SSH à chaque utilisateur, et surveiller les connexions manuellement, vous installez un serveur Teleport.

Les utilisateurs se connectent d’abord à ce serveur, s’authentifient avec leur compte habituel (par exemple leur compte Google ou GitHub), puis accèdent aux ressources auxquelles ils ont droit. De votre côté, vous pouvez suivre toutes les connexions en temps réel, revoir les sessions enregistrées, ou suspendre un accès à tout moment.



Et pour l’installer ?

Teleport peut être installé très facilement en auto-hébergement, sur une machine Linux. Il suffit de télécharger les binaires, ou d'utiliser un conteneur Docker. Il existe aussi une offre **Teleport Cloud** si vous préférez ne pas héberger vous-même l'infrastructure.

Installation



Prérequis

- Définir le nom de domaine sur le serveur
- Déclarer le nom de domaine via OVH

Installation

Version

Tout d'abord, il faut définir la version que l'on veux, ainsi que l'édition :

```
TELEPORT_EDITION="oss"
TELEPORT_VERSION="17.4.3"
```

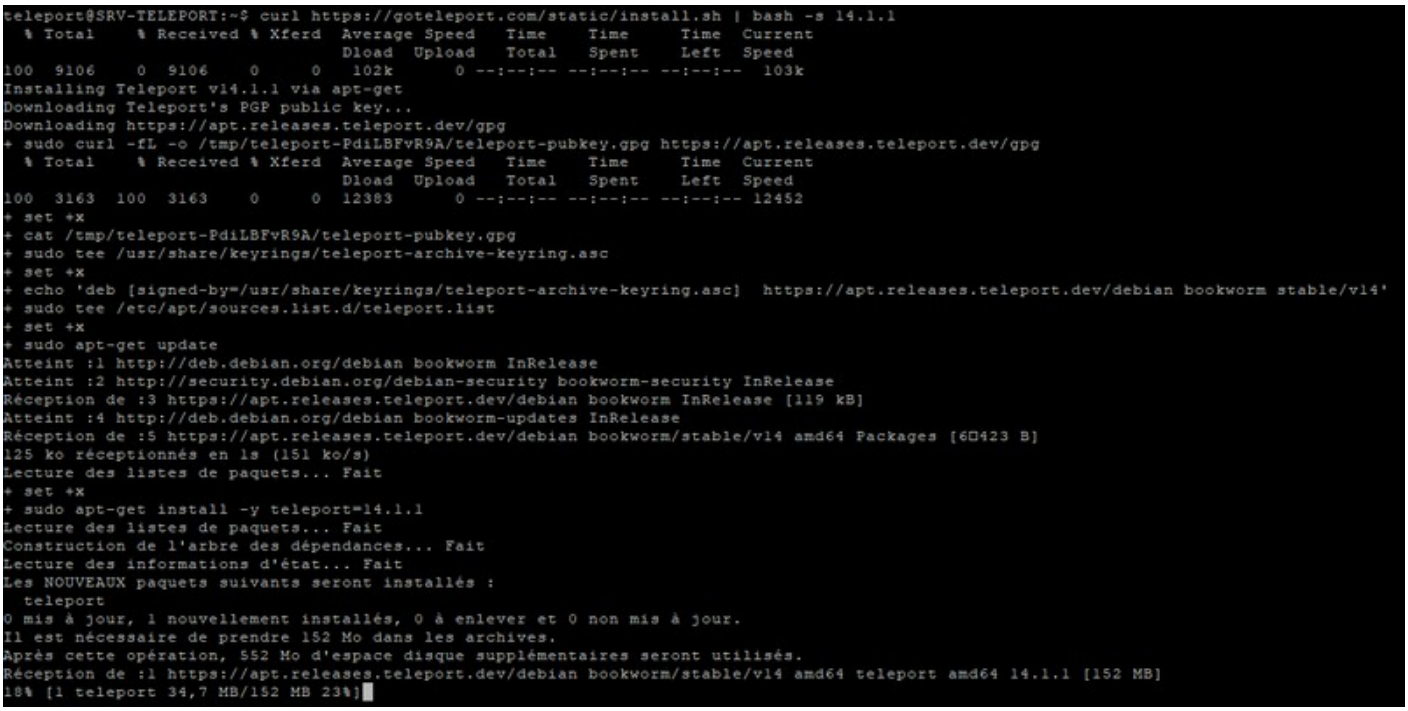
Ici on veut l'édition communautaire, donc gratuite, et non la version entreprise.

Script

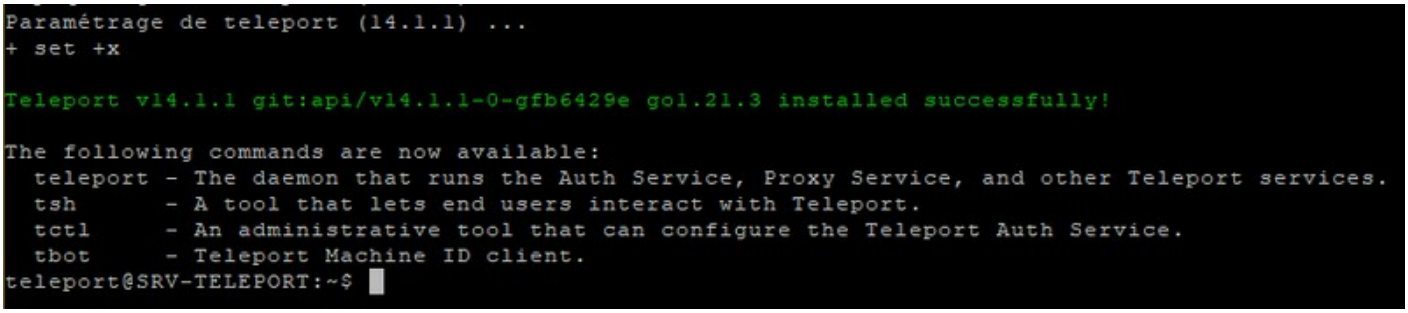
Une fois cela fait, on peut lancer le script d'installation :

```
curl https://cdn.teleport.dev/install-v17.4.3.sh | bash -s ${TELEPORT_VERSION?}
${TELEPORT_EDITION?}
```

Cela télécharge le script d'installation avant de le lancer :



Une fois l'installation terminée, voici le retour console :



Configuration

Il faut ensuite générer le fichier de configuration pour Teleport via la commande :

```
teleport configure -o file --cluster-name=teleport.rakouns.bzh
```

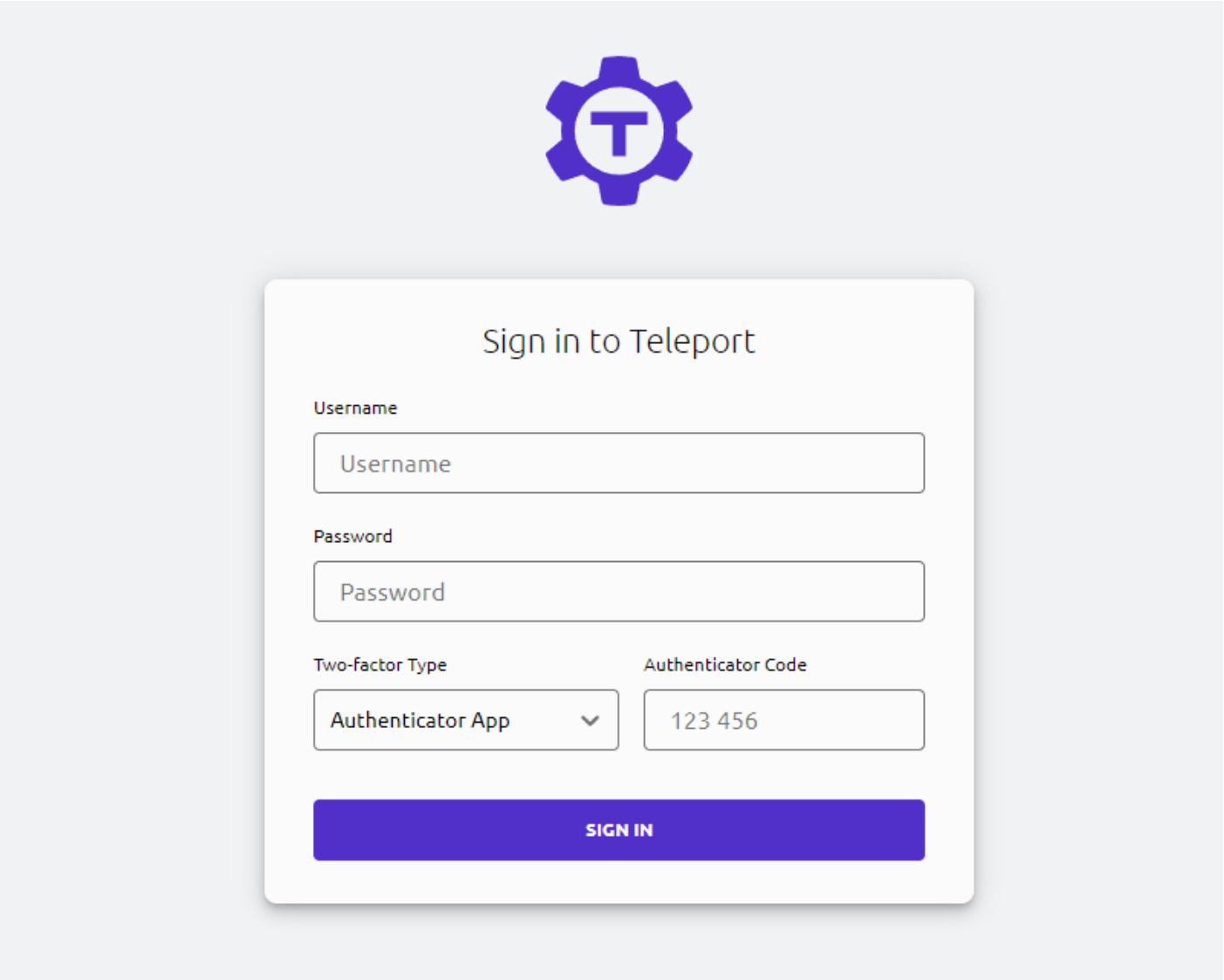
Cela créé le fichier /etc/teleport.yml

Il est préférable de faire en sorte que le service se lance automatiquement :

```
systemctl enable teleport
systemctl start teleport
```

Interface web

On peut alors se rendre sur son interface web (http://<IP>:3080) pour vérifier son bon fonctionnement :



Créer comptes :

```
tctl users add <username> --roles=editor,access --logins=<login,des,machines>
```

Il y a ensuite un retour console comme celui-ci :

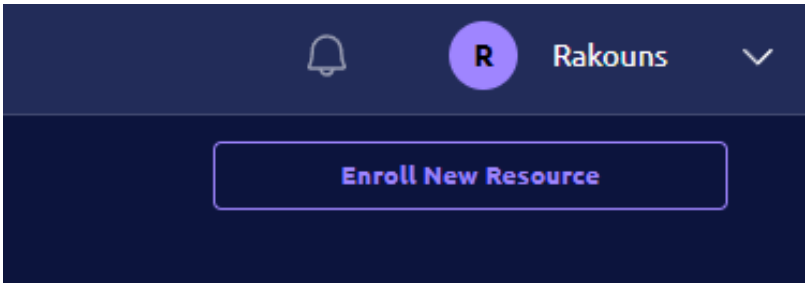
```
User <"username"> has been created but requires a password. Share this URL with the user to
complete user setup, link is valid for 1h:
https://teleport.rakouns.bzh:443/web/invite/46d49a7b4456c5421a2628bdcabe41c4
NOTE: Make sure teleport.rakouns.bzh:443 points at a Teleport proxy which users can access.
```

L'installation de base de Teleport est terminée, il est maintenant possible d'enrôler des ressources facilement grâce au guide de l'interface web.

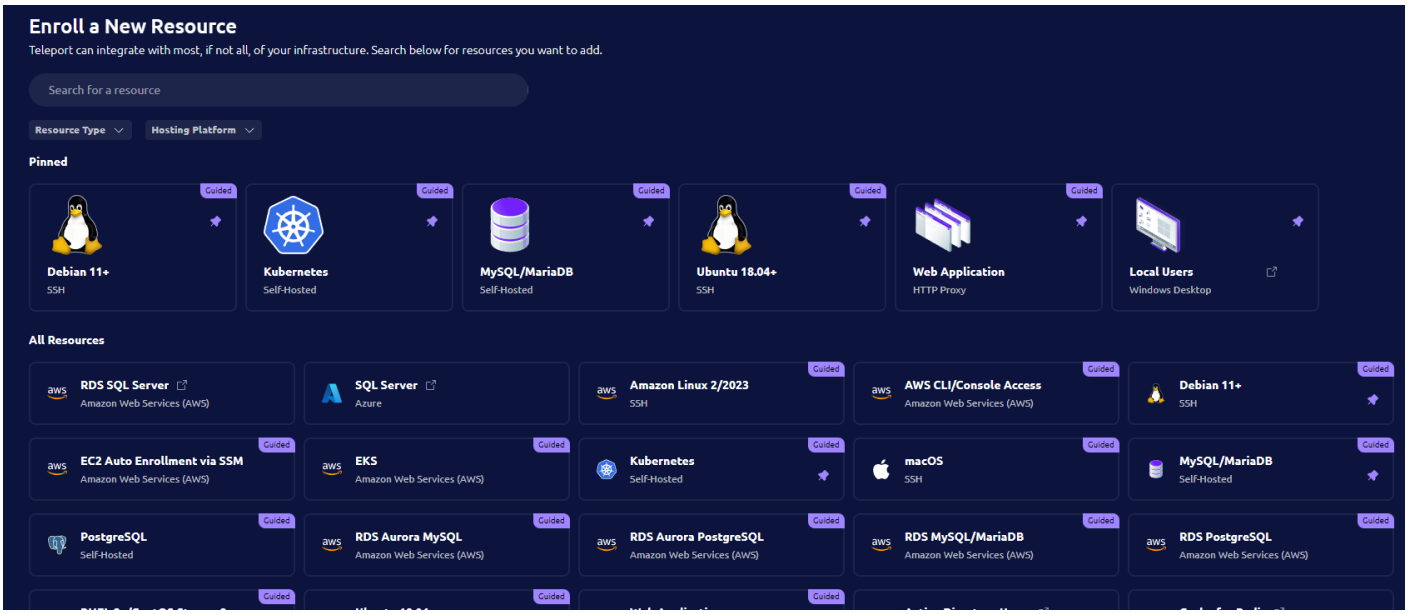
Enroler des resources

Enroler un serveur Linux

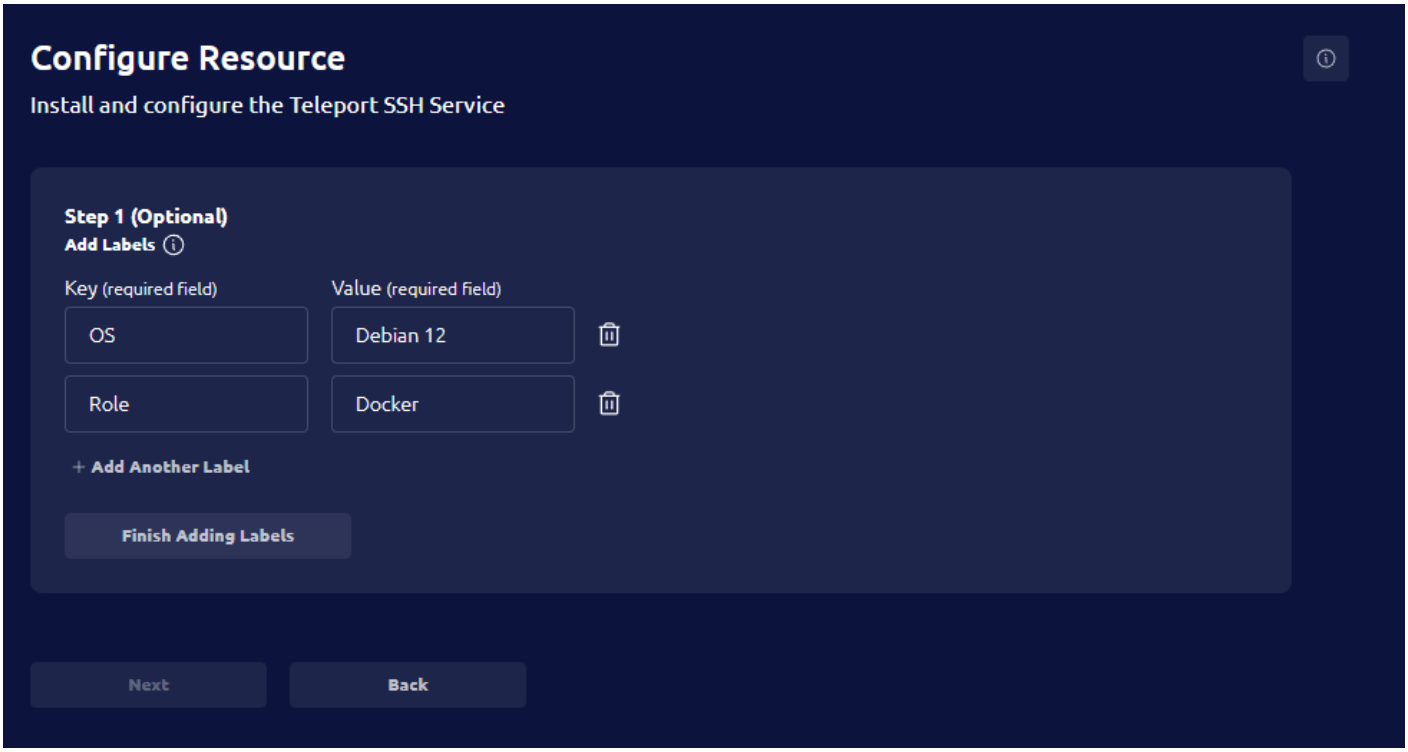
Depuis l'interface web, une fois connecté, on peut cliquer, en haut à droite, sur "Enroll New Resource"



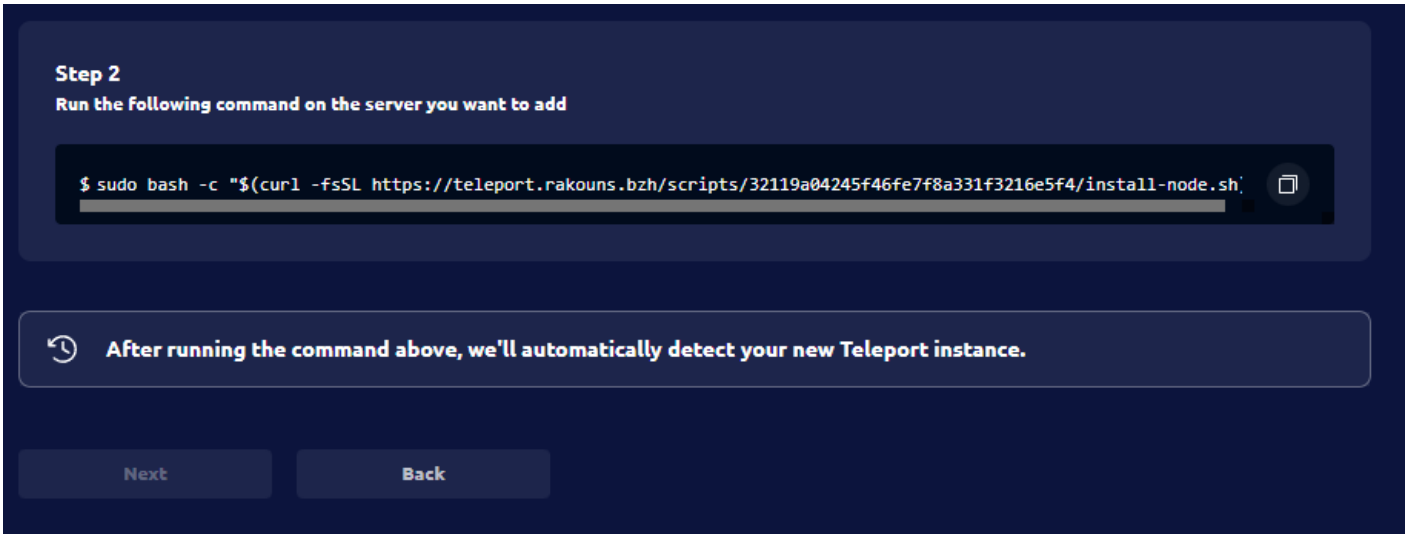
Cela nous amène sur cette page :



on choisit alors l'option voulue, ici Debian 11+, en plus c'est une procédure guidée :



On ajoute les eventiel labels que l'on voudrait mettre, puis on clique sur "Finish Adding Labels", ce qui nous donne alors une ligne de commande, qui installera et lancera le client teleport :



Chaque ligne de commande est unique, car est générée par un token temporaire, une même commande ne peut donc être utilisée qu'une seule fois.
Une fois la commande lancée sur le serveur cible, "Next" se colore en violet, et l'installation est terminée !

La procédure est la même pour Ubuntu, et pour toutes les procédures "guided", il est très simple d'enroller de nouvelles resources.