

# Teleport를 활용한 접근제어 맛보기

오픈소스 접근제어 솔루션 teleport 도입 검토 후기 및 고찰 (DB 접근제어 관점)

# 목차

---

1. 개요
2. 도입 시 고려사항
3. Teleport 오픈소스 주요 기능
4. 결론

# 개요

---

1. 도입 검토의 목적 및 배경
2. Teleport 소개

# 1. 도입 검토의 목적 및 배경

아시아투데이

## “LGU+ 29만 고객 정보 유출, 인증DB 접근 경로 부실했다”

연초 벌어진 LG유플러스 약 29만명의 고객 개인정보 유출은 '고객 인증DB' 접근 경로의 허술함으로 발생된 것으로 추정된다.

1개월 전



특히 이중 2만7000건은 2014년 6월부터 2021년 8월까지 진행된 이 회사의 사용자 계정 통합 과정에서 작업 오류로 남아있던 고객 인증 DB도 포함됐다. 이 DB에는 해지 고객도 포함됐다.

과기부는 LG유플러스의 고객 인증 시스템에서 암호나 데이터베이스(DB) 접근 제어가 미흡했고, 대용량 데이터 이동 등에 대한 실시간 탐지 체계가 없었던 것이 사고 원인으로 추정했다. 당시 고객인증 DB 시스템에서 웹 관리자 계정 암호가 시스템 초기 암호로 설정돼 있었고 관리자 계정으로 악성코드(웹셀)를 설치할 수 있었으며, 관리자의 DB 접근 제어 등 인증체계가 미흡했기 때문이다.

<<http://www.newsroad.co.kr/news/articleView.html?idxno=21682>>

보안뉴스

## [신현구의 기업보안 길라잡이-3] 보안 투자의 경제성 문제

보안의 중요성에 대한 인식은 매우 높아졌으나, 보안에 대한 투자는 인식수준 만큼에 미치지 못하고 있다. 보안 투자는 기업의 정보환경에 많은 변화를...

2022. 8. 22.

아이티비즈

한나로연결된 모든 금융

UPDATED. 2023-06-21 17:49 (수) | 로그인 회원가입 기사제보 모바일

전체 최신뉴스 기획&정책 리서치&오피니언 디지털경제 라이프 피플&포토 기사 검색

인사 동정 부음 축하 사무실이전

HOME > 리서치&오피니언 > 시장조사

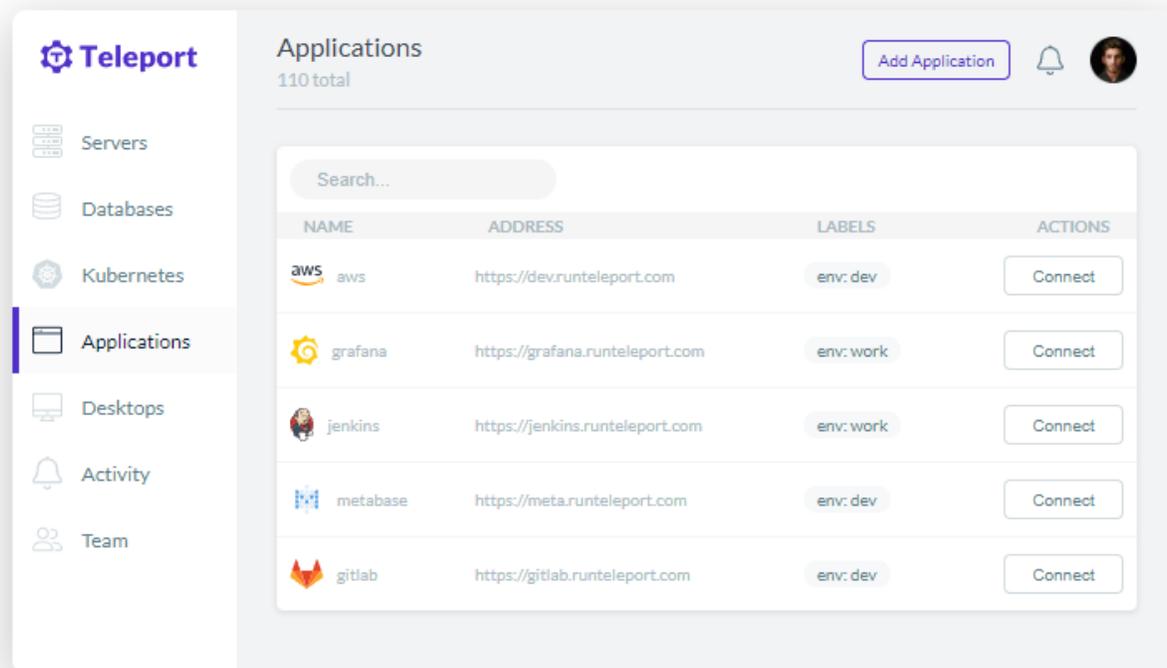
중소기업이 보안에 투자 않는 이유는... "절반이 솔루션 비용이 너무 비싸기 때문"

<http://www.it-b.co.kr/news/articleView.html?idxno=9337>

## 2. Teleport 소개

### What is Teleport?

The open source access platform used by DevSecOps teams for SSH, Kubernetes, databases, internal web applications and Windows. Teleport prevents phishing by relying on biometrics and machine identity, stops attacker pivots with the Zero Trust architecture, is compatible with everything you have, comes as a cloud service or a self-hosted option and doesn't get in the way of an engineer's productivity.



The screenshot displays the Teleport web interface. On the left is a navigation sidebar with the Teleport logo and menu items: Servers, Databases, Kubernetes, Applications (highlighted), Desktops, Activity, and Team. The main content area is titled 'Applications' and shows '110 total'. It includes a search bar and a table of applications with columns for NAME, ADDRESS, LABELS, and ACTIONS. Each application row has a 'Connect' button.

NAME	ADDRESS	LABELS	ACTIONS
aws	https://dev.runteleport.com	env: dev	Connect
grafana	https://grafana.runteleport.com	env: work	Connect
jenkins	https://jenkins.runteleport.com	env: work	Connect
metabase	https://meta.runteleport.com	env: dev	Connect
gitlab	https://gitlab.runteleport.com	env: dev	Connect

SAMSUNG

SHOCKBYTE

snowflake

softat home

SpotOn

## 2. Teleport 소개

### Access controls

	Open Source	Enterprise	Cloud	Team
<a href="#">Access Requests</a>	Limited	✓	✓	✗
<a href="#">Single Sign-On</a>	GitHub	GitHub, Google Workspace, OIDC, SAML, Teleport	GitHub, Google Workspace, OIDC, SAML, Teleport	GitHub, Teleport
<a href="#">Role-Based Access Control</a>	✓	✓	✓	✓
<a href="#">Moderated Sessions</a>	✗	✓	✓	✗
<a href="#">Device Trust</a>	✗	✓	✓	✗
<a href="#">Dual Authorization</a>	✗	✓	✓	✗
<a href="#">Hardware Key Support</a>	✗	✓	✓	✗

## Team

Protect your infrastructure with essential security & compliance capabilities

**\$15**/Monthly Active User

### Support

	Open Source	Enterprise	Cloud	Team
Support	Community	24x7 support with premium SLAs and account managers	24x7 support with premium SLAs and account managers	Community

총 4가지 Edition 존재하며, 위 내용 외 Infrastructure access, Audit logging and session recording 들에 대한 기능 Edition 간 큰 차이 없음

# 도입 시 고려사항

---

1. 관련 법령 준수 가능 여부
2. 기존 시스템과의 통합 및 호환성 문제
3. 기타 고려사항 (비용, 지원 등)

# 1. 관련 법령 준수 가능 여부

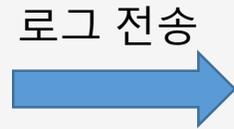
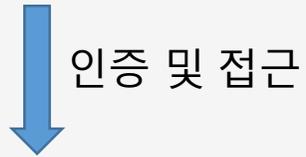
항 목		2.6.4 데이터베이스 접근
인증기준	테이블 목록 등 데이터베이스 내에서 저장·관리되고 있는 정보를 식별하고, 정보의 중요도와 응용프로그램 및 사용자 유형 등에 따른 접근통제 정책을 수립·이행하여야 한다.	
주요 확인사항	<ul style="list-style-type: none"> <li>데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 있는가?</li> <li>데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하고 있는가?</li> </ul>	
관련 법규	<ul style="list-style-type: none"> <li>개인정보 보호법 제29조(안전조치의무)</li> <li>개인정보의 안전성 확보조치 기준 제5조(접근권한의 관리), 제6조(접근통제)</li> <li>개인정보의 기술적·관리적 보호조치 기준 제4조(접근통제)</li> </ul>	

## 세부 설명

- 데이터베이스의 테이블 목록 등 저장·관리되고 있는 정보를 식별하고 지속적으로 현행화하여 관리하여야 한다.
  - ▶ 데이터베이스에서 사용되는 테이블 목록, 저장되는 정보, 상관관계 등을 식별
  - ▶ 중요정보 및 개인정보의 저장 위치(데이터베이스 및 테이블명·컬럼명) 및 현행(건수, 암호화 여부 등) 식별
  - ▶ 데이터베이스 현황에 대하여 정기적으로 조사하여 현행화 관리
- 데이터베이스 내 정보에 접근이 필요한 응용프로그램, 정보시스템(서버) 및 사용자를 명확히 식별하고 접근통제 정책에 따라 통제하여야 한다.
  - ▶ 데이터베이스 접속 권한을 관리자(DBA), 사용자로 구분하여 직무별 접근통제 정책 수립·이행(최소 권한 원칙에 따른 테이블, 뷰, 컬럼, 쿼리 레벨에서 접근통제 등)
  - ▶ 중요정보가 포함된 테이블, 컬럼은 업무상 처리 권한이 있는 자만 접근할 수 있도록 제한
  - ▶ DBA 권한이 부여된 계정과 조희 등 기타 권한이 부여된 계정 구분
  - ▶ 응용프로그램에서 사용하는 계정과 사용자 계정의 공용 사용 제한
  - ▶ 계정별 사용 가능 명령어 제한
  - ▶ 사용하지 않는 계정, 테스트용 계정, 기본 계정 등 삭제
  - ▶ 일정시간 이상 업무를 수행하지 않는 경우 자동 접속차단
  - ▶ 비인가자의 데이터베이스 접근 제한
  - ▶ 개인정보를 저장하고 있는 데이터베이스는 DMZ 등 공개된 네트워크에 위치하지 않도록 제한
  - ▶ 다른 네트워크 영역 및 다른 서버에서의 비인가 접근 차단
  - ▶ 데이터베이스 접근을 허용하는 IP주소, 포트, 응용프로그램 제한
  - ▶ 일반 사용자는 원칙적으로 응용프로그램을 통해서만 데이터베이스에 접근 가능하도록 조치 등

## 2. 기존 시스템과의 통합 및 호환성 문제

---



### 3. 기타 고려사항 (비용, 지원 등)

---



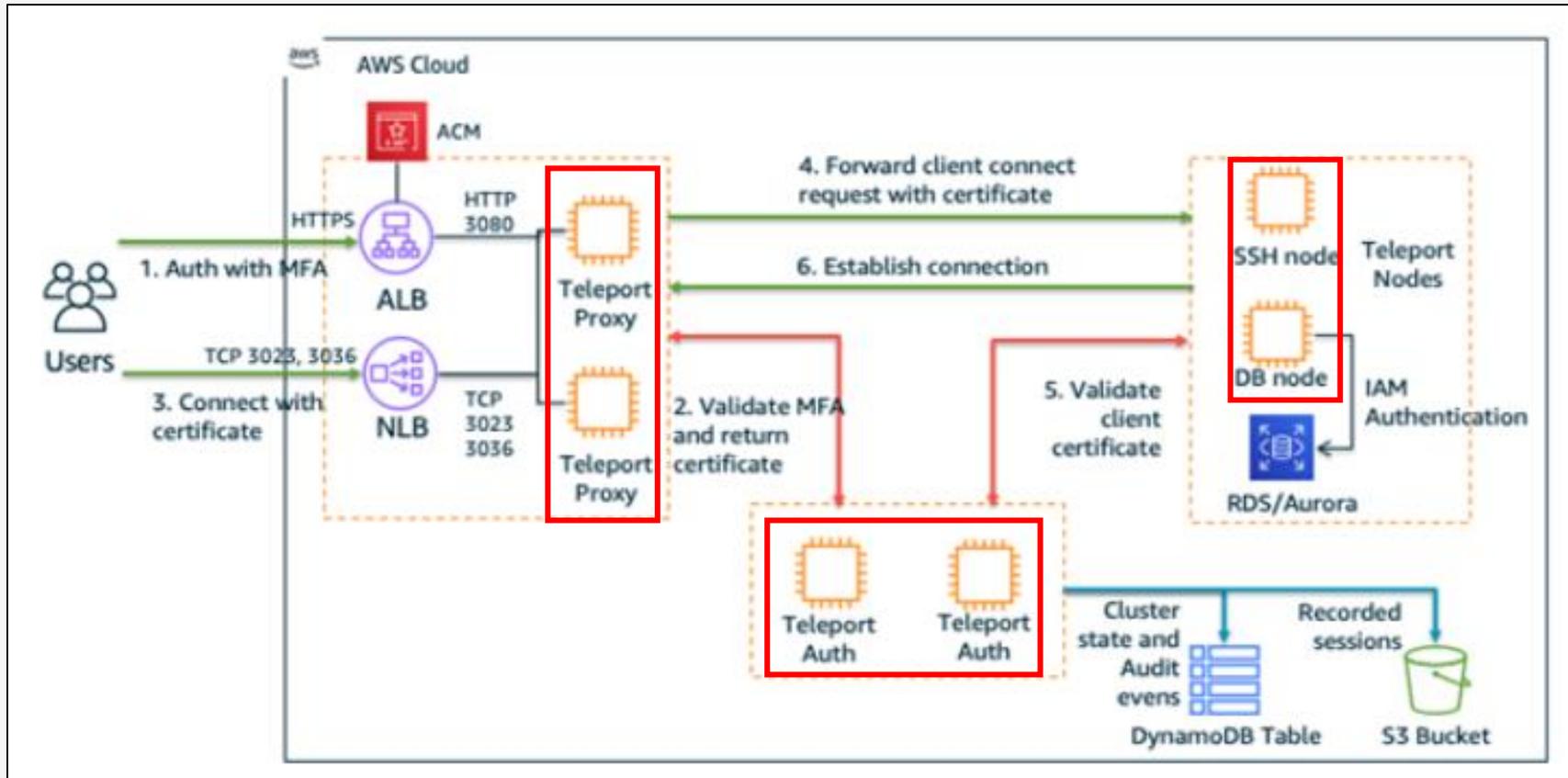
- 정보보안 솔루션에 **투자하는 비용을 적절**하게 계획하고 예산화해야 함
- 성능 및 기능을 최대화하고, 문제 발생 시 신속하게 대응하기 위해 제공업체의 **전문적인 기술 지원**이 중요
- 정보보안 솔루션 도입 후 **운영 리소스에 대한 최소화**에 대한 고려 필요

# Teleport 오픈소스 주요 기능

---

1. Core-Concepts 및 설치 방법
2. 역할 기반 접근 제어 (Role-Based Access Control, RBAC)
3. Teleport DB Service
4. 감사 로그
5. Active Session
6. (기타) SSH, Kubernetes, 웹 애플리케이션 등에 대한 접근

# 1. Core-Concepts 및 데모 설치 방법



<<http://www.newsroad.co.kr/news/articleView.html?idxno=21682>>

# 1. Core-Concepts 및 데모 설치 방법

The image shows two overlapping screenshots of the Teleport documentation website. The top-left screenshot displays the 'Helm deployment guides' section, which includes a sidebar with navigation links and a main content area with a list of guides. The bottom-right screenshot displays the 'Migration Guides' section, also with a sidebar and a list of guides.

**Helm deployment guides**

These guides show you how to set up a full self-hosted Teleport deployment

- [Teleport Cluster](#): Run a Teleport cluster in a Kubernetes cluster using the with minimal resources.
- [HA AWS Teleport Cluster](#): Running an HA Teleport Cluster on AWS with minimal resources.
- [HA GCP Teleport Cluster](#): Running an HA Teleport Cluster on GCP with minimal resources.
- [Custom Teleport config](#): Running a Teleport cluster with a custom configuration.

**Migration Guides**

- [Migrating from v11 to v12](#)
- [Kubernetes 1.25 and PSP removal](#)

**Deploy to your Cloud**

- [AWS Terraform](#): Deploy HA Teleport with Terraform on AWS.
- [AWS Multi-region Proxy Deployment](#): Deploy HA Teleport on AWS with a multi-region proxy.
- [GCP](#): Deploy HA Teleport on GCP.
- [IBM Cloud](#): Deploy HA Teleport on IBM cloud.

다양한 설치 방법 지원 (ec2 quick start, helm, k8s, eks, terraform, Free-Trial 등등)

# 1. Core-Concepts 및 데모 설치 방법\_서버

## Step 1/4. Configure DNS ¶

Teleport uses TLS to provide secure access to its Proxy Service and Auth Service, and this requires a domain name that clients can use to verify Teleport's certificate. Set up two DNS `A` records, each pointing to the IP address of your Linux host. Assuming

`teleport.example.com` is your domain name, set up records for:

Domain	Reason
<code>teleport.example.com</code>	Traffic to the Proxy Service from u
<code>*.teleport.example.com</code>	Traffic to web applications register domain name to each application.

Route 53 > 호스팅 영역 > jinchoi.net

퍼블릭 jinchoi.net 정보 [영역 삭제] [레코드 테스트] [쿼리 로깅 구성]

▶ 호스팅 영역 세부 정보 [호스팅 영역 편집]

레코드(3) | DNSSEC 서명 | 호스팅 영역 태그(0)

레코드 (3) 정보  
Automatic 모드는 최상의 필터 결과에 최적화된 현재 검색 동작입니다. 모드를 변경하려면 설정(settings)으로 이동합니다.

[새로고침] [레코드 삭제] [영역 파일 가져오기] [레코드 생성]

속성 또는 값을 기준으로 레코드 필터링 [유형 ▼] [라우팅 정책 ▼] [별칭 ▼] < 1 > [설정]

<input type="checkbox"/>	레코드 이름	유형	라우팅 ...	차별...	별칭	값/트래픽 라우팅 대상	TTL(초)
<input type="checkbox"/>	jinchoi.net	NS	단순	-	아니요	ns-1462.awsdns-54.org. ns-1360.awsdns-27.co.uk. ns-598.awsdns-33.net. ns-485.awsdns-93.com.	17280
<input type="checkbox"/>	jinchoi.net	SOA	단순	-	아니요	ns-1462.awsdns-54.org. sev...	900
<input type="checkbox"/>	teleport.jinchoi.net	A	단순	-	아니요	5.56.180.69	300

# 1. Core-Concepts 및 데모 설치 방법\_서버

## Step 2/4. Set up Teleport on your Linux host

### Install Teleport

On your Linux host, run the following command to install the Teleport binary:

```
$ curl https://goteleport.com/static/install.sh | bash -s 13.1.1
```

Public internet deployment with Let's Encrypt

Private network deployment

Let's Encrypt verifies that you control the domain name of your Teleport cluster by communicating with the HTTPS server listening on port 443 of your Teleport Proxy Service.

You can configure the Teleport Proxy Service to complete the Let's Encrypt verification process when it starts up.

On the host where you will start the Teleport Auth Service and Proxy Service, run the following `teleport configure` command. Assign `tele.example.com` to the domain name of your Teleport cluster and `user@example.com` to an email address used for notifications (you can use any domain):

```
$ teleport configure --acme --acme-email= user@example.com --cluster-name= tele.example.com | sudo tee /etc
```

```
$ sudo systemctl enable teleport
```

```
$ sudo systemctl start teleport
```

```
[ec2-user@ip-10-0-0-185 ~]$ ls /etc/teleport.yaml  
/etc/teleport.yaml
```

<teleport config file>

```
auth_service:  
  enabled: "yes"  
  listen_addr: 0.0.0.0:3025  
  cluster_name: teleport.jinchoi.net  
  proxy_listener_mode: multiplex  
ssh_service:  
  enabled: "yes"  
  commands:  
  - name: hostname  
    command: [hostname]  
    period: 1m0s  
proxy_service:  
  enabled: "yes"  
  web_listen_addr: 0.0.0.0:443  
  public_addr: teleport.jinchoi.net:443  
  https_keypairs: []  
  https_keypairs_reload_interval: 0s  
acme:  
  enabled: "yes"  
  email: andy89a@naver.com
```

<teleport.yaml>

# 1. Core-Concepts 및 데모 설치 방법\_서버

## Step 3/4. Create a Teleport user and set up two-factor authentication

In this step, we'll create a new Teleport user, `teleport-admin`, which is allowed to log into SSH hosts as any of the principals `root`, `ubuntu`, or `ec2-user`.

On your Linux host, run the following command:

```
tctl is an administrative tool that is used to configure Teleport's auth service.  
$ sudo tctl users add teleport-admin --roles=editor,access --logins=root,ubuntu,ec2-user
```

The command prints a message similar to the following:

```
User "teleport-admin" has been created but requires a password. Share this URL with the user to complete user setup, link  
is valid for 1h:  
https://teleport.example.com:443/web/invite/123abc456def789ghi123abc456def78  
  
NOTE: Make sure teleport.example.com:443 points at a Teleport proxy which users can access.
```

Login

teleport.jinchoi.net/web/login?redirect\_uri=ht...

Sign in to Teleport

USERNAME

Username

PASSWORD

Password

TWO-FACTOR TYPE

Authenticator App

AUTHENTICATOR CODE

123 456

SIGN IN

# 1. Core-Concepts 및 데모 설치 방법\_에이전트 접속

- teleport
- tsh
- tctl
- tbot

Teleport Binary Install:  
<https://goteleport.com/docs/installation/>

```
[ec2-user@ip-10-0-0-185 ~]$ tsh login --proxy=teleport.jinchoi.net --user=teleport-admin
Enter password for Teleport user teleport-admin:
Enter your OTP token:
> Profile URL:      https://teleport.jinchoi.net:443
  Logged in as:    teleport-admin
  Cluster:        teleport.jinchoi.net
  Roles:          access, editor
  Logins:         root, ubuntu, ec2-user
  Kubernetes:     enabled
  Kubernetes cluster: "demo-cluster-dev"
  Valid until:    2023-06-22 03:48:03 +0000 UTC [valid for 12h0m0s]
  Extensions:    login-ip, permit-agent-forwarding, permit-port-forwarding, permit-pty, private-key-policy
```

로그인

```
[ec2-user@ip-10-0-0-185 ~]$ tsh db ls
Name                Description Allowed Users Labels                               Connect
-----
demo-mysql-aurora   [alice]     account-id=354913817145,endpoint-type=...
jinchoi-db          [alice]     account-id=354913817145,endpoint-type=...
```

DB 목록 확인

```
[ec2-user@ip-10-0-0-185 ~]$ tsh ls
Node Name                Address                Labels
-----
ip-10-0-0-185.ap-northeast-2.compute.in... 127.0.0.1:3022 hostname=ip-10-0-0-185.ap-northe...
ip-10-0-0-80.ap-northeast-2.compute.int... — Tunnel              hostname=ip-10-0-0-80.ap-northea...
```

서버 목록 확인

```
[ec2-user@ip-10-0-0-185 ~]$ tsh kube ls
Kube Cluster Name Labels Selected
-----
demo-cluster-dev *
```

k8s 목록 확인

## 2. 역할 기반 접근 제어 (Role-Based Access Control, RBAC)

```
kind: role
version: v5
metadata:
  name: developer
spec:
  allow:
    # Label selectors for database instances this role has access to.
    #
    # These will be matched against the static/dynamic labels set on the
    # database service.
    db_labels:
      environment: ["dev", "stage"]
    # Database account names this role can connect as.
    db_users: ["viewer", "editor"]
    # Database names this role will be able to connect to.
    #
    # Note, this is not the same as the "name" field in "db_service", this is
    # the database names within a particular database instance.
    #
    # Also note, this setting has effect only for PostgreSQL. It does not
    # currently have any effect on MySQL databases/schemas.
    db_names: ["user", "billing", "core"]
```

### Role 생성

### 권한 정의

```
[ec2-user@ip-10-0-0-185 ~]$ sudo tctl create -f developer roles.yaml
role 'developer' has been created
[ec2-user@ip-10-0-0-185 ~]$ sudo tctl users add alice --roles=developer
User "alice" has been created but requires a password. Share this URL with the user to
or 1h:
https://teleport.jinchoi.net:443/web/invite/23cb39eb4013848216f3363469b00dd7
```

### Role 생성

### User 생성

```
kind: role
version: v5
metadata:
  name: prod_db
spec:
  allow:
    db_labels:
      environment: ["prod"]
    db_users: ["*"]
    db_names: ["*"]
  deny:
    db_users: ["root"]
    db_names: ["root"]
```

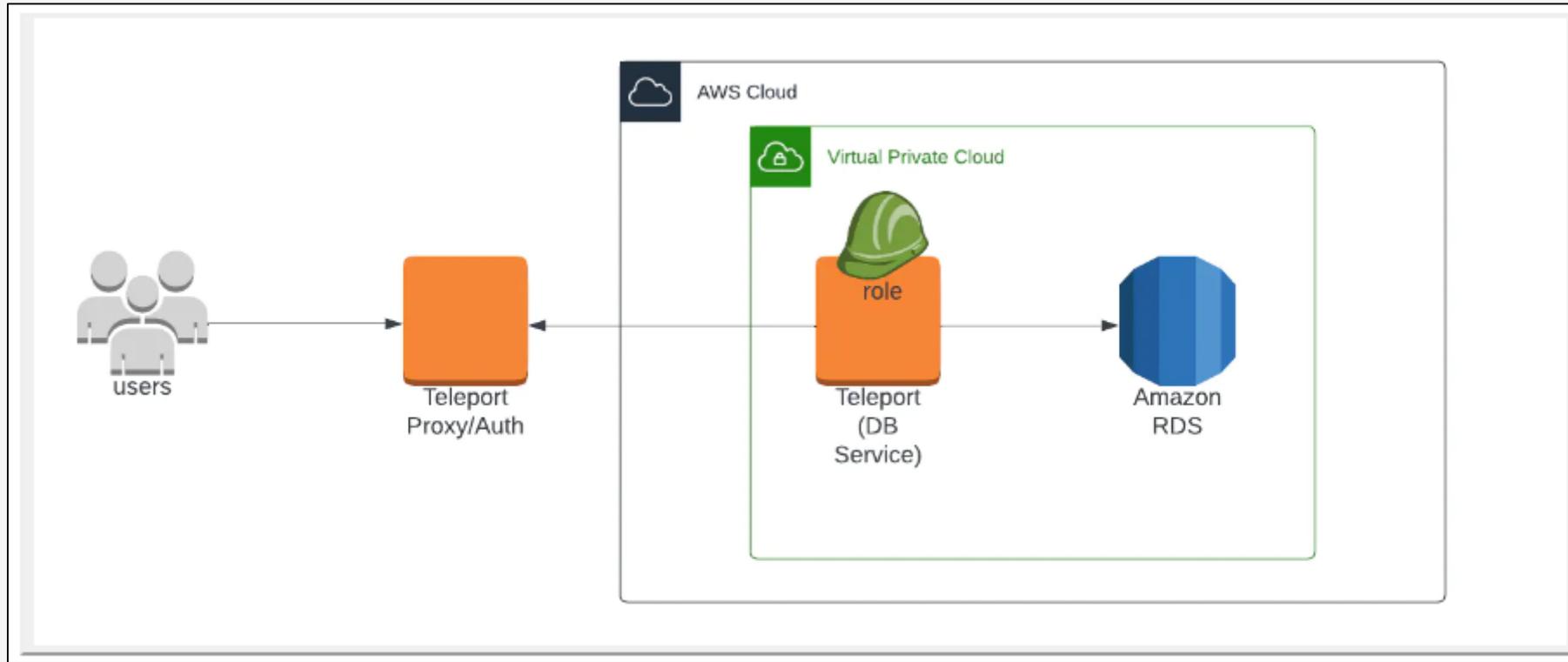
```
[ec2-user@ip-10-0-0-185 ~]$ sudo tctl create -f prod_db_roles.yaml
role 'prod_db' has been created
[ec2-user@ip-10-0-0-185 ~]$ sudo tctl users add bob --roles=prod_db
User "bob" has been created but requires a password. Share this URL with the user to
or 1h:
https://teleport.jinchoi.net:443/web/invite/dc058e5e9c75746c02f58eb9d
```

Access	SEARCH...
Users	NAME ^ ROLES ⇅
Roles	alice developer
Auth Connectors	bob prod_db

DML, DCL, DDL 등에 대한 세부 권한 설정이 불가능하여, DB에서 User에 대한 권한 제어 필요

## 2. Teleport DB Service

---



## 2. Teleport DB Service

### Step 2/4. Start the Teleport Database Service

The Database Service requires a valid auth token to connect to the cluster. Generate one by running the following command against your Teleport Auth Service and save it in `/tmp/token` on the node that will run the Database Service:

```
$ tctl tokens add --type=db
```

#### Alternative methods

Install Teleport on the host where you will run the Teleport Database Service:

Use the appropriate commands for your environment to install your package.

Teleport Edition

Debian 8+/Ubuntu 16.04+ (apt)

Amazon Linux 2/RHEL 7 (yum)

Amazon Linux 2023/RHEL 8+ (dnf)

Ta

Download Teleport's PGP public key

```
$ sudo curl https://apt.releases.teleport.dev/gpg \  
-o /usr/share/keyrings/teleport-archive-keyring.asc
```

Source variables about OS version

```
$ source /etc/os-release
```

Add the Teleport APT repository for v13. You'll need to update this file for each major release of Teleport.

```
$ echo "deb [signed-by=/usr/share/keyrings/teleport-archive-keyring.asc] \  
https://apt.releases.teleport.dev/${ID?} ${VERSION_CODENAME?} stable/v13" \  
| sudo tee /etc/apt/sources.list.d/teleport.list > /dev/null  
$ sudo apt-get update  
$ sudo apt-get install teleport
```

```
$ teleport db start \  
--token=/tmp/token \  
--name=aurora \  
--auth-server=teleport.example.com:3080 \  
--protocol=postgres \  
--uri=postgres-aurora-instance-1.abcdefghijklm.us-west-1.rds.amazonaws.com:5432 \  
--aws-region=us-west-1
```

# 2. Teleport DB Service

Identity and Access Management(IAM)

IAM > 자격 증명 공급자 > teleport.jinchoi.net

## teleport.jinchoi.net

요약 **DB List 조회 IAM Role (본체)**

공급자	공급자 유형	생성 시간	ARN
teleport.jinchoi.net	OpenID Connect	June 19, 2023, 15:49 (UTC+09:00)	arn:aws:iam::3549...c-provider/teleport.jinchoi.net

대상 (1) 작업

지문 (1) 권한

클라이언트 ID라고도 하는 대상은 OpenID Connect 공급자가 키를 제공하는 도메인에서 사용하는 X.509 인증서의 16진수 인코딩 SHA-1 해시 값입니다.

서버 인증서 지문은 OpenID Connect 공급자가 키를 제공하는 도메인에서 사용하는 X.509 인증서의 16진수 인코딩 SHA-1 해시 값입니다.

IAM > 역할 > teleport\_db\_role\_new

## teleport db role new

요약

생성 날짜  
June 19, 2023, 15:50 (UTC+09:00)

마지막 활동  
2일 전

**권한** | 신뢰 관계 | 태그 | 액세스 관리자 | 세션 취소

신뢰할 수 있는 엔터티  
지정된 조건에서 이 역할을 수임할 수 있는 엔터티입니다.

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Principal": {
7-         "Federated": "arn:aws:iam::3549...145:oidc-provider/teleport.jinchoi.net"
8-       },
9-       "Action": "sts:AssumeRoleWithWebIdentity",
10-      "Condition": {
11-        "StringEquals": {
12-          "teleport.jinchoi.net:aud": "discover.teleport"
13-        }
14-      }
15-    }
16-  ]
17- }
```

권한 정책 (1) 정보

최대 10개의 관리형 정책을 연결할 수 있습니다.

속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

정책 이름 > 유형 > 설명

**rds\_describe\_policy** 고객 관리형

```
1- {
2-   "Version": "2012-10-17",
3-   "Statement": [
4-     {
5-       "Effect": "Allow",
6-       "Action": [
7-         "rds:DescribeDBInstances",
8-         "rds:DescribeDBClusters"
9-       ],
10-      "Resource": "*"
11-     }
12-   ]
13- }
```

# 2. Teleport DB Service

## DB 접속 IAM Role (Node)

권한 | 신뢰 관계 | 태그 | 액세스 관리자 | 세션 취소

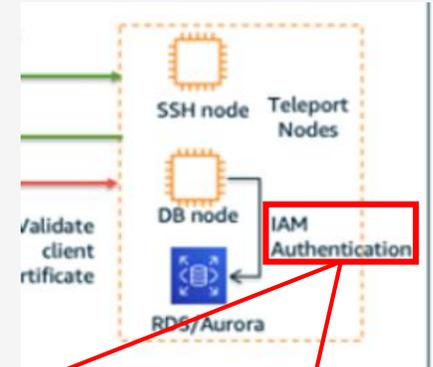
권한 정책 (5) 정보  
최대 10개의 관리형 정책을 연결할 수 있습니다.

속성 또는 정책 이름을 기준으로 정책을 필터링하고 Enter를 누릅니다.

정책 이름	유형	설명
DatabaseAccess	고객 관리형	
DatabaseAccessBoundary	고객 관리형	
TeleportDatabaseAccess_demo-mysql-aurora	고객 관리형	
TeleportDatabaseAccess_jinchoi-db	고객 관리형	

**TeleportDatabaseAccess\_jinchoi-db**

```
1 {
2   "Version": "2012-10-17",
3   "Statement": [
4     {
5       "Effect": "Allow",
6       "Action": "rds-db:connect",
7       "Resource": "arn:aws:rds-db:ap-northeast-2:35:bmq/*"
8     }
9   ]
10 }
```



**인스턴스**

구성	인스턴스 클래스
DB 인스턴스 ID	인스턴스 클래스
jinchoi-db	db.t3.micro
엔진 버전	vCPU
8.0.28	2
DB 이름	RAM
jinchoi_db	1 GB
라이선스 모델	가용성
General Public License	마스터 사용자 이름
옵션 그룹	andy89a
default:mysql-8-0 동기화 중	마스터 암호
Amazon 리소스 이름(ARN)	*****
arn:aws:rds:ap-northeast-2:35:jinchoi-db	<b>IAM DB 인증 활성화됨</b>

# 2. Teleport DB Service

The screenshot shows the 'Enroll New Resource' page in the Teleport web interface. The breadcrumb trail is: **aws Aurora MySQL/MariaDB** > **Connect AWS Account** > **Enroll RDS Database** > **Deploy D...**. The 'Connect to your AWS Account' section explains that Teleport uses short-lived credentials from AWS. A dropdown menu for 'AWS INTEGRATIONS' is set to 'teleport'. There are 'NEXT' and 'BACK' buttons at the bottom.

The 'CONNECT TO DATABASE' modal window contains three steps with terminal commands and 'COPY' buttons:

- Step 1 - Login to Teleport**  
`$ tsh login --proxy=teleport.jinchoi.net:443 --auth=local --user=teleport-admin 1`
- Step 2 - Retrieve credentials for the database**  
`$ tsh db login [--db-user=<user>] [--db-name=<name>] jinchoi-db`
- Step 3 - Connect to the database**  
`$ tsh db connect [--db-user=<user>] [--db-name=<name>] jinchoi-db`

A note at the bottom states: \* Note: To connect with a GUI database client, see our [documentation](#) for instructions. A 'CLOSE' button is at the bottom left.

The screenshot shows the 'Databases' page in the Teleport web interface. The cluster is 'teleport.jinchoi.net' and the user is 'teleport-admin'. There is an 'ADD DATABASE' button. A table lists two databases:

NAME	DESCRIPTION	TYPE	LABELS
demo-mysql-aurora	Amazon RDS MySQL/MariaDB	Amazon RDS MySQL/MariaDB	account-id:354913817145 endpoint-type:primary engine:aurora-mysql engine-version:5.7.mysql_aurora.2.11.2 region:ap-northeast-2 status:available teleport.dev/origin:dynamic
jinchoi-db	Amazon RDS MySQL/MariaDB	Amazon RDS MySQL/MariaDB	account-id:354913817145 endpoint-type:Instance engine:mysql engine-version:8.0.28 region:ap-northeast-2 status:available teleport.dev/origin:dynamic

Red boxes highlight the 'CONNECT' buttons for both database entries. A red arrow points from the 'Enroll New Resource' page to the 'ADD DATABASE' button, and another red arrow points from the 'CONNECT' buttons to the 'CONNECT TO DATABASE' modal.

## 2. Teleport DB Service

```
[ec2-user@ip-10-0-0-185 ~]$ tsh db ls
Name                Description Allowed Users Labels                    Connect
-----
demo-mysql-aurora   [alice]     account-id=354913817145,endpoint-type=primary,engine-version=5.7.my...
jinchoi-db          [alice]     account-id=354913817145,endpoint-type=instance,engine-version=8.0.2...

[ec2-user@ip-10-0-0-185 ~]$ tsh db connect --db-user=alice --db-name mysql aurora
ERROR: database "aurora" not found, use 'tsh db ls' to see registered databases

[ec2-user@ip-10-0-0-185 ~]$ tsh db connect --db-user=alice --db-name mysql jinchoi-db
Reading table information for completion of table and column names
You can turn off this feature to get a quicker startup with -A

Welcome to the MySQL monitor.  Commands end with ; or \g.
Your MySQL connection id is 10013
Server version: 8.0.28 Source distribution

Copyright (c) 2000, 2023, Oracle and/or its affiliates.

Oracle is a registered trademark of Oracle Corporation and/or its
affiliates. Other names may be trademarks of their respective
owners.

Type 'help;' or '\h' for help. Type '\c' to clear the current input statement.

mysql> select 1;
+----+
| 1 |
+----+
| 1 |
+----+
1 row in set (0.01 sec)

mysql>
```

쿼리에 대한 제한 기능 (ex. delete, limits) 없음  
-> 별도 보안 대책 필요 (피어 리뷰, SIEM 등등)

### DATABASE SESSION STARTED

```
1 {
2   "cluster_name": "teleport.jinchoi.net",
3   "code": "TD8001",
4   "db_name": "mysql",
5   "db_protocol": "mysql",
6   "db_service": "jinchoi-db",
7   "db_uri": "jinchoi-db.c9qnfbk38gro.ap-northeast-2.rds.amazonaws.com:3306",
8   "db_user": "alice",
9   "ei": 0,
10  "event": "db.session.start",
11  "namespace": "default",
12  "server_id": "2a11e7c9-09ac-4f02-8abf-4c3971acf95e",
13  "sid": "37c48d16-6ef8-4dd6-8730-c3474378781c",
14  "success": true,
15  "time": "2023-06-21T17:17:50.664Z",
16  "uid": "d5fe77cc-371d-4e08-a1a5-c63c470aefa3",
17  "user": "teleport-admin"
18 }
```

# 3. 감사 로그

Audit Log Today ▾

Database SHOWING 1 - 6 OF 6

TYPE	DESCRIPTION	CREATED (UTC)	
Database Session Ended	User [teleport-admin] has disconnected from database [mysql] on [jinchoi-db]	2023-06-21T17:24:03.95Z	DETAILS
Database Query	User [teleport-admin] has executed query [select 1] in database [mysql] on [jinchoi-db]	2023-06-21T17:18:37.284Z	DETAILS
Database Query	User [teleport-admin] has executed query [select @@version_comment limit 1] in database [mysql] on [jinchoi-db]	2023-06-21T17:17:50.994Z	DETAILS
Database Query	User [teleport-admin] has executed query [show tables] in database [mysql] on [jinchoi-db]	2023-06-21T17:17:50.702Z	DETAILS
Database Query	User [teleport-admin] has executed query [show databases] in database [mysql] on [jinchoi-db]	2023-06-21T17:17:50.667Z	DETAILS
Database Session Started	User [teleport-admin] has connected to database [mysql] as [alice] on [jinchoi-db]	2023-06-21T17:17:50.664Z	DETAILS

DATABASE QUERY

```
1 {
2   "cluster_name": "teleport.jinchoi.net",
3   "code": "TDB02I",
4   "db_name": "mysql",
5   "db_protocol": "mysql",
6   "db_query": "show databases",
7   "db_service": "jinchoi-db",
8   "db_uri": "jinchoi-db.c9qnfbk3gro.ap-northeast-2.rds.amazonaws.com",
9   "db_user": "alice",
10  "ei": 1,
11  "event": "db.session.query",
12  "sid": "37c48d16-6ef8-4dd6-8730-c3474378781c",
13  "success": true,
14  "time": "2023-06-21T17:17:50.667Z",
15  "uid": "8d333822-547d-44c0-a382-a273e9dc9436",
16  "user": "teleport-admin"
}
```

DATABASE QUERY

```
1 {
2   "cluster_name": "teleport.jinchoi.net",
3   "code": "TDB02I",
4   "db_name": "mysql",
5   "db_protocol": "mysql",
6   "db_query": "show tables",
7   "db_service": "jinchoi-db",
8   "db_uri": "jinchoi-db.c9qnfbk3gro.ap-northeast-2.rds.amazonaws.com",
9   "db_user": "alice",
10  "ei": 2,
11  "event": "db.session.query",
12  "sid": "37c48d16-6ef8-4dd6-8730-c3474378781c",
13  "success": true,
14  "time": "2023-06-21T17:17:50.702Z",
15  "uid": "c7bba235-5809-4efa-aeb1-2ae02e99ec6e",
16  "user": "teleport-admin"
17 }
```

DATABASE QUERY

```
1 {
2   "cluster_name": "teleport.jinchoi.net",
3   "code": "TDB02I",
4   "db_name": "mysql",
5   "db_protocol": "mysql",
6   "db_query": "select 1",
7   "db_service": "jinchoi-db",
8   "db_uri": "jinchoi-db.c9qnfbk3gro.ap-northeast-2.rds.amazonaws.com",
9   "db_user": "alice",
10  "ei": 4,
11  "event": "db.session.query",
12  "sid": "37c48d16-6ef8-4dd6-8730-c3474378781c",
13  "success": true,
14  "time": "2023-06-21T17:18:37.284Z",
15  "uid": "36808e46-fcb0-4ac2-893c-1e78a3dccc2d",
16  "user": "teleport-admin"
17 }
```

보완 대책...

# 4. Active Session

The screenshot shows the Teleport web interface. On the left is a sidebar with the Teleport logo and a 'Resources' dropdown menu containing 'Servers', 'Applications', 'Kubernetes', 'Databases', 'Desktops', and 'Active Sessions'. The main content area shows the 'Active Sessions' page for the cluster 'teleport.jinchoi.net'. At the top right of the main area, the user 'teleport-admin' is logged in. Below the title 'Active Sessions' is a search bar and a pagination indicator 'SHOWING 1 - 1 OF 1'. A table displays the active session details:

TYPE	NAME	SESSION ID	USERS	DURATION
	jinchoi-db	37c48d16-6ef8-4dd6-8730-c3474378781c	teleport-admin	6 minutes

## 5. SSH에 대한 접근 제어

```
ec2-user@ip-10-0-0-... x +
[ec2-user@ip-10-0-0-80 ~]$ ls
[ec2-user@ip-10-0-0-80 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-80 ~]$ touch test.sh
[ec2-user@ip-10-0-0-80 ~]$ chmod 777 test.sh
[ec2-user@ip-10-0-0-80 ~]$ ./test.sh
[ec2-user@ip-10-0-0-80 ~]$
```

**Upload Files** x

UPLOAD DESTINATION

~/

Drag your files here  
or Browse your computer to start uploading

**Upload Files** x

UPLOAD DESTINATION

~/

Drag your files here  
or Browse your computer to start uploading

ISMS-P 인증기준 안내서(2022.4.22) (1).pdf ✓

```
ec2-user@ip-10-0-0-... x +
[ec2-user@ip-10-0-0-80 ~]$ ls
[ec2-user@ip-10-0-0-80 ~]$ pwd
/home/ec2-user
[ec2-user@ip-10-0-0-80 ~]$ touch test.sh
[ec2-user@ip-10-0-0-80 ~]$ chmod 777 test.sh
[ec2-user@ip-10-0-0-80 ~]$ ./test.sh
[ec2-user@ip-10-0-0-80 ~]$ ls
'ISMS-P 인증기준 안내서(2022.4.22) (1).pdf' test.sh
[ec2-user@ip-10-0-0-80 ~]$
```

Session Manager? 업/다운로드 편함 (장점..?단점..?)  
Pem key X

# 5. SSH에 대한 접근 제어

The screenshot shows the Teleport web interface. At the top, it displays 'CLUSTER: teleport.jinchoi.net' and the user 'teleport-admin'. The main section is titled 'Active Sessions' and contains a table with two rows of session data. A search bar is located above the table. A dropdown menu is open over the 'JOIN' button of the second session, showing three options: 'As an Observer', 'As a Moderator', and 'As a Peer', each with a brief description of its capabilities.

TYPE	NAME	SESSION ID	USERS	DURATION	
>_	ip-10-0-0-80.ap-northeast-2.compute.internal	9768e7e4-015a-4b3f-8850-8edd904fe1e4	teleport-admin	2 minutes	JOIN
>_	ip-10-0-0-185.ap-northeast-2.compute.internal	a5737e61-cd48-4dee-9742-17c446f249c6	teleport-admin	3 min	JOIN

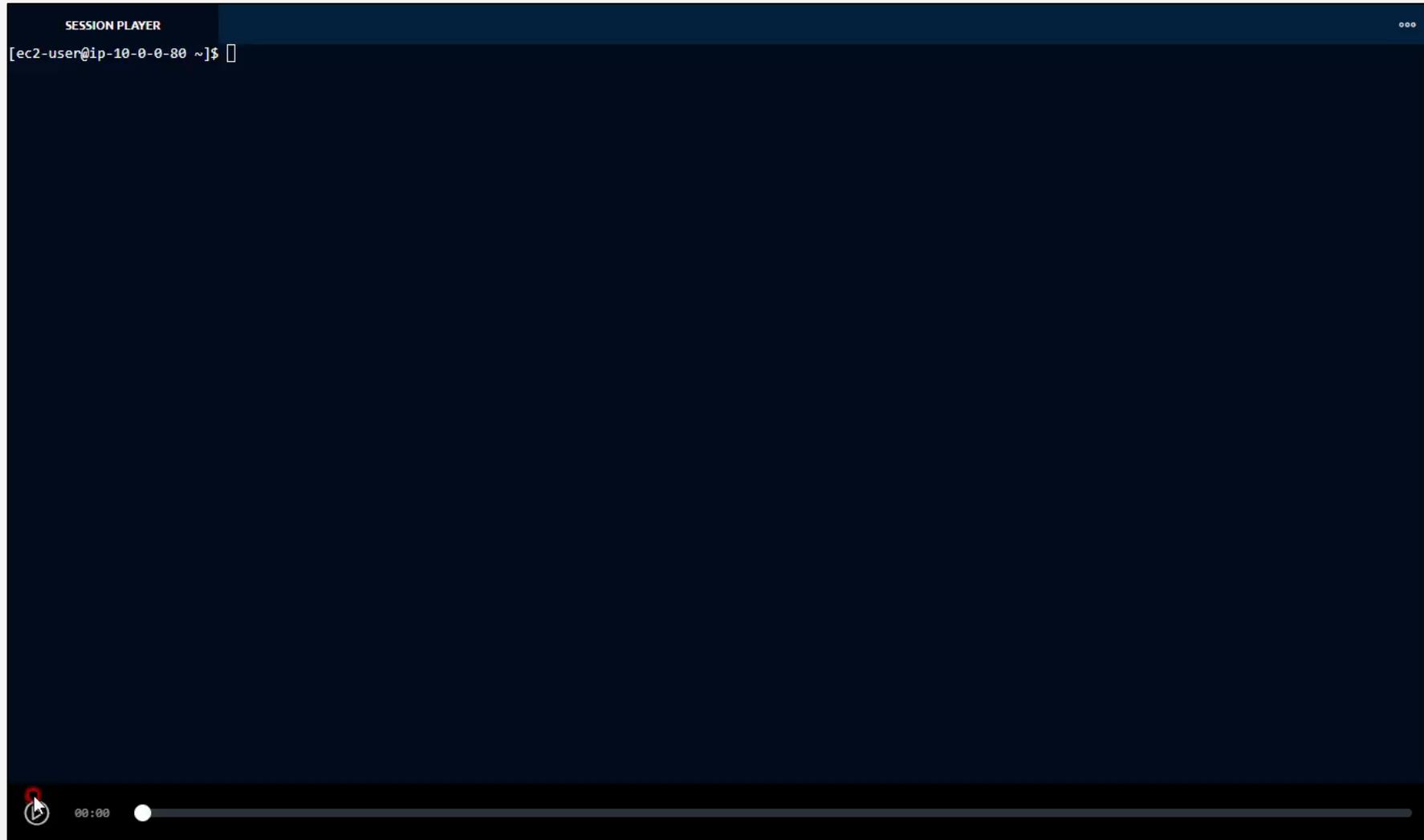
- As an Observer**  
Can view output but cannot send input.
- As a Moderator**  
Can view output & terminate the session.
- As a Peer**  
Can view output & send input.

Two terminal windows are shown side-by-side. Both windows are connected to an 'ec2-user@ip-10-0-0-80' instance. The left terminal shows the execution of a script 'test.sh' which creates a file, sets permissions, and runs a command. The right terminal shows the same script execution followed by the 'monitor realtime' command, which displays the output of the script in real-time.

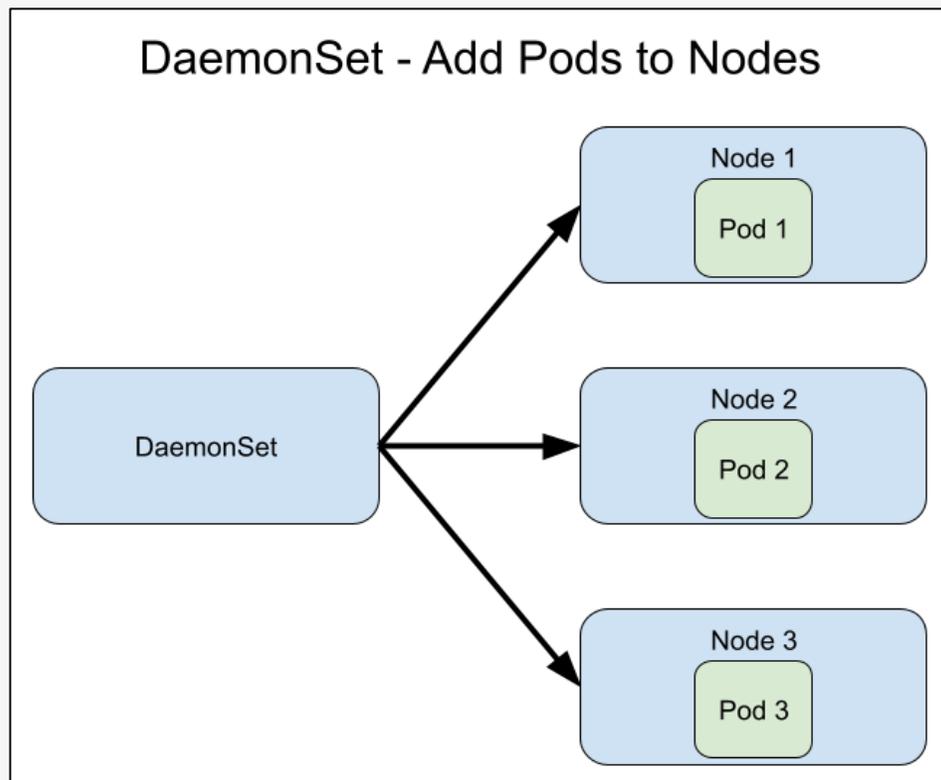
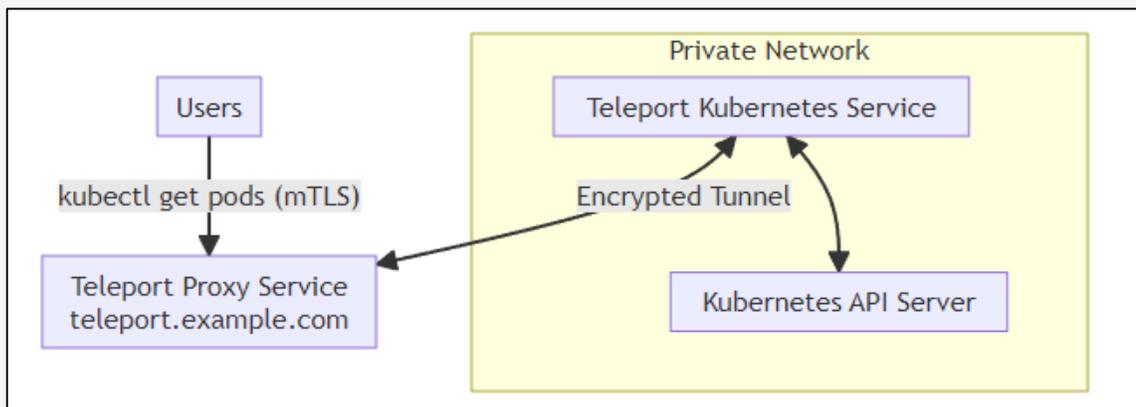
```
ec2-user@ip-10-0-0-80 ~$ ls
ec2-user@ip-10-0-0-80 ~$ pwd
/home/ec2-user
ec2-user@ip-10-0-0-80 ~$ touch test.sh
ec2-user@ip-10-0-0-80 ~$ chmod 777 test.sh
ec2-user@ip-10-0-0-80 ~$ ./test.sh
ec2-user@ip-10-0-0-80 ~$ ls
'ISMS-P 인증기준 안내서(2022.4.22) (1).pdf' test.sh
ec2-user@ip-10-0-0-80 ~$ monitor realtime
```

## 5. SSH에 대한 접근 제어

---



## 6. Kubernetes에 대한 접근 제어



```
C:\Users\j in\teleport-v13.1.0-windows-amd64-bin\teleport>kubectl get pod -o wide
NAME          READY  STATUS   RESTARTS  AGE  IP             NODE
teleport-agent-0  1/1    Running  0         2d2h  192.168.201.140  ip-192-168-201-17.ap-no
```

## 6. Kubernetes 에 대한 접근 제어

```
C:\Users\jin\teleport-v13.1.0-windows-amd64-bin\teleport>tsh kube login demo-cluster-dev
Logged into Kubernetes cluster "demo-cluster-dev". Try 'kubectl version' to test the connection.

C:\Users\jin\teleport-v13.1.0-windows-amd64-bin\teleport>kubectl get pods
NAME                READY   STATUS    RESTARTS   AGE
teleport-agent-0    1/1     Running   0           40h

C:\Users\jin\teleport-v13.1.0-windows-amd64-bin\teleport>kubectl get nodes
NAME                                                    STATUS    ROLES    AGE   VERSION
ip-192-168-200-9.ap-northeast-2.compute.internal      Ready    <none>   41h   v1.25.9-eks-0a21954
ip-192-168-201-17.ap-northeast-2.compute.internal     Ready    <none>   41h   v1.25.9-eks-0a21954
```

```
{
  "kubernetes_groups": [
    "system:authenticated",
    "system:masters"
  ],
  "kubernetes_users": [
    "tele-admin"
  ],
  "login": "tele-admin",
  "namespace": "default",
  "proto": "kube",
  "request_path": "/api/v1/namespaces/default/pods",
  "resource_api_group": "core/v1",
  "resource_kind": "pods",
  "resource_namespace": "default",
  "response_code": 200,
  "server_id": "588de4da-c644-4eb2-bbb5-775cf7a58c0d",
  "time": "2023-06-21T18:23:06.526Z",
  "uid": "103c77e8-e15c-490f-b0f8-b48adf947fb3",
  "user": "tele-admin",
  "verb": "GET"
}
```

```
{
  "kubernetes_cluster": "demo-cluster-dev",
  "kubernetes_groups": [
    "system:authenticated",
    "system:masters"
  ],
  "kubernetes_users": [
    "tele-admin"
  ],
  "login": "tele-admin",
  "namespace": "default",
  "proto": "kube",
  "request_path": "/api/v1/nodes",
  "resource_api_group": "core/v1",
  "resource_kind": "nodes",
  "response_code": 200,
  "server_id": "588de4da-c644-4eb2-bbb5-775cf7a58c0d",
  "time": "2023-06-21T18:23:10.262Z",
  "uid": "cc069f34-a708-493f-966d-28b3fdf5c1d0",
  "user": "tele-admin",
  "verb": "GET"
}
```

### COMMAND EXECUTION FAILED

```
1 {
2   "addr.local": "10.100.0.1:443",
3   "addr.remote": "175.197.129.31:65464",
4   "cluster_name": "teleport.jinchoi.net",
5   "code": "T3002E",
6   "command": "bash",
7   "ei": 2,
8   "event": "exec",
9   "kubernetes_cluster": "demo-cluster-dev",
10  "kubernetes_container_image": "public.ecr
11  "kubernetes_container_name": "teleport",
12  "kubernetes_groups": [
13    "system:authenticated",
14    "system:masters"
15  ]
16 }
```

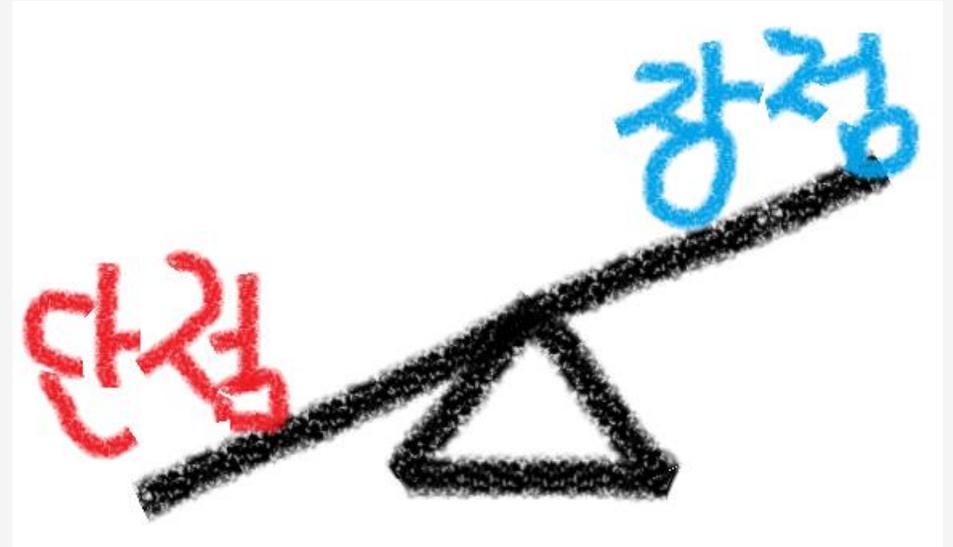
# (굉장히 주관적인) 결론

## 장점

- **무료** 인데 아래 기능들이 다 지원됨
- DB 접근 인증/권한 제어, 감사 로그 확인 가능
- 다양한 형태의 설치 방법 및 운영 방법을 제공하여, 고객 환경에 맞는 유연한 설치 가능
- AWS 기준 다양한 형태의 DB 지원
- **서버/쿠버네티스/웹/데스크탑/Mac OS 에 대한 추가적인 접근 제어 기능**
- 다양하고 디테일한 사용 가이드 및 슬랙 커뮤니티 활성화
- 2FA 지원, Syslog 전송(별도 작업 필요) 가능

## 단점

- **SSO 연동 불가**
- DML, DCL, DDL 제어 불가
- 구축 및 운영에 대한 **리소스가 상용에 비해 상대적으로 큼**
- **컴플라이언스 맞춤형 기능 제공이 없어 별도 보완 대책이 필요함**  
(ex. DB 테이블 목록 불러오기 및 테이블 별 권한 부여, DB 변경사항 자동 반영, Maskign, GUI 기반 인터페이스, DB 테이블 단위 권한 관리)
- Only Shell 기반
- 긴급 장애 시 즉각적인 기술지원 기대 어려움
- **기존 구축되어 있는 DB 접근제어가 있으므로, 새로 구축 시 사용자 경험에 대한 우려 (추후 다시 사달라고 하기도 애매함...)**



하지만, 회사 사정에 따라 '장점 > 단점' 이 될 수도...

# Q&A

