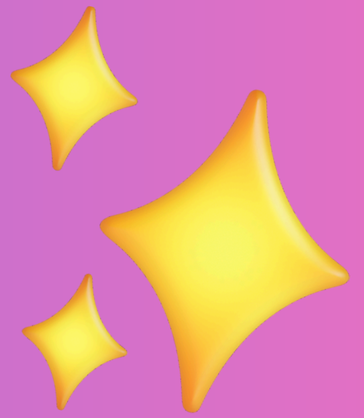
SCC

DEVELOPERS CONFERENCE

2025



BUILDING A ZERO-TRUST ACCESS MANAGEMENT WITH TELEPORT

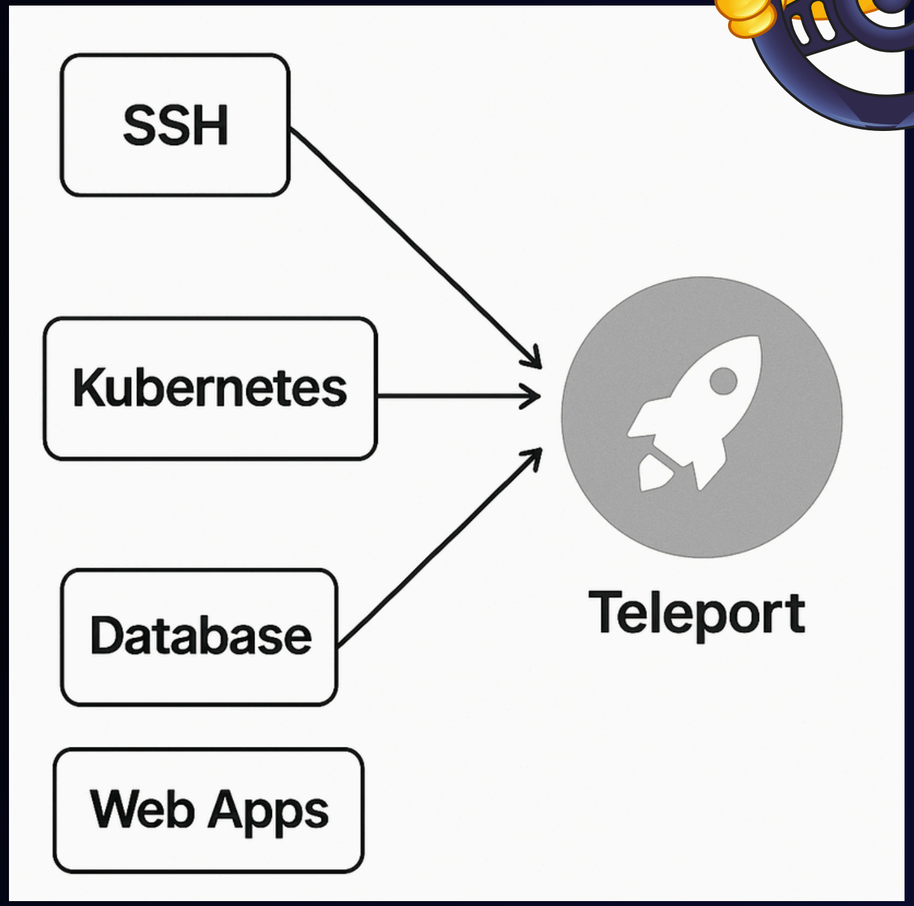
PRESENTED BY: GIRISH MAHABIR
TEAM LEAD AT OCEANDBA

Context & Business Drivers

Hybrid Cloud Growth: Organizations connect on-prem servers, public cloud VMs, and managed Kubernetes clusters.

Security Gaps: Static keys and multiple access tools increase attack surface and overhead.

Compliance Pressure: ISO 27001, SOC 2, GDPR, NIST SP 800-53 require strong, auditable access controls.

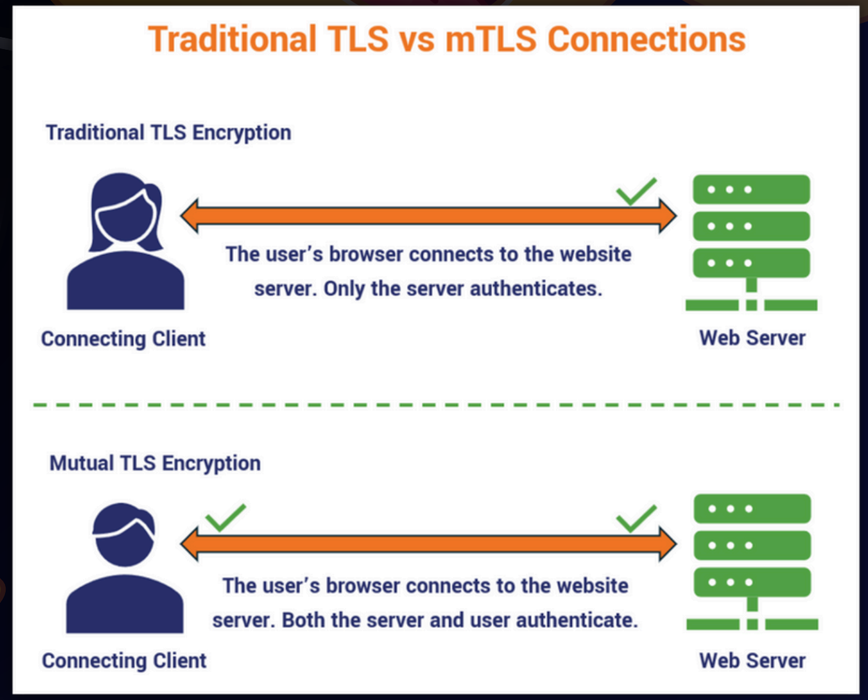


ZERO-TRUST SECURITY FUNDAMENTALS

- **Never Trust, Always Verify:** Assume breaches and verify every request.

- **NIST SP 800-207 Pillars:**
  - **Identity:** Short-lived certificates for users.
  - **Device:** Node health checks before granting access.
  - **Network:** mTLS tunnels instead of open trusts.
  - **Environment:** Dynamic authorization using user traits -> Attribute-Based Access Control (ABAC)

- **Benefits:**
  - Fewer lateral movements.
  - Instant revocation and session logs.

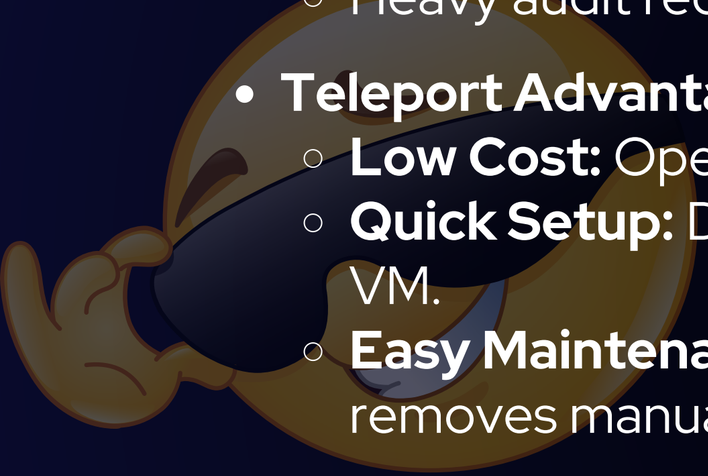


TELEPORT COMMUNITY EDITION FEATURE-TO-COMPLIANCE MAPPING

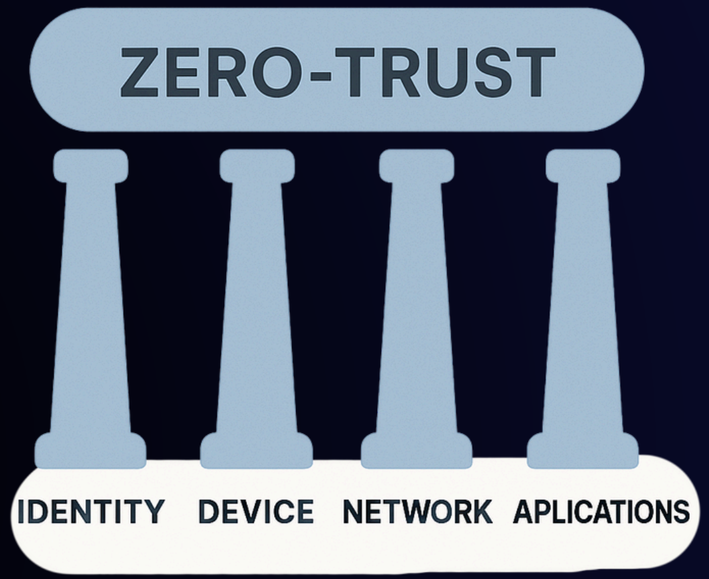
Teleport Feature	Compliance Need	Reference Standard(s)	Notes
Role-Based Access Control (RBAC)	Access Control (Least Privilege, Segregation of Duties)	ISO/IEC 27001 A.9; NIST SP 800-53 AC-2; PCI DSS Req 7	Fine-grained permissions model ensures minimal rights per role.
Session Recording & Audit Logs	Audit & Accountability	ISO/IEC 27001 A.12.4; NIST SP 800-53 AU-2; SOC 2 CC6.5	Records and exports session data for forensics and continuous monitoring.
Multi-Factor Authentication (MFA)	Authentication Security	PCI DSS Req 8.3; HIPAA Security Rule; NIST SP 800-63	Per-session MFA (hardware/software tokens) for SSH/K8s.
Certificate-Based Authentication (Short-Lived)	Identification & Authentication	ISO/IEC 27001 A.9.2; NIST SP 800-53 IA-5	CA issues ephemeral X.509/SSH certs for all sessions (GitHub)
Access to SSH, Kubernetes, Databases, Web Apps	Data Access Security	ISO/IEC 27001 A.10.1; HIPAA Security Rule (Technical Safeguards)	Unified proxy for multiple resource types without VPN.
Just-In-Time Access Requests & Reviews	Time-Limited Access Control	NIST SP 800-53 AC-2(5); SOC 2 Trust Service Criteria CC4 (Monitoring of Controls)	CLI-based JIT role requests minimize standing privileges.
Single Sign-On (GitHub) Integration	Identity & Access Management	ISO/IEC 27001 A.9.4; NIST SP 800-63 C (Federation) (NIST); PCI DSS Req 8	GitHub-only SSO connector in open-source edition.
Encryption of Data in Transit (mTLS)	Data Protection	PCI DSS Req 4; HIPAA Security Rule (Technical Safeguards)	Enforces mTLS for all protocol communications (GitHub)
API & Extensibility (IaC, SIEM, ITSM integrations)	Integration & Monitoring	SOC 2 Trust Service Criteria CC4; NIST SP 800-53 AU-6	Supports Terraform, Kubernetes Operator, SIEM plugins, Slack/Teams alerts.

SME & STARTUP ADOPTION FOCUS

- **Challenges for Start Ups/SMEs:**
  - Tight budgets and small DevOps teams.
  - Limited security expertise.
  - Heavy audit requirements.



- **Teleport Advantages:**
  - **Low Cost:** Open-source core; optional paid features.
  - **Quick Setup:** Deploy in minutes as a container or VM.
  - **Easy Maintenance:** Auto certificate rotation removes manual updates.



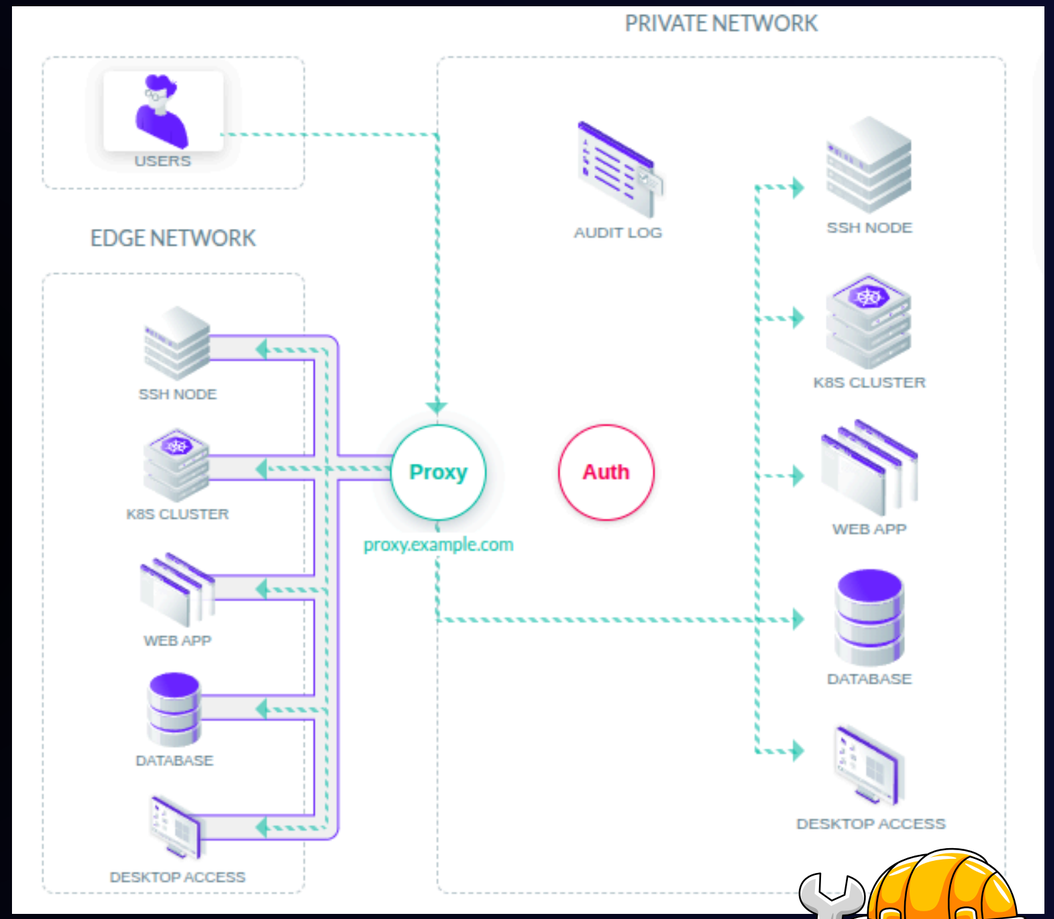
- **Standards Alignment:**
  - **NIST SP 800-53:** Controls AC-2 (Account Management), AC-17 (Remote Access).
  - **ISO 27001 Annex A:** A.9 Access Control, A.12 Ops Security.
  - **Audit Logs:** Built-in sessions logging support SOC 2, GDPR, PCI-DSS.

INTRODUCING TELEPORT

- **What Is Teleport?** Open-source access plane unifying WEB-APP, SSH, Kubernetes, and database access.
- **Key Features:**
  - Certificate-based login instead of static SSH keys.
  - Central RBAC with dynamic roles.
  - Session recording and audit logs.
- **Deploy Options:**
  - Docker Compose, Helm chart, or binaries.

TELEPORT CORE ARCHITECTURE

- **Auth Server & CA:** Issues short-lived certificates.
- **Proxy Service:** Receives connections and forwards via mTLS.
- **Node Agents:** SSH, Kubernetes proxy, and DB proxy.
- **Key Management:**
  - **Hot Root Key:** Online, issues user certs.
  - **Cold Root Key:** Offline, for key rotation only.



https://goteleport.com/how-it-works/

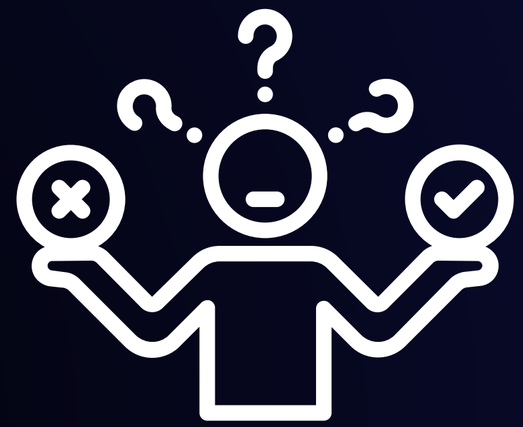
ROLE & POLICY MODEL

- **Roles:** Specify allowed logins, commands, and resources.
- **Traits:** User attributes like department for dynamic access.
- **Policy Files:** YAML, version-controlled.

```
kind: role
metadata:
  name: DBManager
spec:
  options:
    # Desktop access & sharing
    create_desktop_user: true
    desktop_clipboard: true
    desktop_directory_sharing: true

    # Session security
    enhanced_recording: [command, network]
    record_session:
      desktop: true
      ssh: best_effort
    require_session_mfa: 1
    max_session_ttl: 30h
    # SSO/MFA
    idp:
      saml:
        enabled: true

  allow:
    # Unix logins
    logins: [root, db-manager]
    # Target filtering
    node_labels:
      "DB": "True"
    database_labels:
      "DB": "True"
    database_names: ["*"]
    # Host groups & sudo rules
    host_groups: [mysql, nginx]
    host_sudoers:
      - 'ALL = (root) NOPASSWD: /usr/bin/systemctl restart
mysql.service'
version: v7
```



DEMO TEASER

- **SSH:** Live cert issuance and revocation.
- **Kubernetes:** tsh kube login and kubectl exec.
- **Database:** tsh db login with query logs.
- **Audit:** Replay sessions in Web UI.

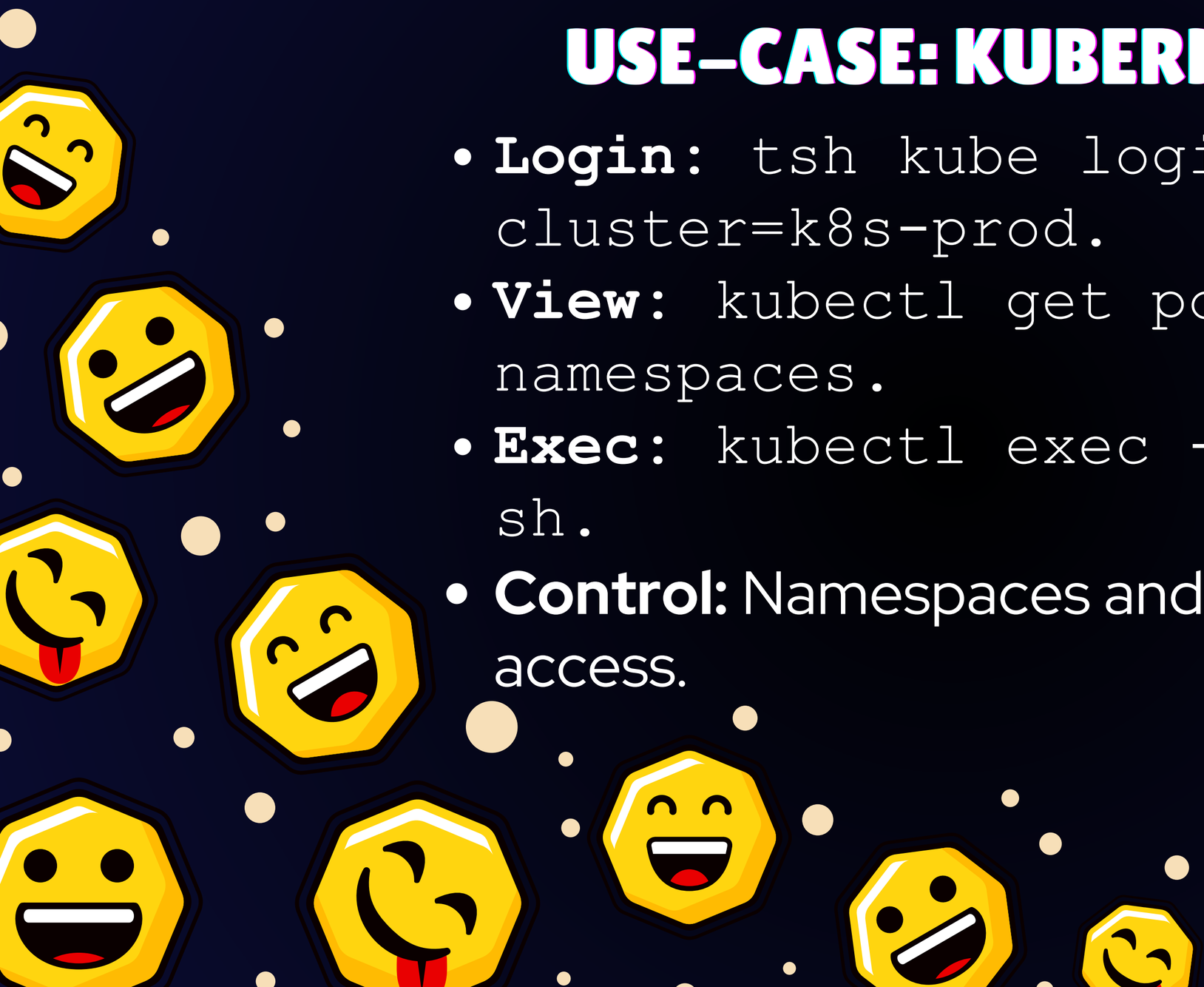
USE-CASE: EPHEMERAL SSH ACCESS

- **Login:** `tsh login --proxy=proxy.example.com --user=alice` (12h cert).
- **Access:** tsh ssh node1 via mTLS.

DEMO TIME

USE-CASE: KUBERNETES ACCESS

- **Login:** `tsh kube login --cluster=k8s-prod.`
- **View:** `kubectl get pods --all-namespaces.`
- **Exec:** `kubectl exec -it demo-pod -- sh.`
- **Control:** Namespaces and groups restrict access.



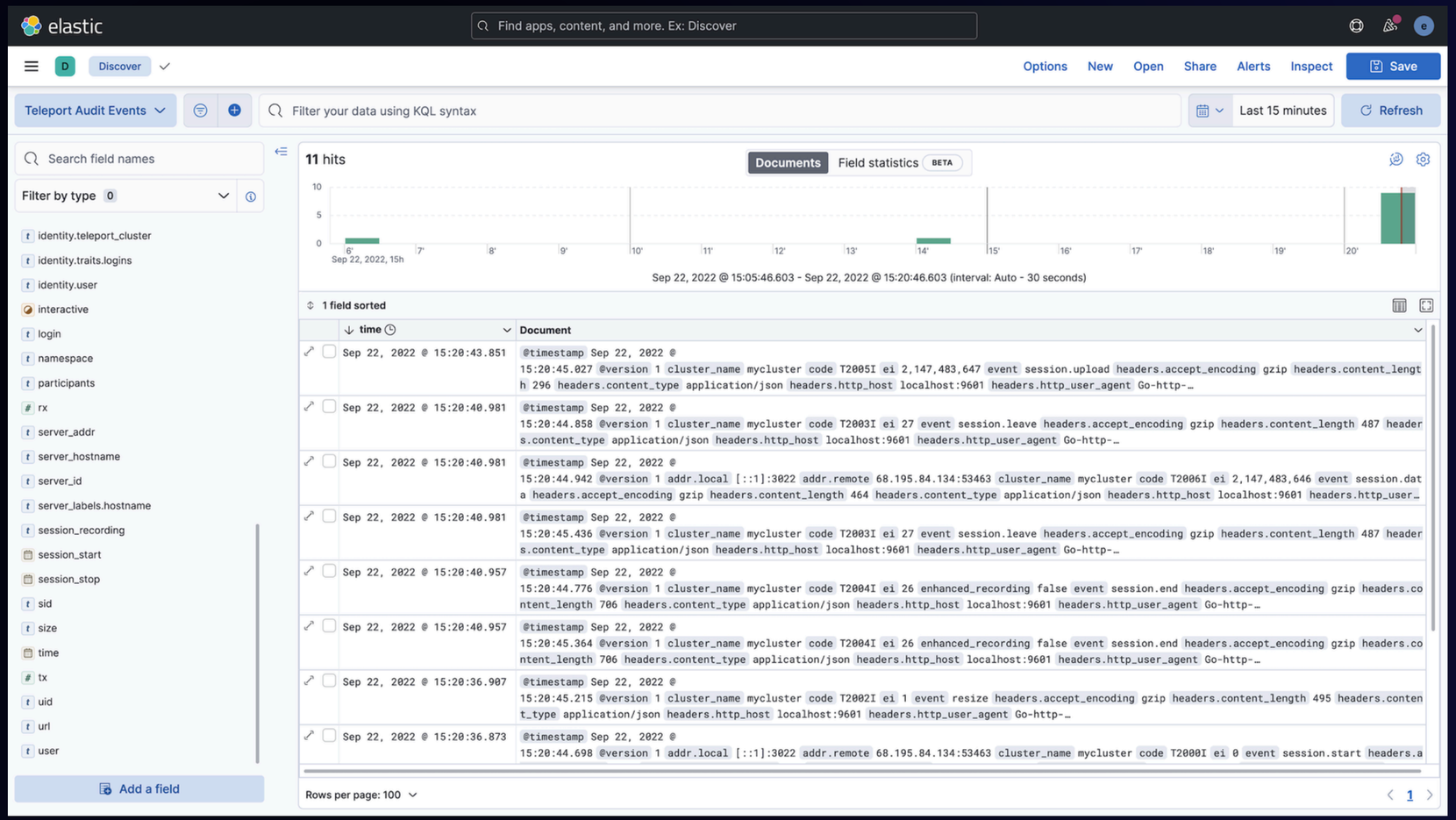
USE-CASE: DATABASE ACCESS

- **Connect:** `tsh db connect h-GM-teleport-db --db-user=db-manager --db-name=information_schema.`
- **Query:** `select TABLE_NAME from tables limit 5;.`
- **Log:** Each query saved with user and time.

Type	Description	Created (UTC)	
Database Session Ended	User [girishmahabir.gm@gmail.com] has disconnected from database [information_schema] on [h-GM-teleport-db]	2025-07-14T07:23:30.561Z	Details
Certificate Issued	User certificate issued for [girishmahabir.gm@gmail.com]	2025-07-14T07:23:05.504Z	Details
Database Query	User [girishmahabir.gm@gmail.com] has executed query [select TABLE_NAME from tables limit 5] in database [information_schema] on [h-GM-teleport-db]	2025-07-14T07:22:50.676Z	Details
Database Query	User [girishmahabir.gm@gmail.com] has executed query [select @@version_comment limit 1] in database [information_schema] on [h-GM-teleport-db]	2025-07-14T07:22:19.485Z	Details
Database Query	User [girishmahabir.gm@gmail.com] has executed query [show tables] in database [information_schema] on [h-GM-teleport-db]	2025-07-14T07:22:01.640Z	Details
Database Query	User [girishmahabir.gm@gmail.com] has executed query [show databases] in database [information_schema] on [h-GM-teleport-db]	2025-07-14T07:22:01.417Z	Details
Database Session Started	User [girishmahabir.gm@gmail.com] has connected to database [information_schema] as [db-manager] on [h-GM-teleport-db]	2025-07-14T07:22:01.090Z	Details
Certificate Issued	User certificate issued for [girishmahabir.gm@gmail.com]	2025-07-14T07:21:59.477Z	Details

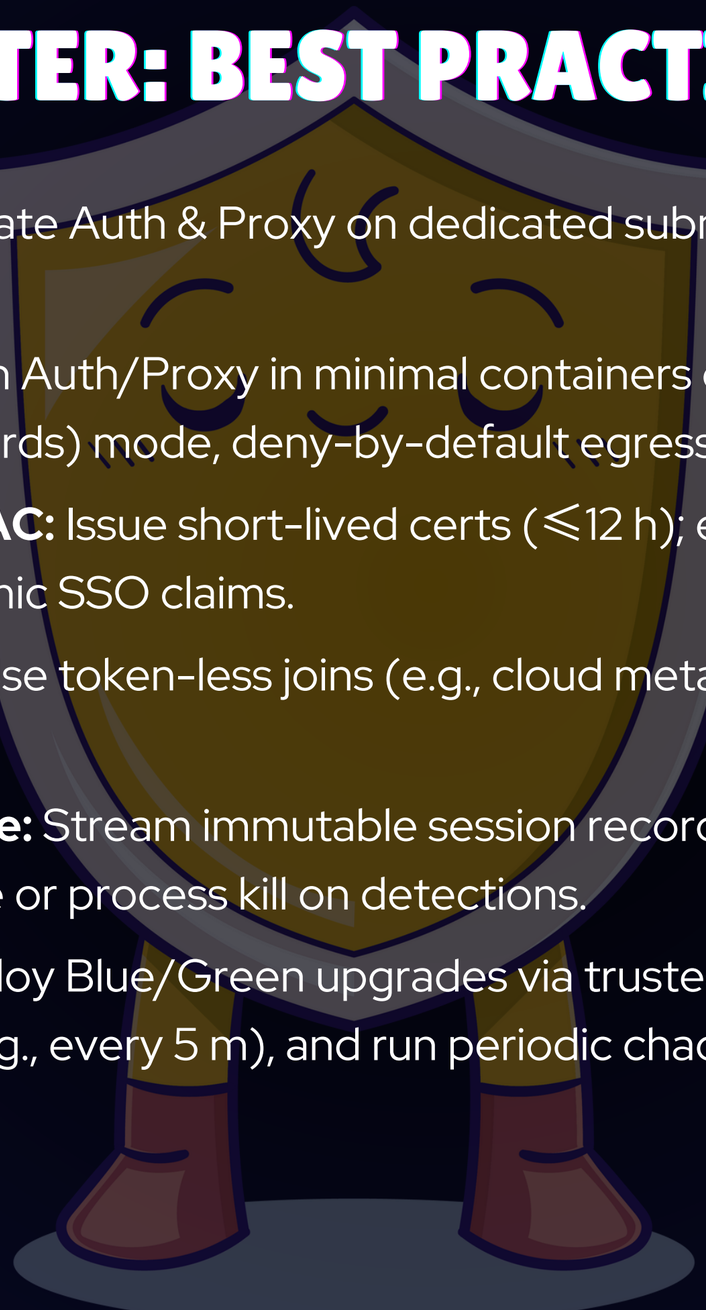
UNIFIED AUDIT & VISIBILITY

- **Web UI:** Dashboard for sessions, events, users.
- **Filters:** By user, resource, time.
- **SIEM:** Send logs to ELK, Splunk, or Wazuh.
- **Visual:** UI with highlighted filters and timeline



https://goteleport.com/docs/admin-guides/management/export-audit-events/elastic-stack/

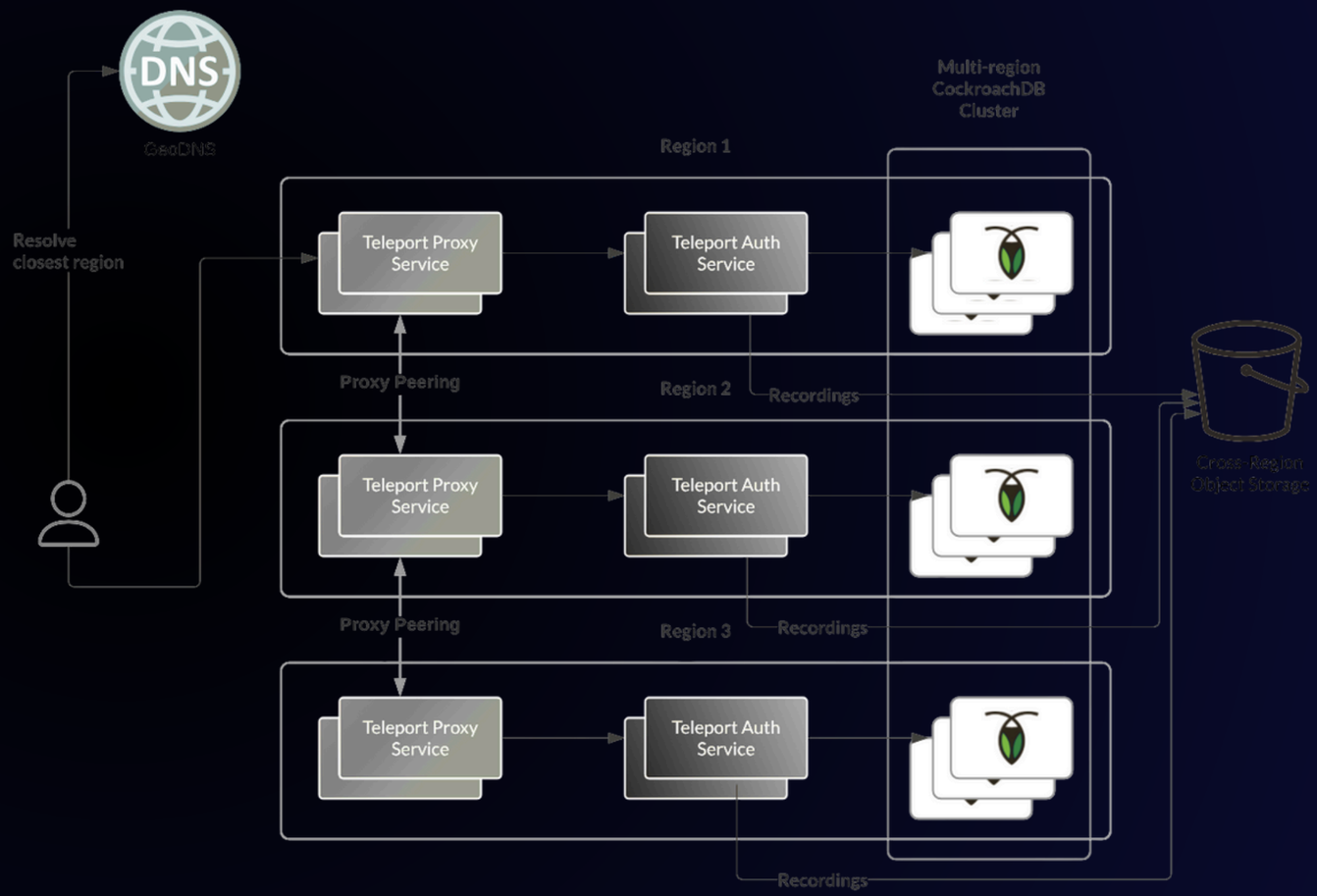
TELEPORT CLUSTER: BEST PRACTICES & HARDENING



- **Zero-Trust Architecture:** Isolate Auth & Proxy on dedicated subnets; enforce mTLS with reverse-tunnel-only inbound (443/TCP).
- **Control Plane Hardening:** Run Auth/Proxy in minimal containers or distroless images, enable **FIPS** (Federal Information Processing Standards) mode, deny-by-default egress, and automate patch updates.
- **Strong Authentication & RBAC:** Issue short-lived certs (⩽12 h); enforce WebAuthn/FIDO2 MFA; model least-privilege roles with dynamic SSO claims.
- **Secure Node On-boarding:** Use token-less joins (e.g., cloud metadata) and ephemeral machine IDs to avoid static creds on disk.
- **Centralized Audit & Response:** Stream immutable session recordings/logs to S3 (Object Lock); leverage active-response for quarantine or process kill on detections.
- **Operational Excellence:** Employ Blue/Green upgrades via trusted-cluster mode, schedule encrypted backup of storage backend (e.g., every 5 m), and run periodic chaos drills.

SCALABLE DEPLOYMENT PATTERNS

- **HA Clusters:** Multiple Auth & Proxy behind load balancer.
- **DR:** Backup CA keys offsite.
- **IaC:** Terraform modules for repeatable setup.
- **K8s Operator:** Helm chart for scale.
- **Visual:** Multi-region Teleport diagram



THANK YOU FOR LISTENING!

DO NOT HESITATE TO ASK ANY QUESTIONS!

- **Resources:**
  - **Teleport Docs**: https://goteleport.com/docs
  - **GitHub**: https://github.com/gravitational/teleport
  - **Slack**: teleport-users@goteleport.slack.com

- **Contact:**
  - **EMAIL**: girishmahabir.gm@gmail.com
  - **Linkedin**: www.linkedin.com/in/girish-mahabir

THANK YOU FOR LISTENING!

QR CODE TO DOWNLOAD THE SLIDES