

Gravitational Teleport on AWS

Towards a Safety Culture



- David Bock - dbock@decisiv.com / @bokmann
- Hunter Madison - hmadison@decisiv.com / @355E3B

Let's Discuss

- What is a “Safety Culture”?
- How do we convince users to change the way they access systems?
- What we commonly do for access
- What Teleport gives us
- Demos and Examples

Safety Culture

Changing access

People Don't Change

People Don't Change

- End user workflows are generally set in stone
 - Workflows don't change as the company scales up
 - What is ok with 5 developers isn't ok with 60
- Anything change made that an end user doesn't see immediate benefit in is hard to sell

Laptops getting stolen

- This does happen
- It happened to us
- Rotating credentials aren't fun

Audits

- Standards like
 - ISO 27002
 - PCI DSS
 - ISO 9000
 - FedRamp
 - ISO 9660
 - NIST 500-292

Sometimes you need
to

Sometimes you need to

- *When Security Gets in the Way - Interactions, volume 16, issue 6: Norman, D. A.*
- “The audience, either not understanding the rationale or simply disagreeing with the necessity for the procedures imposed upon them, see these as impediments to accomplishing their jobs.”

Making Security Usable

- Its not good enough to change an existing workflow to make it more secure
- You need to go and provide your users a better experience

**We've all seen this
before**

User Management

- A user playbook
- Which...
 - Creates user accounts
 - Adds ssh keys
 - (Sometimes) tries to keep the UIDs consistent
 - (Sometimes) sets up a `.bash_profile`
 - `EDITOR=emacs`

User Management

- What happens when new people join and need access?
 - Hopefully, their key is provided to you the day they start
 - And they don't need access immediately
 - Script needs to get run everywhere
- What happens when people leave?
 - Script needs to run everywhere again
 - Revocations don't happen as fast as they should

User Management

- What happens when access is used to change application or server state improperly?
 - Installing apps onto boxes scheduled for decommissioning
 - App console schenaginas
- What happens when one developer really wants to connect their blackberry to the vpn and ssh into boxes?
- How do you debug connection issues?

User Management

- This process isn't very usable
- End users don't have a good way to understand what state their user account is in
- We don't have a good way to diagnose access issues
- When something happens, we get minimal logging
 - Usually /etc/security connections

Teleport

Teleport

- Is a system used to implement high availability bastion ssh hosts
- Handles user access and logging user sessions
 - Also lets you share ssh sessions
- Generally stateless
- Open Source with paid enterprise extensions
 - SAML / LDAP / IDP Integration
 - RBAC
 - Kubernetes

SSH Backed

- Built on top of the SSH Protocol
 - Fully interoperable with OpenSSH
 - Integrates with your ssh agent
- Works with most tools built on SSH
 - Ansible!
 - Parminko / Net::SSH!
 - Inspec!

Real sshd replacement

- All of the standard unix stuff works out of the box
- Any text based tool / tui
 - Emacs, Ed, top, mc
- Any alternative shell
 - Zsh, fish, lshell, git-shell
- Respects /etc/passwd; Makes real login sessions

Three Layers

Auth Servers

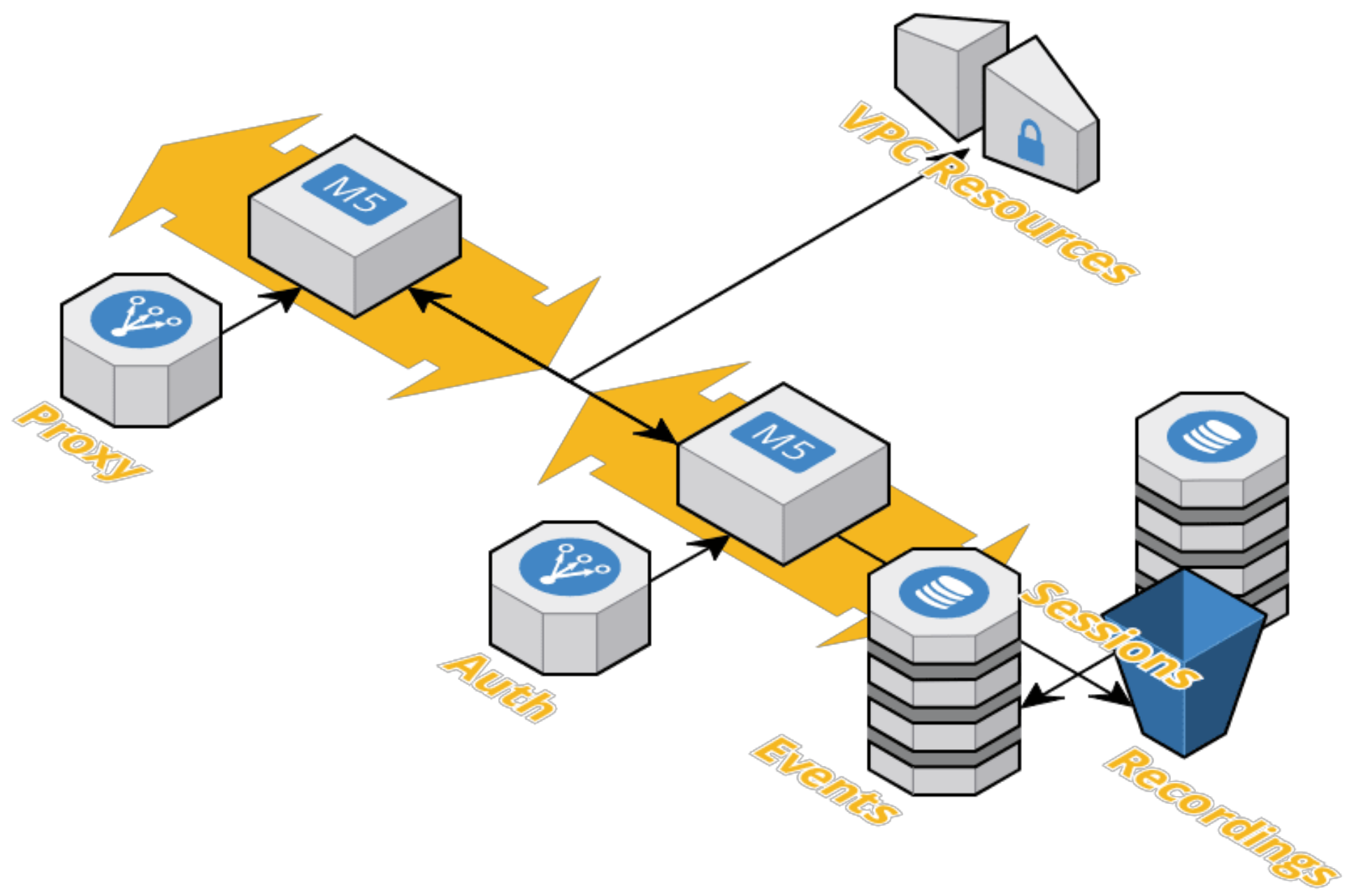
- Manages users, proxies, nodes and trusted clusters
 - This happens via join tokens
 - Or some other IDP for users (on enterprise)
- This is the only stateful component of the system

Proxy Servers

- Public facing endpoint
- Routes all of the traffic to the nodes
- Also hosts the web interface

Nodes

- These are the servers you want to connect to
- They also run teleport
- They only need to be reachable by the proxy and auth servers
- You can run of your nodes inside of a VPC, the user connection gets tunneled through the proxy



Demos!

github.com/hmadison/
dc-devops-teleport