Protecting your Linux environment through Identity Consolidation

Who Am I

Patrick van der Veen

- Director, Sales Engineering – Northern Europe
- 3,5 years @ Delinea (Thycotic / Centrify)
- Over 16 years in pre-sales
- Infrastructure, virtualization, disaster recovery, data security, vulnerability management, penetration testing, endpoint detection and response, Privileged Access Management (PAM).

Agenda

PAM Maturity Model

Use Cases

Functionality

Windows

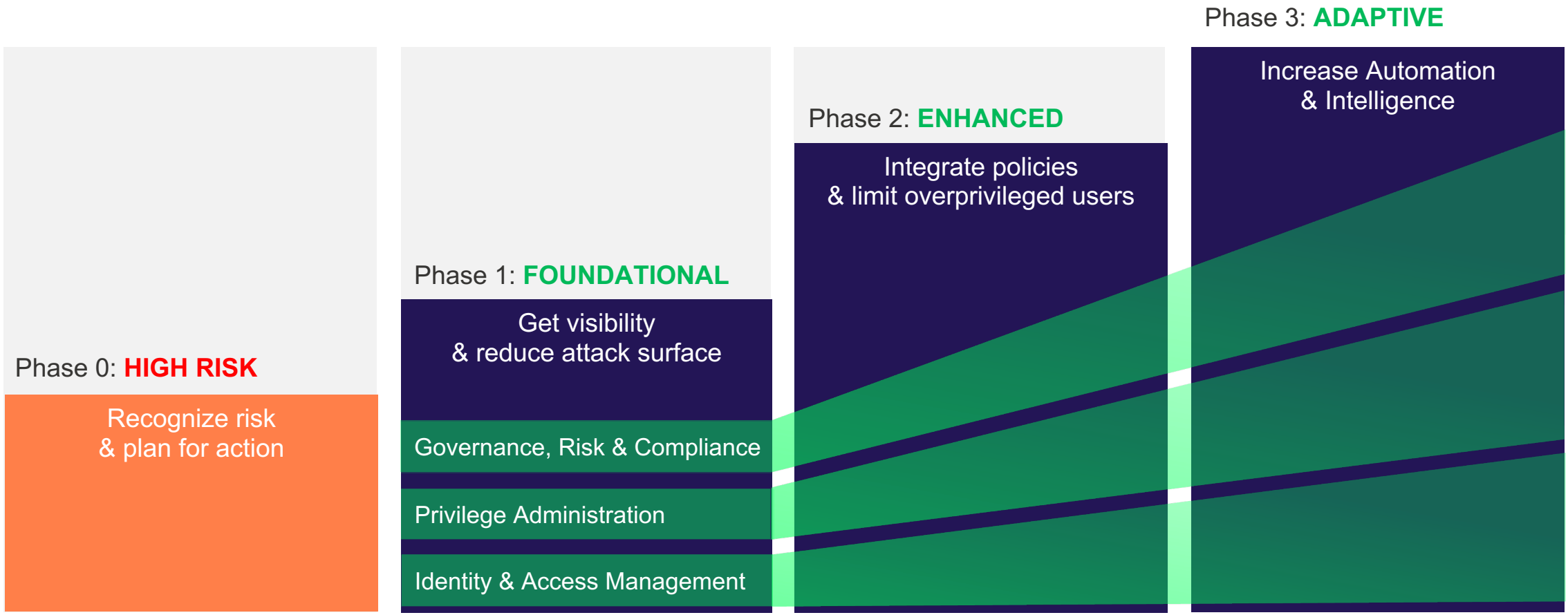
Linux

How it Works

Demo

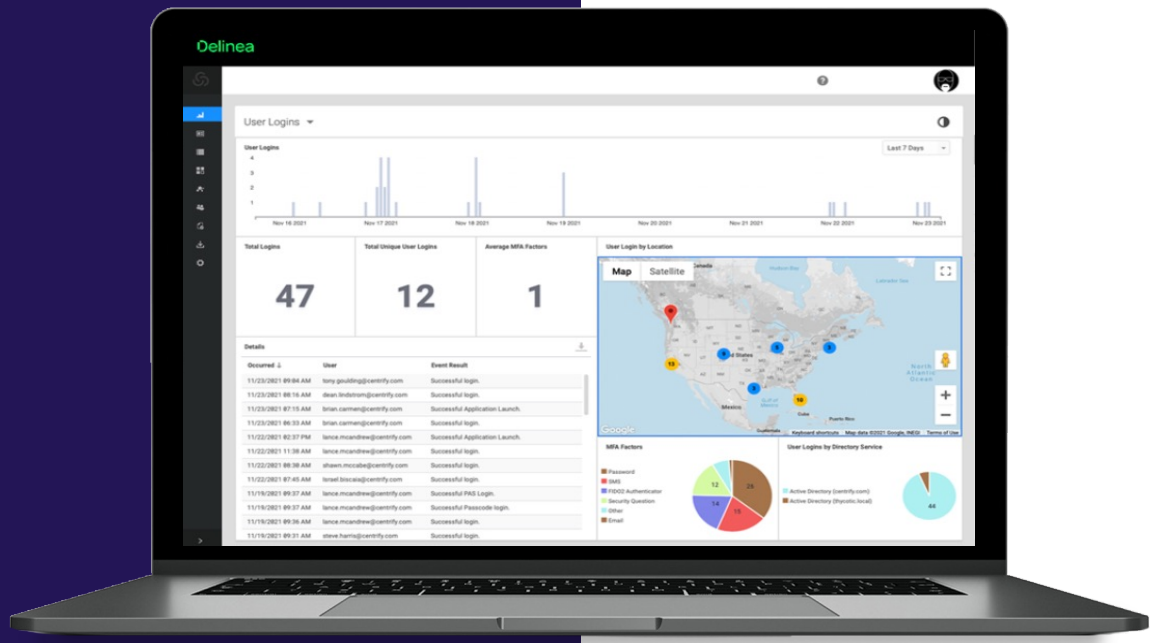
The PAM Maturity Model

Where does Server Suite fit?



Server Suite

Privileged access Management across all Linux, Unix, and Windows systems



- **Consolidate identities**
- **Zero Trust best practices**
- **Implement least privilege**
- **Enforce MFA**
- **Improve compliance**

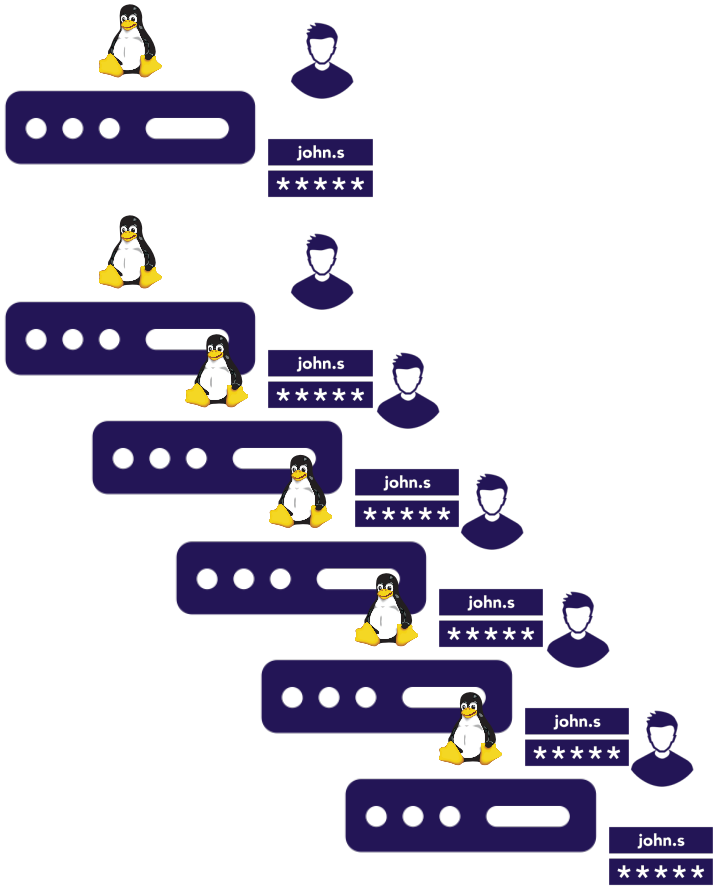
What are we trying to address – Use Cases

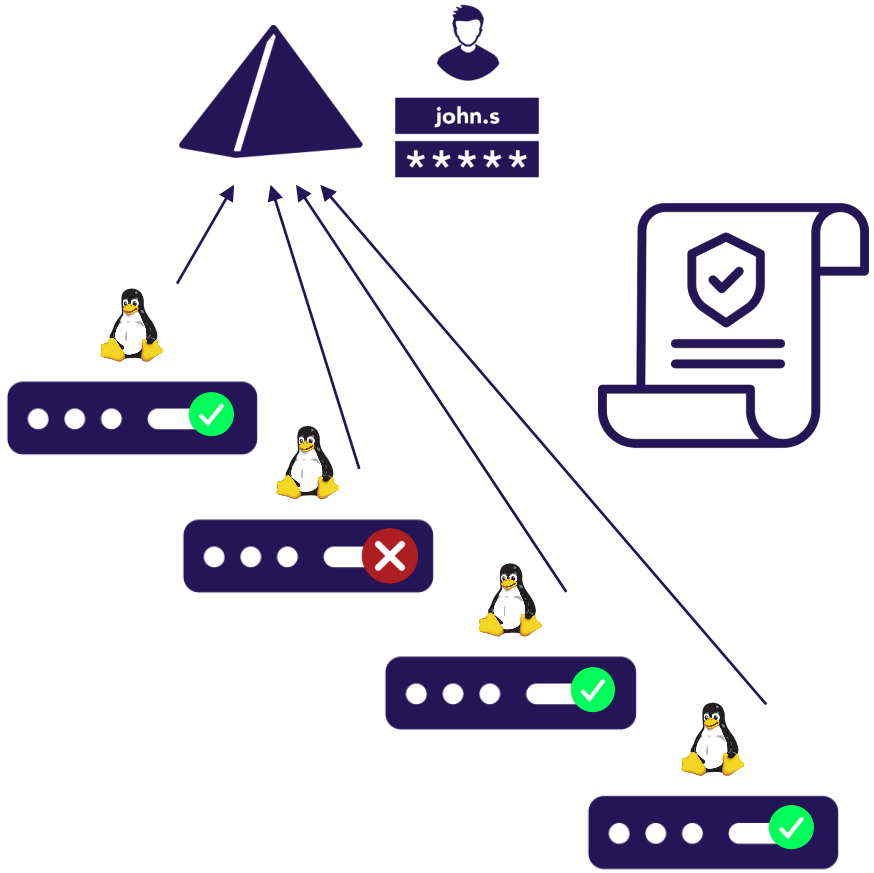
Active Directory focus

- Consolidate identities – Linux / Unix
- Centralized configuration management (GPO) - Linux / Unix
- Reduce attack surface by removing standing privileges – Linux / Unix - SUDO management
    - Just in Time
    - Just Enough
- Host level auditing – Linux / Unix

Identity Consolidation / Active Directory integration

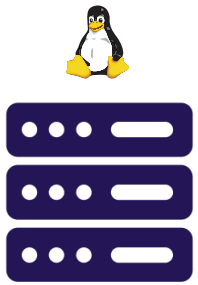
Linux / Unix





Reducing attack surface

Remove standing privileges

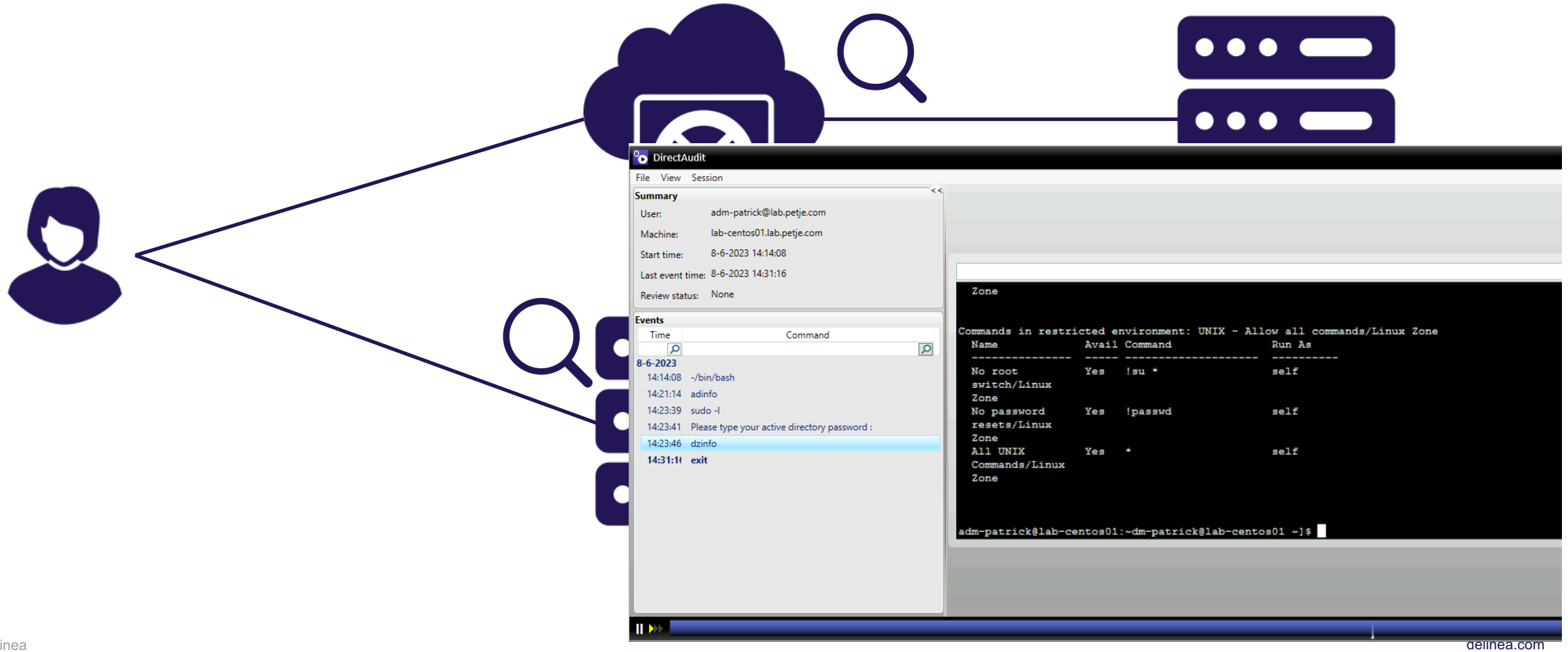


```
[adm-patrick@lab-centos01 ~]$ dzinfo


    Always permit login:
        false


  PAM Application  Avail Source Roles
  ---------------  ----- --------------------
  *                Yes   UNIX Login/Linux
                         Zone


Privileged commands:
  Name             Avail Command               Source Roles
  ---------------  ----- --------------------  --------------------
  No root          Yes   !su *                 UNIX - Allow all
  switch/Linux                                 commands/Linux Zone
  Zone
  No password      Yes   !passwd               UNIX - Allow all
  resets/Linux                                 commands/Linux Zone
  Zone
  All UNIX         Yes   *                     UNIX - Allow all
  Commands/Linux                               commands/Linux Zone
  Zone


Commands in restricted environment: UNIX - Allow all commands/Linux Zone
  Name             Avail Command               Run As
  ---------------  ----- --------------------  ----------
  No root          Yes   !su *                 self
  switch/Linux
  Zone
  No password      Yes   !passwd               self
  resets/Linux
  Zone
  All UNIX         Yes   *                     self
  Commands/Linux
  Zone
```

```
/usr/bin/net, /sbin/iptables, /usr/bin/r
```

Host level auditing

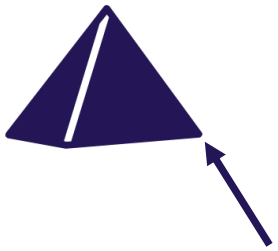
Record always

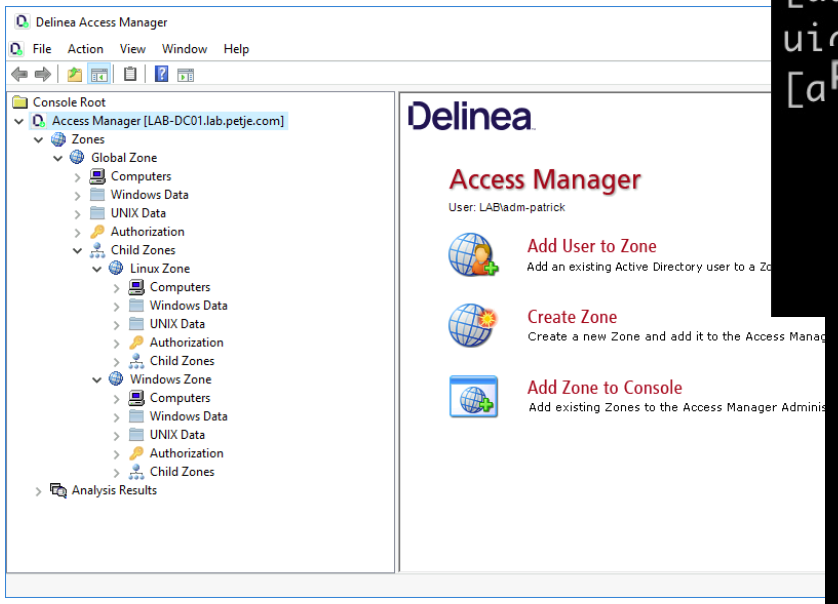


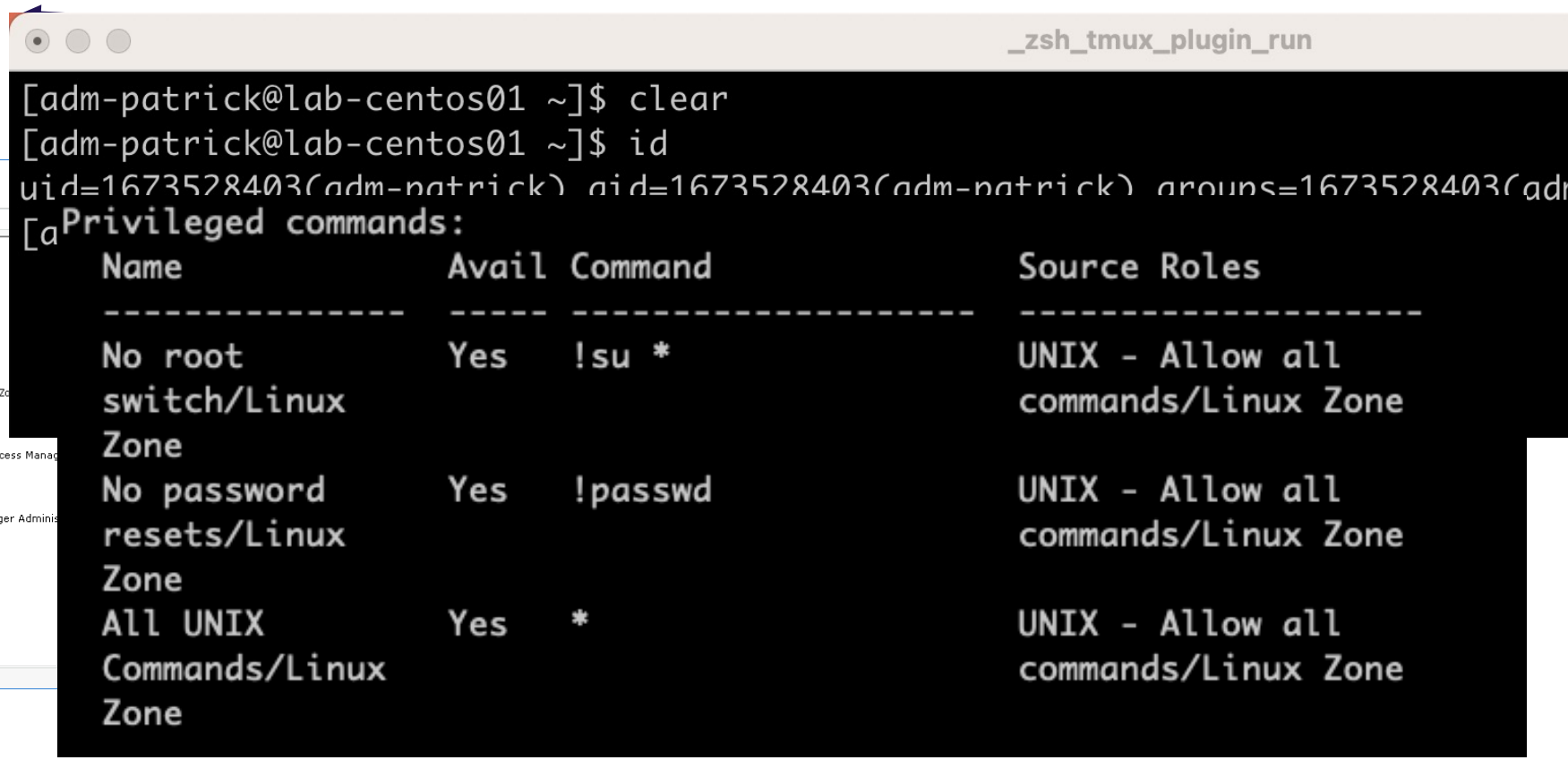
How does it work?

Components involved

Direct Control – Authentication / Authorization / Elevation

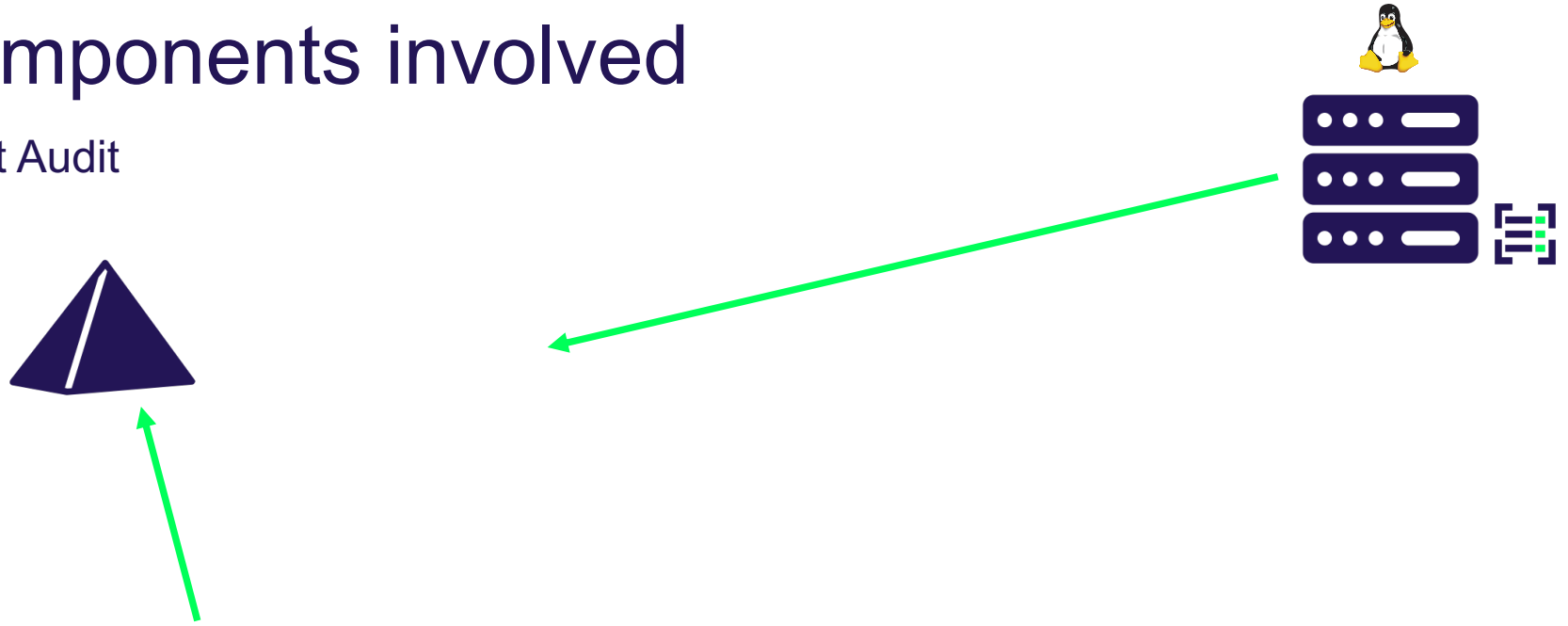


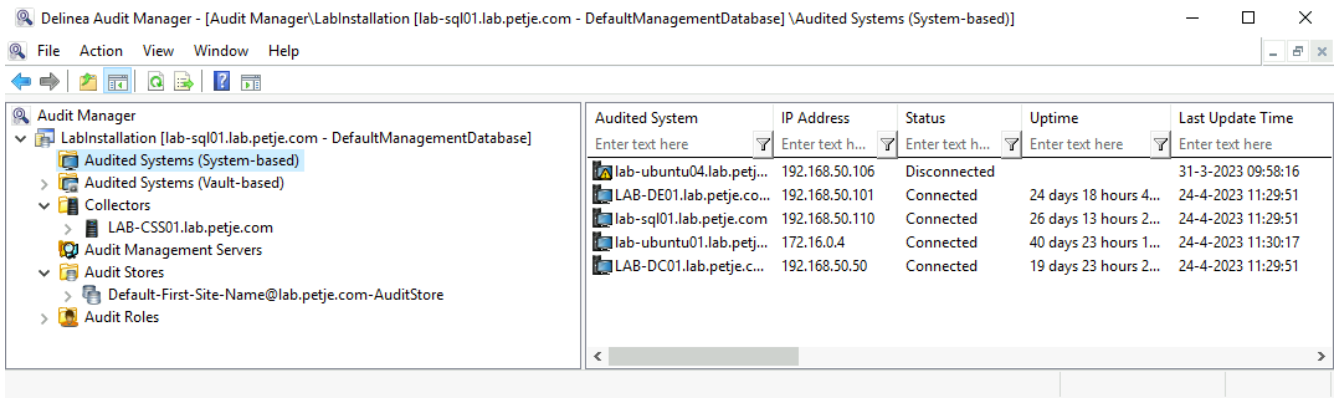


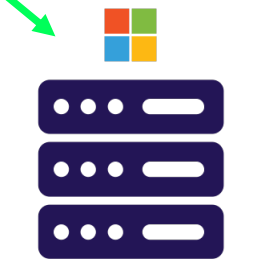


Components involved

Direct Audit





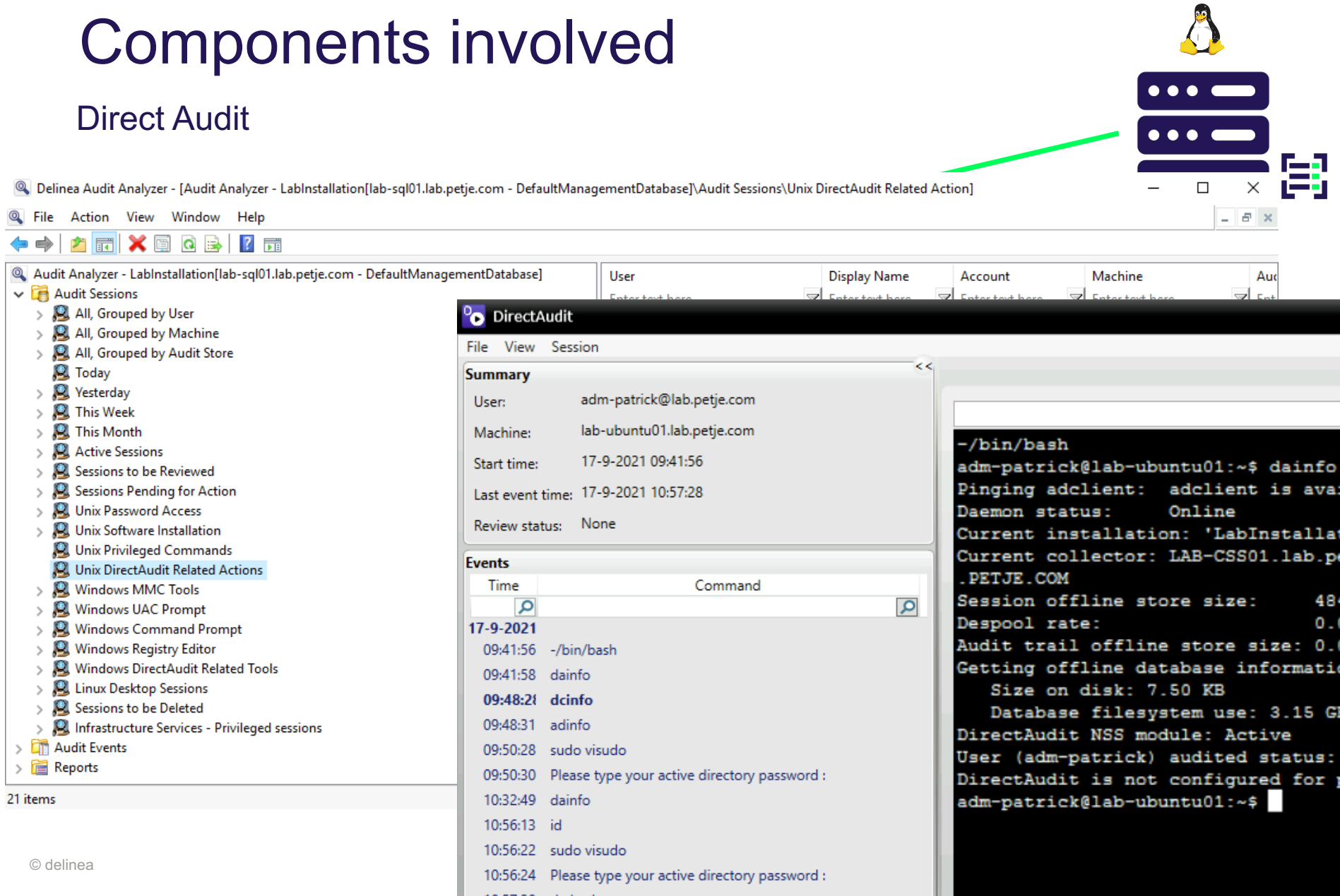


Audit Collector

Audit DB Store

Components involved

Direct Audit



DEMO

Conclusion / Summary

- Consolidate identities – Linux / Unix
- Centralized configuration management (GPO) - Linux / Unix
- Reduce attack surface by removing standing privileges – Linux / Unix - SUDO
    - Just in Time
    - Just Enough
- Host level auditing – Linux / Unix

Thank you

Delinea

Defining the boundaries of access