Successful Security Practices: Counting Failed Login Attempts

Moderator:
Jacob Farmer, Indiana University

Speakers:
Brett Bieber, University of Nebraska-Lincoln

Benn Oshrin, University of California-Berkeley

INTERNET2

InCommon ASSURANCE

Topics

- Brief Introduction to the Profiles and Context
- Case Studies:
  - University of Nebraska-Lincoln
  - University of California-Berkeley
- Your questions here

Compliance vs. Security

- Sometimes you implement a control to achieve compliance
- Sometimes you implement a control to improve security
- Hopefully they're both aimed at the same target, mitigating risk
- However, one is not necessarily a condition of the other
- But can working towards achieving compliance improve security?

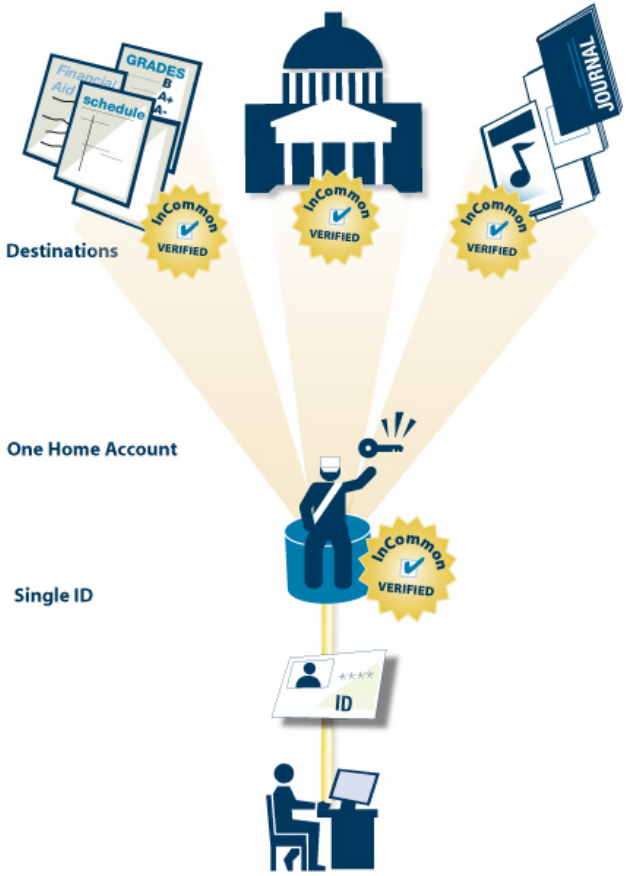
Federated Transactions

Services Relying on External Identities:

- I need to trust you to manage online identities for me?
- What are my risks?
- What are the odds and the degree of harm?

Parties need agreed-upon criteria for identity assurance

Trust. Measuring and balancing: cost, risk, adoption.



Provenance: InCommon Profiles

- US Government FICAM
  - Based on NIST 800-63
  - Assesses comparability
- Profiles
  - Developed for HE
  - Address FICAM requirements with HE flexibility
- Due Diligence
  - What standard do you use now?

InCommon Identity Assurance Profiles

Criteria:

1. Business, Policy and Operational
2. Registration and Identity Proofing
3. Credential Technology
4. Credential Issuance and Management
5. Authentication Process
6. Identity Information Management
7. Assertion Content
8. Technical Environment

Credential Technology

- 4.2.3.3 Strong Resistance to Guessing Authentication Secret
- 1. The Authentication Secret and the controls used to limit online guessing attacks shall ensure that an attack targeted against a given Subject's Authentication Secret shall have a probability of success of less than 2-14 (1 chance in 16,384) over the life of the Authentication Secret. This requires that an Authentication Secret be of sufficient complexity and that the number of invalid attempts to enter an Authentication Secret for a Subject be limited.
- 2. The Authentication Secret shall have at least 10 bits of min-entropy to protect against an untargeted attack.

AuthN Failure Counter

Brett Bieber | University of Nebraska-Lincoln

Why count? | Password Entropy Reqs

- Password Length
- Character Set
- Attempts before lockout
- Lockout duration

New Password Policy Discussion

Please No! | Limiting User Impact

- Faculty, Staff, Students don't want to change!

- Passwords = #1 call to Help Desk

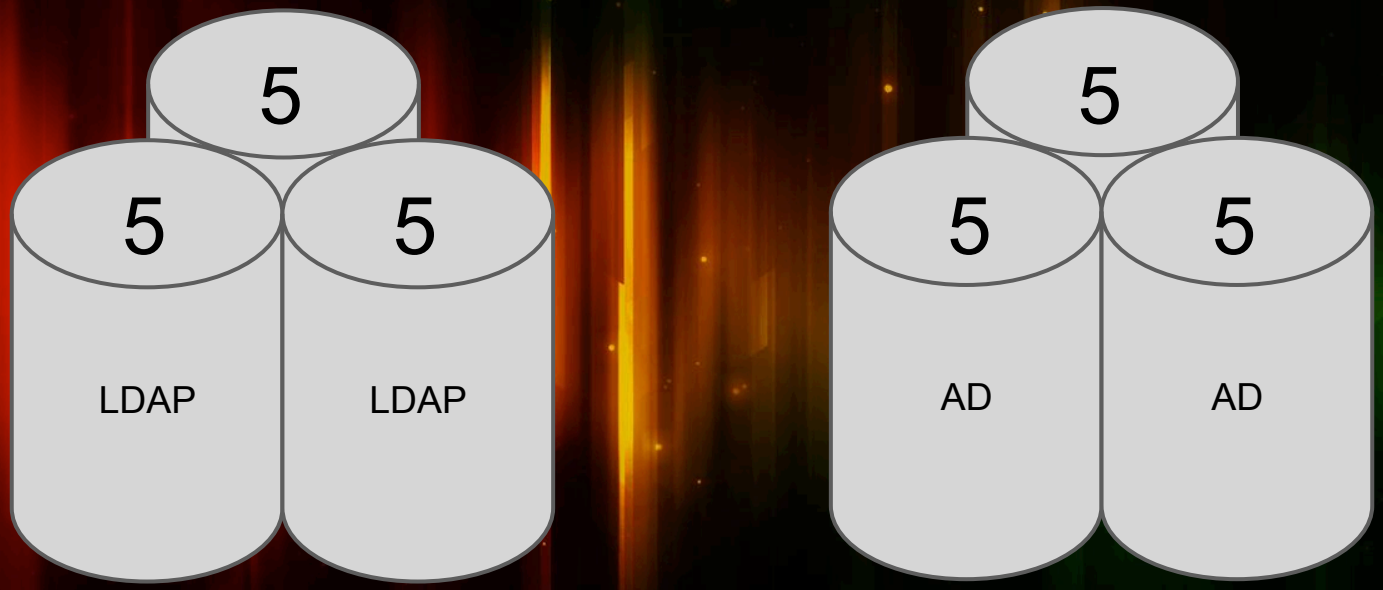
How do I lockout thee?

Let me count the ways.

LDAP + LDAP + LDAP + AD + AD + AD = ????

How do I lockout thee?

Let me count the ways.



LDAP + LDAP + LDAP + AD + AD + AD = **30**

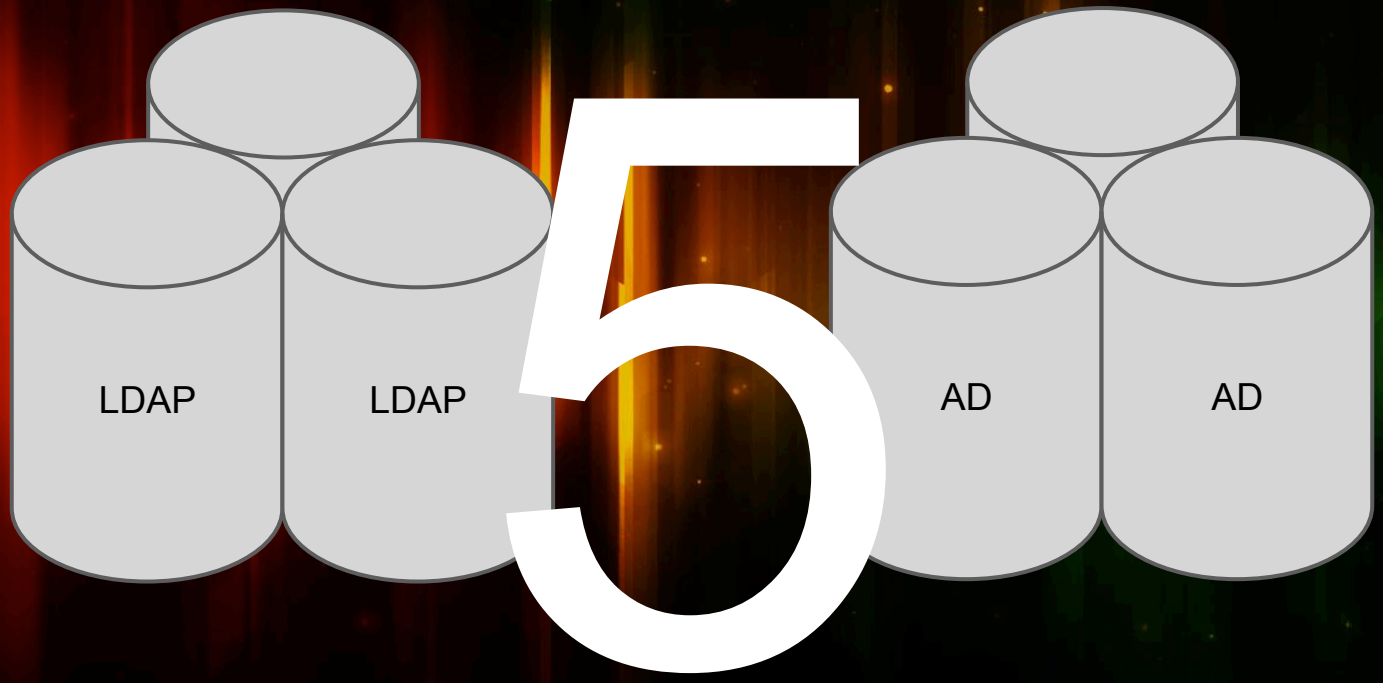
How do I lockout thee?

Let me count the ways.

LDAP + LDAP + LDAP + AD = ????

How do I lockout thee?

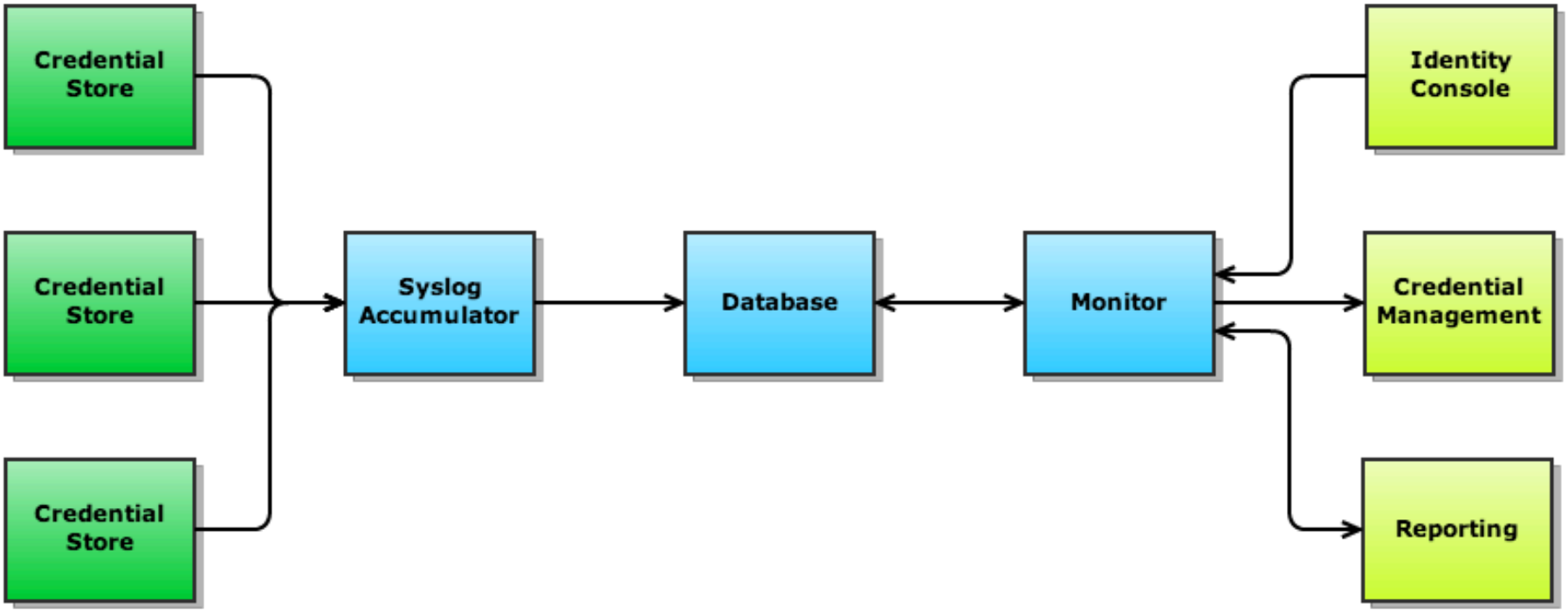
Let me count the ways.



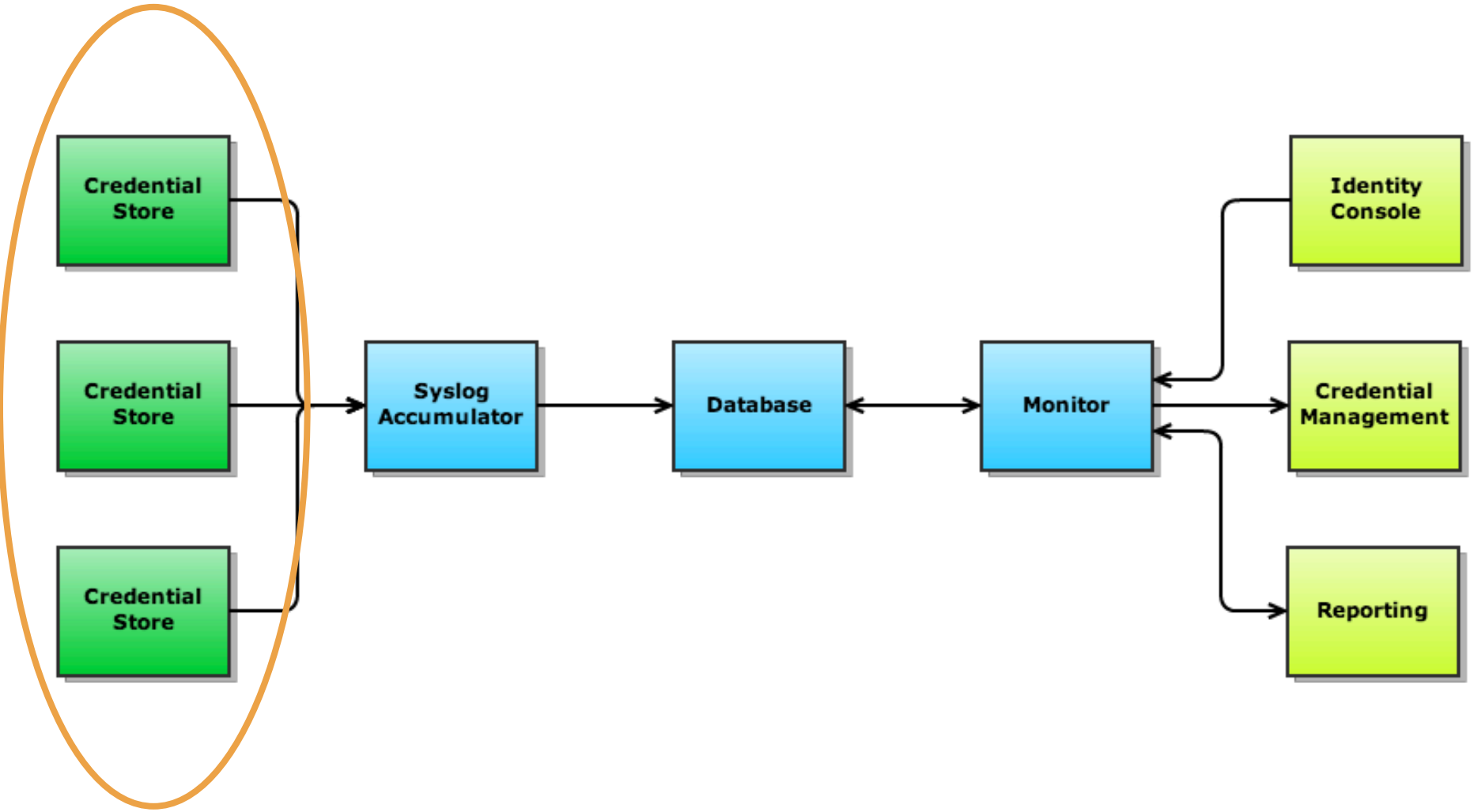
How do I lockout thee?

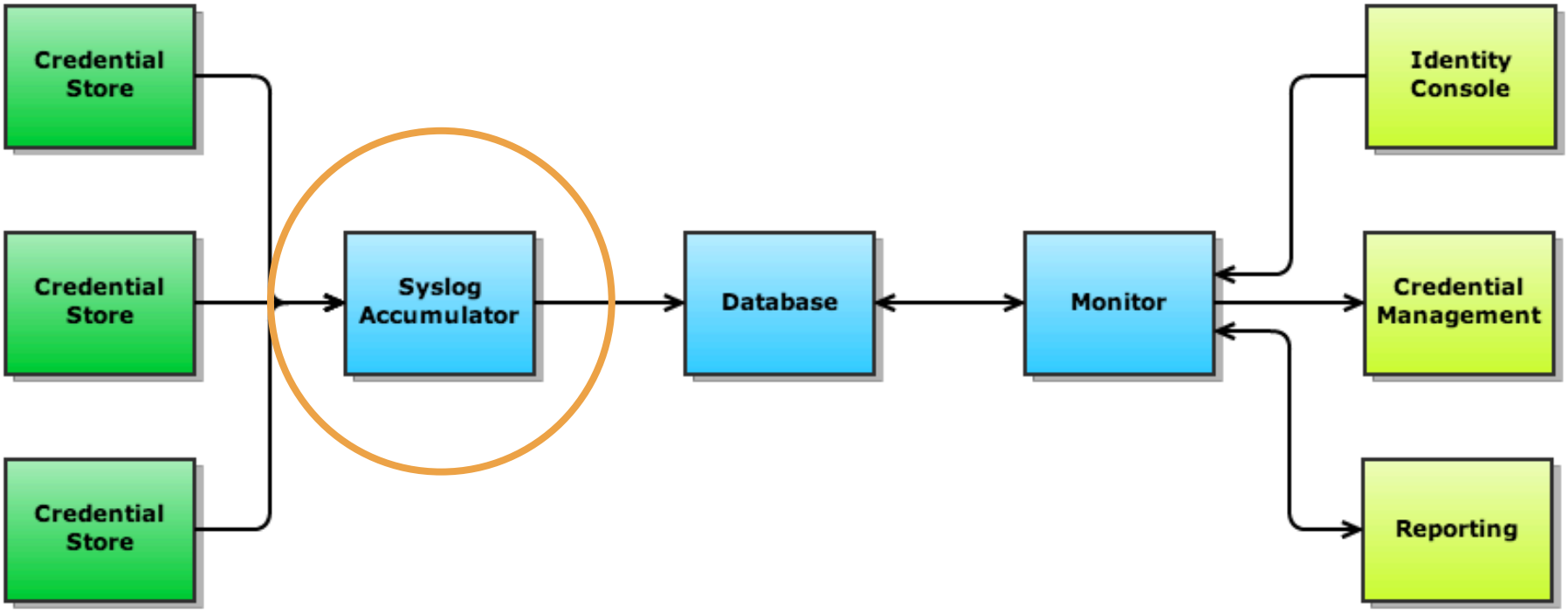
Let me count the ways.

5000


Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting

AuthN Failure Counter


Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting


Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting

Accumulator | Technology

rsyslog — open source, Highly available, etc

Splunk — fancy whiz-bang features

Accumulator | Active Directory

EventCode = "4771"
OR
EventCode = "4776"

Accumulator | Active Directory

EventCode = "4771"
OR
(EventCode = "4776"
AND
Failure)

Accumulator | Active Directory

```
(EventCode = "4771" AND
Account_Name !=*$ AND
Account_Name != - )
OR
(EventCode = "4776" AND
Failure AND
Logon_Account != *$)
```

Accumulator | Active Directory

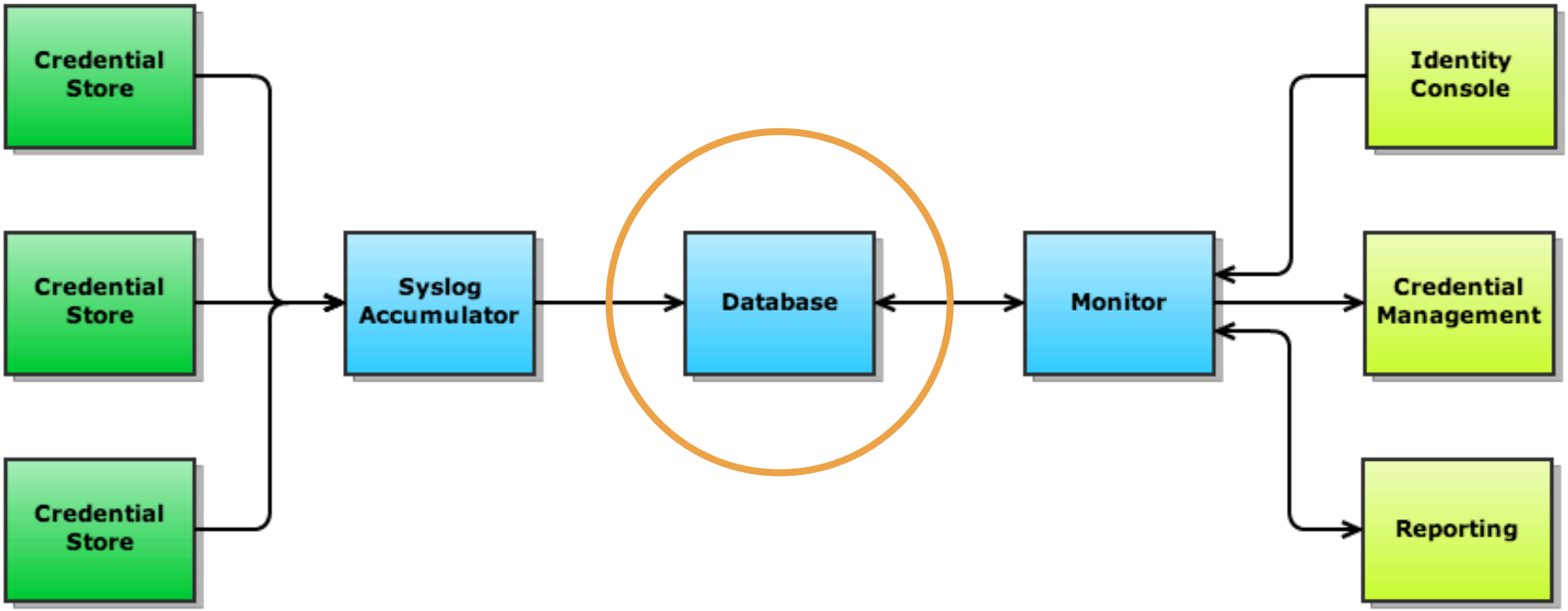
```
sourcetype="WinEventLog:Security" (EventCode="4771" AND Account_Name !=*$ AND Account_Name != - ) OR (EventCode="4776" AND Failure AND Logon_Account != *$) | eval uid=coalesce(Logon_Account,Account_Name) | eval client = coalesce(Client_Address,Source_Workstation)
```

Accumulator | LDAP/OpenLDAP

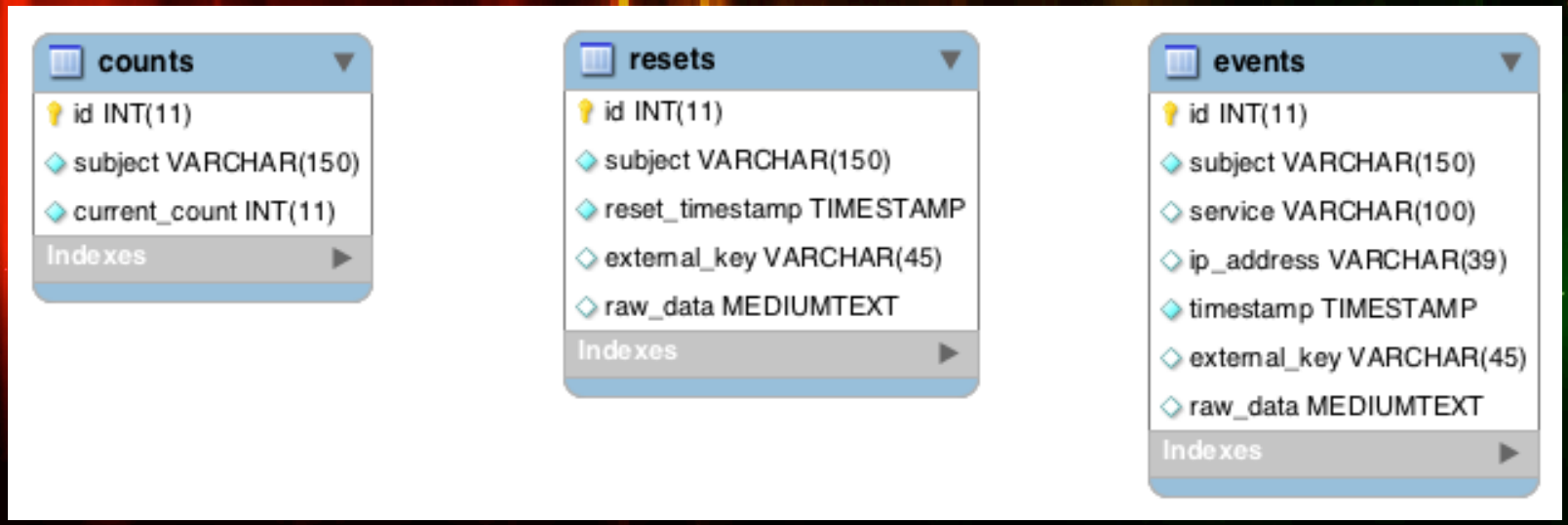
err = 49

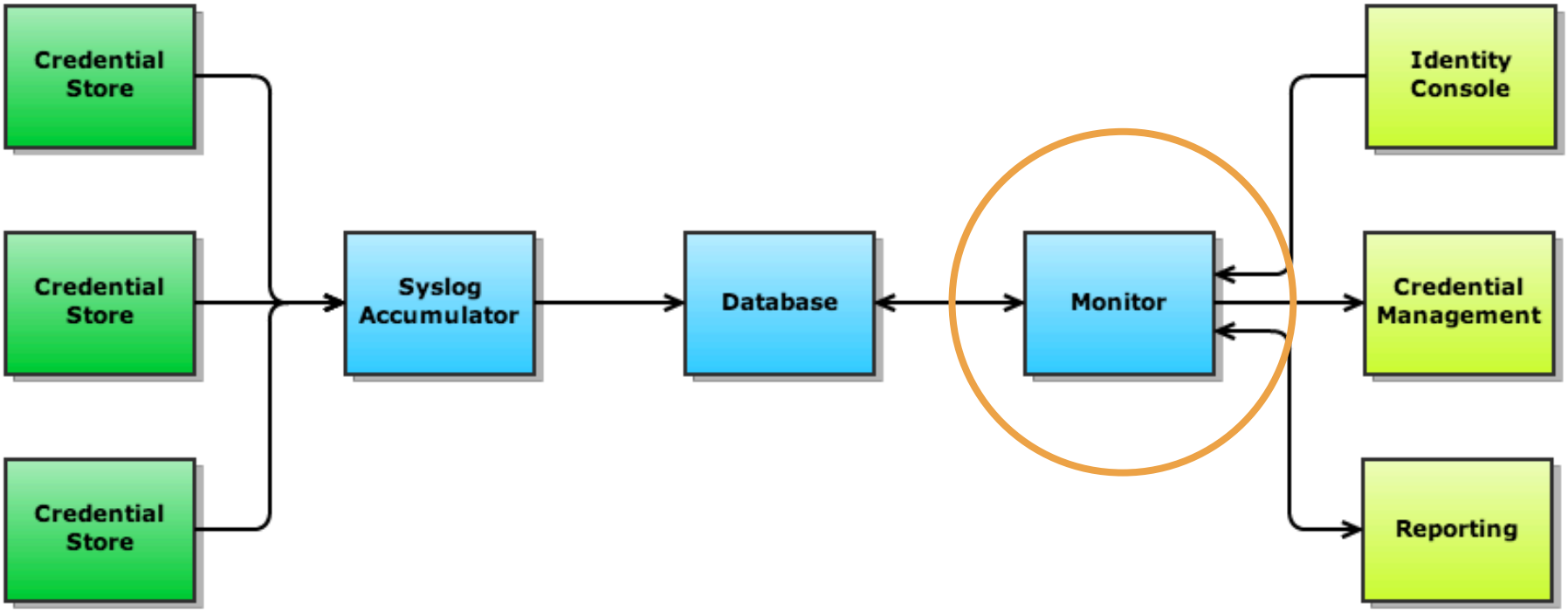
Accumulator | LDAP/OpenLDAP

```
source="unl-is-idm" |
transaction conn
maxpause=30s | where err=49
```


Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting

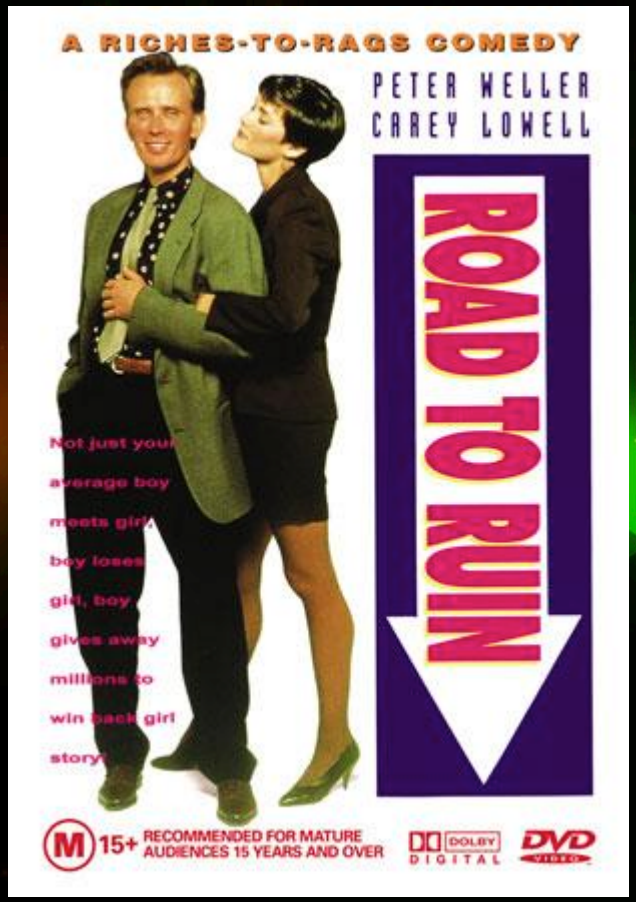
Database | ER Diagram




Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting

memberOf | Riches to Rags

Silver IAQ
Bronze IAQ
No IAQ

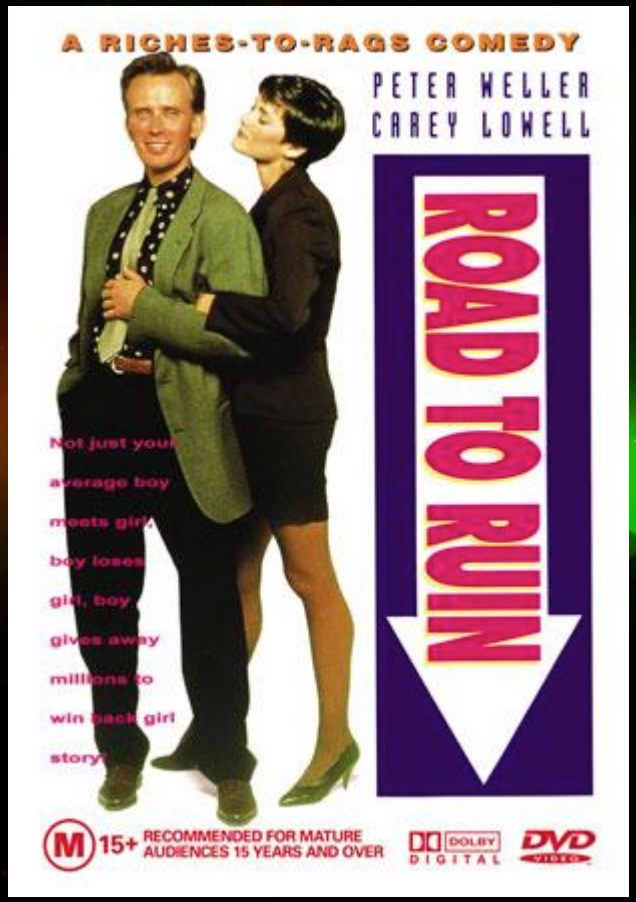


memberOf | Riches to Rags

~~Silver IAQ~~

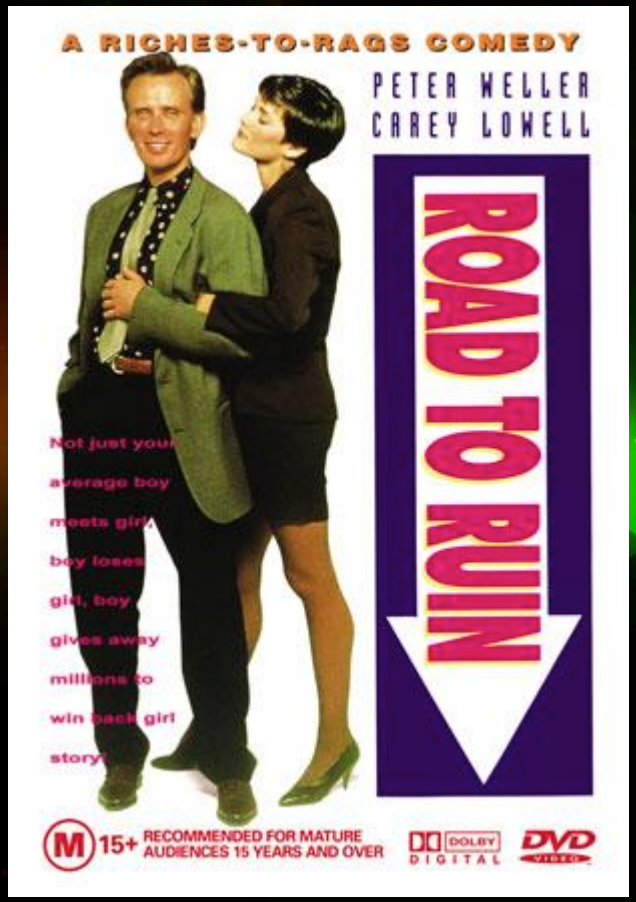
Bronze IAQ

No IAQ

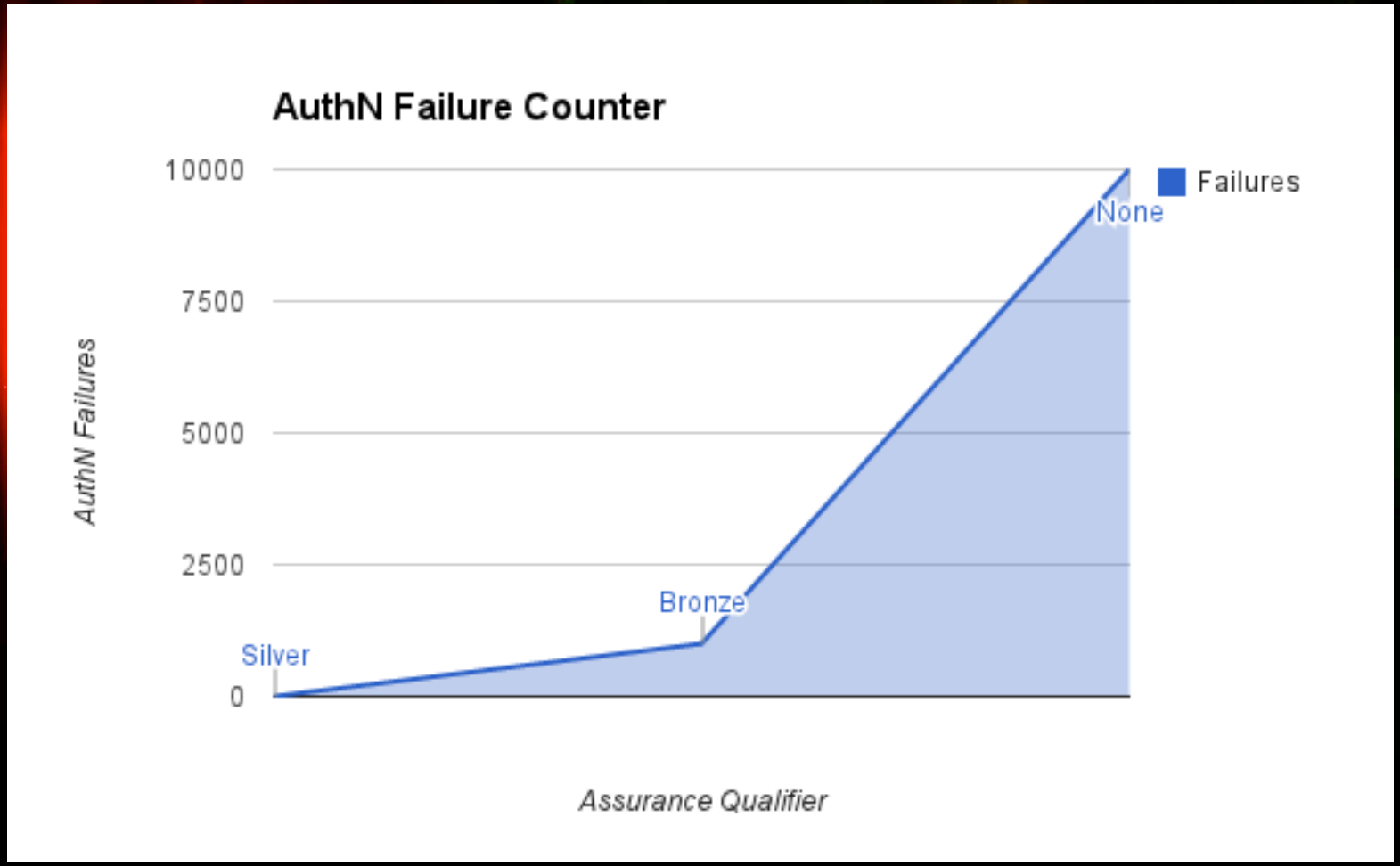


memberOf | Riches to Rags

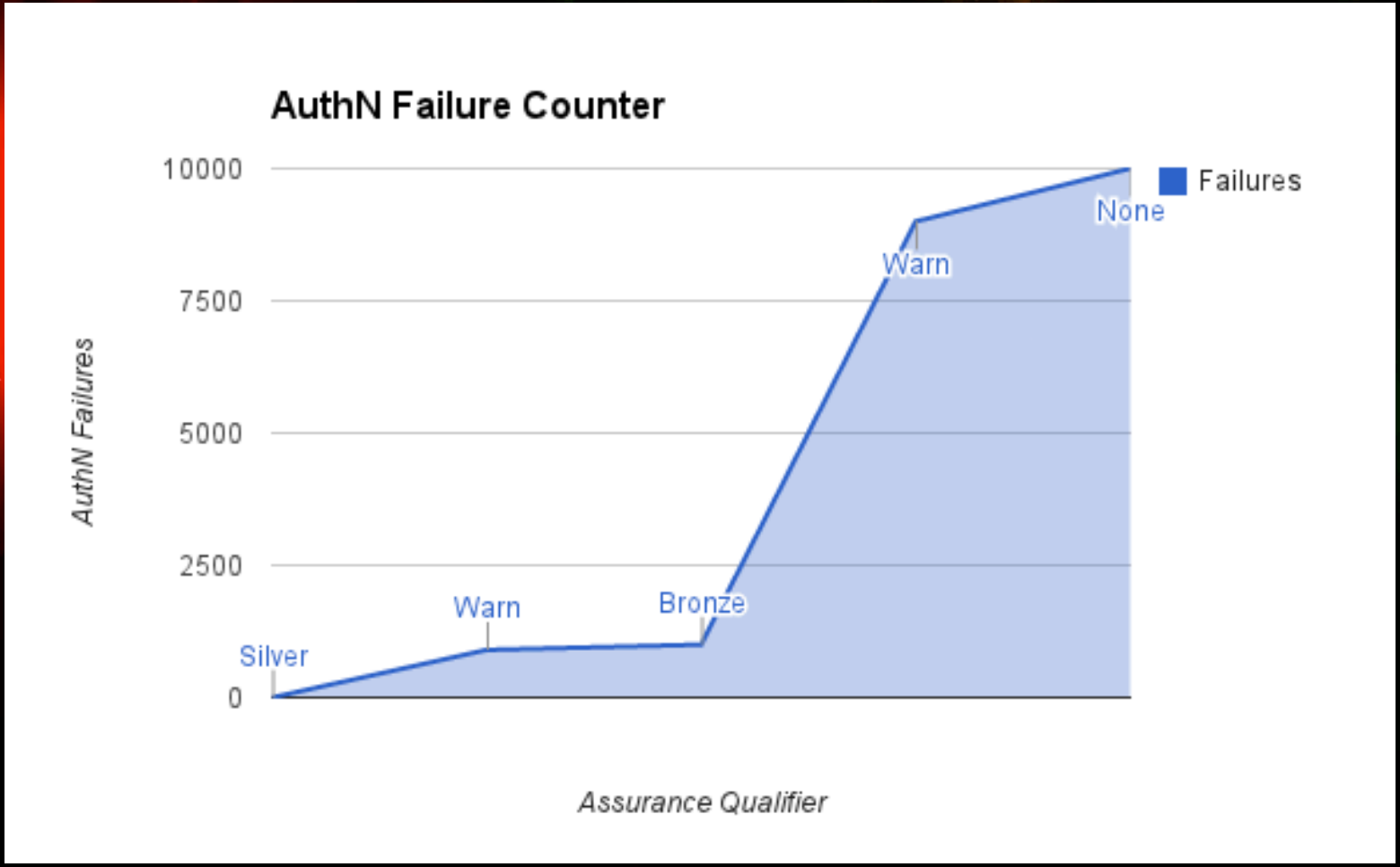
- ~~Silver IAQ~~
- ~~Bronze IAQ~~
- No IAQ



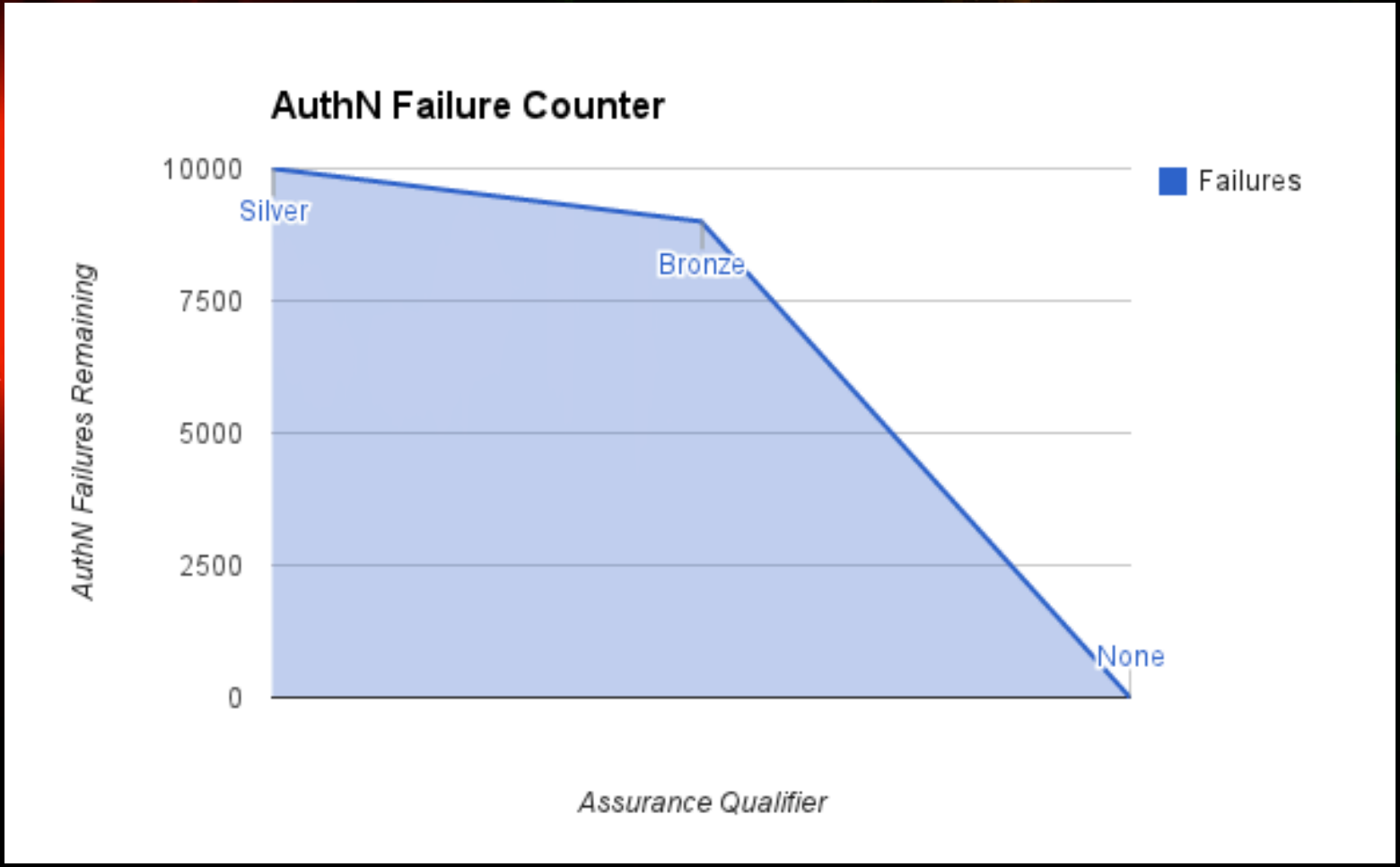
AuthN Addition | Riches to Rags



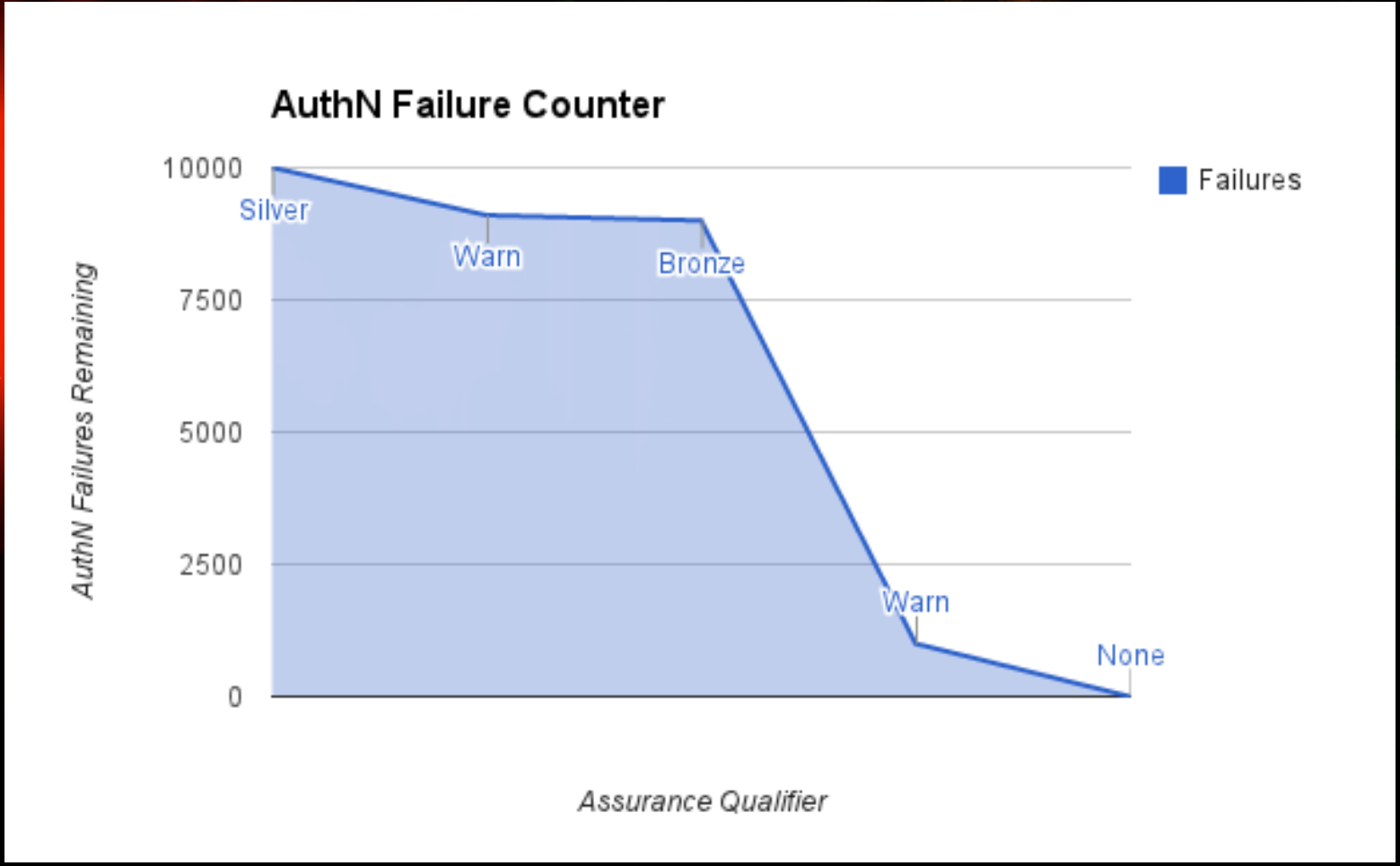
AuthN Addition | Riches to Rags

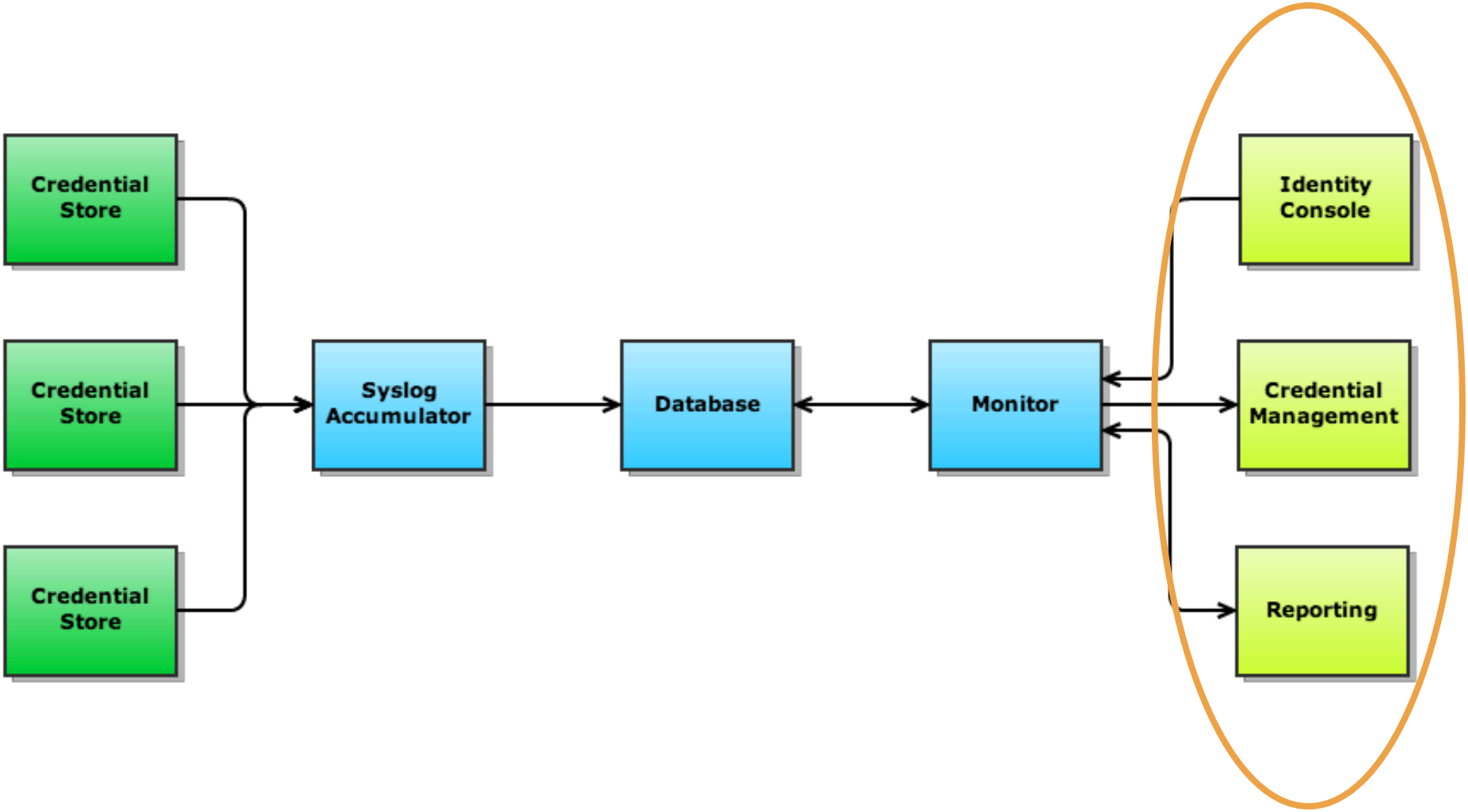


AuthN Subtraction | Riches to Rags



AuthN Subtraction | Riches to Rags




Credential Store
Credential Store
Credential Store
Syslog Accumulator
Database
Monitor
Identity Console
Credential Management
Reporting

Actions | Monitoring Activity

- Failure monitors
- Threshold monitors
- Reset monitors

Actions | Monitoring Activity

- Monitor for attacks (security)
- Monitor for Authentication Success (auditing)
- Deprecated protocols (NTLMv1, unencrypted LDAP)
- Usage stats (service utilization)
- Authentication failures

Your Recent Activity

Date	Event	Location
1:35 PM	Created a new app password	Lincoln, NE, USA
1:35 PM	Deleted an app password	Lincoln, NE, USA
1:35 PM	Signed in from Firefox (Mac)	Lincoln, NE, USA
Mar 13	Signed in (Mac)	Lincoln, NE, USA
Mar 11	Signed in (iPhone)	Omaha, NE, USA
Feb 14	Signed in (Mac)	Lincoln, NE, USA
	Sign-in events unavailable prior to this date. Other activity below.	
Jan 17	Phone number added	Lincoln, NE, USA
Jan 17	Phone number added	Lincoln, NE, USA
Jan 17	Turned ON 2-Step Verification	Unknown
4/16/13	Removed Google Authenticator	Unknown
4/16/13	Phone number deleted	Unknown

Deleted app password

1:35 PM (2 minutes ago)

For 2-Step Verification users, deleting an app password means you can no longer access your account through that app.

Manage

App Password Name

iChat at work

Approximate location (based on IP)

Lincoln, NE, USA

Details

IP Address

129.93.74.107

Findings | Common Usernames

- administrator
- administrateur
- administrator
- db2admin
-
- \x05
- bob

Findings | User Initiated Attacks

- Mobile device not using updated password
- Wrong username
- Typed full name into username box
- Typed email into username box
- Typing password into username box

Questions?

Brett Bieber | University of Nebraska-Lincoln
bieber@unl.edu

Photos

http://www.fatcap.com/article/tallying-soldiers.html
http://s4.photobucket.com/user/Polluxa/media/Macros/simpsons-mob.jpg.html
http://commons.wikimedia.org/wiki/File:%C3%9Altima_Cena_-_Juan_de_Juanes.jpg
http://aladdiescave.com.au/index.php?act=viewProd&productId=539
http://tvloon.ca/2013/06/11/inspector-gadget-reboot-tops-off-teletoon-canadas-latest-original-production-slate/
https://drive.google.com/previewtemplate?id=172RimYd4AObPZw3HyfqO9rkmtWaNlzj3ez7GiIPlogo&mode=public

Failed Authentication Counter @ UC Berkeley

Benn Oshrin, CalNet, UC Berkeley

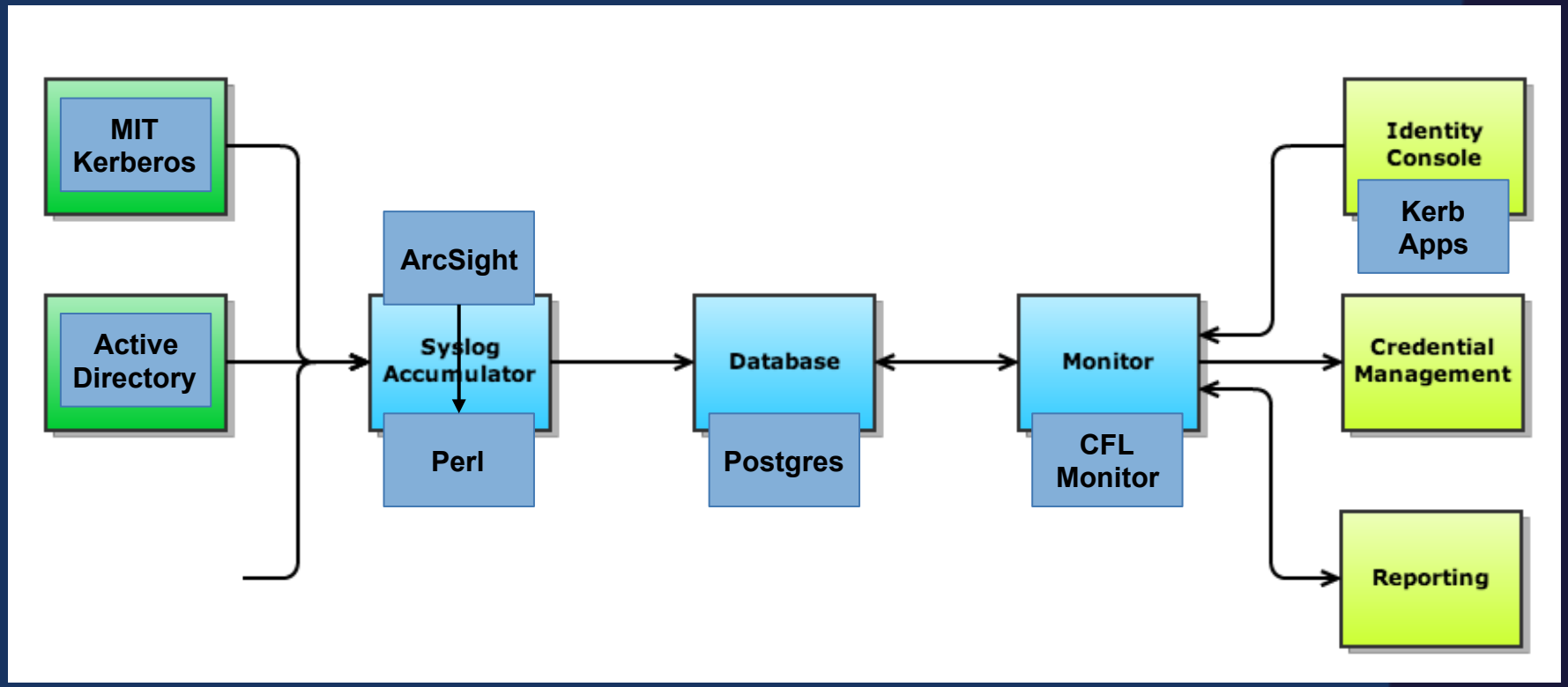
Berkeley
UNIVERSITY OF CALIFORNIA

Counting Failed Logins @ UC Berkeley

Benn Oshrin, CalNet, UC Berkeley

Berkeley
UNIVERSITY OF CALIFORNIA

Counting Failed Logins | Architecture



Credential Stores

- Active Directory
- MIT Kerberos
- Lockouts implemented in AD but not MIT
  - Could implement a “split policy” by having MIT also implement lockout, but this would require periodic password changes which are not currently required
- Logs transferred to security group
  - MIT Kerberos via syslog, AD via agent

Syslog Accumulator

- Security group filters records for authentication failures
  - Using ArcSight CEF
- Filtered records transferred to CalNet via syslog
- Records loaded into database via simple Perl script
  - Switch to rsyslog at some point?

Database Schema

Column	Description
id	Row identifier
ip_address	Source IP address of failed authentication (could be desktop, CAS, etc)
recorded	Timestamp of failed authentication
service	Service handle, usually kerberos name
subject	NetID

Initial Stats From Sample Data

- ~500k records over 17 day period
- Top count = 44298 (~2600/day), then 10075 (593)
- ~20 in the 1000 – 10000 range (59 – 589/day)
- ~151 in the 170 – 1000 range (10 – 59/day)

CFL-Monitor

- OpenSource Grails App
- Flexible model for actions
- Database driven configuration for thresholds
- Monitor periodically (default every 2 minutes) checks for subjects exceeding thresholds (less resets)
- Currently alpha (or maybe pre-alpha)
- https://github.com/ucidentity/cfl-monitor

CFL-Monitor Actions

- Email arbitrary address (implemented)
- Email subject
- Add subject to/remove subject from group
- Send message to endpoint (API oriented)
- Expire credential (Kerberos, etc)
- Update LDAP
- Execute arbitrary SQL
- Open ticket (ServiceNow, etc)

CFL-Monitor Policy

- IAP thresholds are around 100k for Silver, 1M for Bronze
- Initial policy to just email security group, not user; no automatic actions taken
- Start around 1000 failures (absolute, not over *n* days) and adjust from there
  - Based on sample data, this is 1–2 people per day

Todo

- Settle on policy
- More testing of CFL-Monitor, revisions
- Update password change tools to log reset event
- Service Desk tools
- Reporting
- More Actions? Self Service?

Resources

Framework and Profiles

- Identity Assurance Assessment Framework
  www.incommon.org/docs/assurance/IAAF.pdf
- Identity Assurance Profiles
  www.incommon.org/docs/assurance/IAP.pdf

Resources

- Monthly Call: First Wed of the month Noon ET
- Website, discussion list and Implementers wiki:
  assurance.incommon.org
- Password Entropy Calculators on the InCommon Assurance wiki:
  http://bit.ly/1cEI7uA