Rollenbasierte Authentisierung und Autorisierung mit LDAP und sudo in heterogenen Unix-Umgebungen

Jürgen Sprenger, 16.09.2015

swisscom

Agenda

- Über das Projekt
- Anforderungen
- Architektur
- Integration in automatisierte Benutzerverwaltung
- Erreichte Ziele
- Stolpersteine
- Ausblick auf die weitere Entwicklung
- Fragen

Über das Projekt

- Start in 2008
- Produktiv seit Oktober 2009
- >2200 Benutzer
- >4500 Server
- >1200 Rollen
- ~1000 Benutzergruppen
- ~850 Servergruppen
- >11000 sudo Kommandos

swisscom

Anforderungen

- Mandantenfähigkeit
- Unterstützt AIX, HPUX, Linux und Solaris Clients.
- Protokollierung und Archivierung aller Änderungen.
- Nachvollziehbarkeit: Wer hatte wann welche Rolle?
- Keine direkten Zugriffe auf privilegierte Benutzerkonten.
- Jede Ausübung privilegierter Zugriffe wird protokolliert.
- Keine manuellen Eingriffe.
- Vollständige Automation und Integration in Benutzerverwaltung.

Architektur

- Keep it simple!
- OpenLDAP and sudo
- Master-Slave Architektur
  - Zwei LDAP Master Server, Georedundanz
  - Vier LDAP Slave Server pro Netzerkzone, Georedundanz.
  - Multi-Master-Replikation
- Simple authentication
- Single Password
- Kein Kerberos!

Integration in automatische Benutzerverwaltung

- Vollständig in HR-Prozesse integriert.
- Vollautomatischer Prozess von HR feed bis ins LDAP-Verzeichnis.
- Perlskript als Schnittstelle zwischen Control-SA und LDAP-Master.

Erreichte Ziele

- Alle Anforderungen erfüllt.
- Geplante Downtime seit Produktionsstart: 0s
- Ungeplante Downtime seit Produktionsstart: 0s
- Keine Serviceunterbruch für Wartungsarbeiten erforderlich.
- Verfügbarkeit 100% seit Oktober 2009
- 3*30% FTE für Betrieb, Engineering, 3rd Level Support

Stolpersteine

- Unterschiede der unterstützten Betriebssysteme.
- Simple Authentication erforderlich.
- Verhalten der LDAP-Clients einiger Hersteller
- Fehlkonfiguration des Name-Service-Cache bei LDAP-Clients
- Sonderzeichen in Passworten.
- Sonderzeichen in Benutzernamen.
- Bugs in LDAP-Clients einiger Hersteller.

Ausblick auf die weitere Entwicklung

- ssh public keys im LDAP-Verzeichnis
- sudo session logging
- Integration von Applikationen
- Integration Authentisierung auf Serviceprozessoren, ALOM, ILOM.
- Hardware lifecycle

Fragen?

Kontakt

Swisscom (Schweiz) AG
Midrange Operation
Jürgen Sprenger
Ey 10
CH-3036 Ittigen

Phone +41-79-699 90 70
Mail juergen.sprenger@swisscom.com