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

Schwerpunkt : Infrastruktur, Security

Vortragstyp : Projekt- und Erfahrungsbericht

Ziellevel : ALLE

Schlüsselworte: Authentisierung, Autorisierung, Privilegierte Zugriffe, LDAP, sudo.

1 Über das Projekt

Das Projekt wurde im Jahr 2008 gestartet mit dem Ziel die Administration privilegierter Zugriffe zu automatisieren, die Nachvollziehbarkeit der Rechtevergabe und Ausübung zu gewährleisten und die im nächsten Kapitel aufgeführten Anforderungen umzusetzen.

Das Projekt wurde in 2008 gestartet und im Oktober 2009 mit der Übernahme in den produktiven Einsatz erfolgreich abgeschlossen.

Inzwischen sind privilegierte Zugriffe für über 2200 Benutzer auf mehr als 4500 Servern mit 1200 Rollen abgebildet.

2 Anforderungen

Im Projekt war eine Fülle von Anforderungen umzusetzen, von denen die wichtigsten hier aufgeführt sind.

2.1 Hochverfügbar und ausfallsicher, Point in Time Recovery

Der Service muss zwei gleichzeitig auftretende Ereignisse überstehen und weiter verfügbar sein, zum Beispiel Ausfall eines Rechenzentrums während Wartungsarbeiten an einer Maschine des Service im anderen Rechenzentrum.

Die verbleibende Maschine muss die Last alleine bewältigen können.

Nach einem Ausfall muss der Zustand zum Zeitpunkt des Ausfalls wiederhergestellt werden können.

2.2 Unabhängig von anderen Diensten

Der Service darf nur von Stromversorgung, Netzwerkanbindung und Kühlung der Hardware abhängig sein. Deshalb kommt zum Beispiel nur die Verwendung lokaler Speichermedien in Frage und keine SAN-Anbindung.

2.3 Mandantenfähigkeit

Die Benutzerkonten der Kunden sind voneinander getrennt zu halten. Kein Kunde darf Kenntnisse über Benutzerkonten eines anderen Kunden erlangen können, auch nicht darüber, ob ein bestimmtes Benutzerkonto existiert.

2.4 Unterstützt AIX, HPUX, Linux und Solaris Clients

Die vier Plattformen AIX, HPUX, Linux und Solaris müssen über den vom Betriebssystemhersteller mitgelieferten LDAP-Client angebunden werden können. Es darf keine zusätzliche Software erforderlich sein.

2.5 Protokollierung und Archivierung aller Änderungen

Alle Änderungen am Verzeichnisdienst müssen nachvollziehbar protokolliert werden mit:

- Art der Änderung

- Zeitstempel

- Benutzer

- IP-Adresse

2.6 Nachvollziehbarkeit: Wer hatte wann welche Rolle?

Für jeden Zeitpunkt auch in der Vergangenheit muss ersichtlich sein, wer wann für welche Rolle berechtigt war, welche Rechte die Rolle umfasst und auf welchen Systemen diese Rechte ausgeübt werden dürfen.

2.7 Kein direkter Zugriff aus privilegierte Benutzerkonten

Der direkte Zugriff auf privilegiert Benutzerkonten wie etwa root ist zu unterbinden. Ein Zugriff darf nur noch über persönliche Benutzerkonten und die sudo-Rollen im LDAP-Verzeichnisdienst erfolgen.

2.8 Keine manuellen Eingriffe

Ausser zur Fehlerbehebung nach Ausfällen oder Fehlbedienungen dürfen keine manuellen Änderungen am Inhalt des Verzeichnisdienstes vorgenommen werden.

2.9 Vollständige Automation und Integration in Benutzerverwaltung

Um manuelle Eingriffe eliminieren zu können muss die Lösung vollständig in die bestehende Umgebung zur Benutzerverwaltung integriert werden.

3. Architektur

Die Architektur wurde nach dem KISS-Prinzip (Keep it simple and safe) entwickelt.

Da jeder Betriebssystemhersteller seinen eigenen Directory-Server präferierte musste eine Entscheidung für den grössten gemeinsamen Nenner gefunden werden. Sie fiel zugunsten von OpenLDAP als Verzeichnisdienst und sudo für die privilegierten Zugriffe aus. Die eingesetzten Maschinen verwenden ausschliesslich lokale Speichermedien um die Verfügbarkeit auch bei einem grossflächigen SAN-Ausfall zu gewährleisten.

Um Umschaltzeiten bei Ausfällen eines Systems zu vermeiden und die Komplexität der Lösung gering zu halten wurde eine Master-Slave-Architektur gewählt. Der Client wählt hier bei Ausfall eines Servers einfach den nächsten aus der Liste der zur Verfügung stehenden Server aus.

In den beiden georedundant aufgebauten Rechenzentren wird jeweils ein LDAP-Master eingesetzt, die ihre Inhalte über Multi-Master-Replikation synchronisieren.

Für jede Netzwerkzone werden je zwei LDAP-Slaves in jedem der beiden georedundanten Rechenzentren installiert.

Damit ist gewährleistet, dass mindestens zwei unabhängige Ereignisse eintreten können, ohne dass der Service ausfällt.

Für die Authentisierung wurde 'simple authentication' gewählt. Weil die Unterstützung für Hashalgorithmen bei den Benutzerpassworten durch die Betriebssystemhersteller höchst unterschiedlich ist und um Fehlern durch Fehlkonfigurationen vorzubeugen blieb keine andere Wahl.

Jeder Benutzer hat nur ein Passwort, auch wenn er für mehrere Kunden arbeitet. Dies wird durch den Einsatz von Aliasen erreicht, die es gestatten, die Benutzerkonten der Swisscom-Administratoren bei den Kundenverzeichnissen einzublenden.

Auf den Einsatz von Kerberos wurde bewusst verzichtet. Gerade bei privilegierten Zugriffen hätte die Lebensdauer eines Kerberos-Tickets aus Sicherheitsgründen so weit verringert werden müssen, dass die Vorteile des Single-Sign-On ohnehin verschwunden wären.

Die eingesetzten LDAP-Server verwenden für die Authentisierung und Autorisierung der Benutzer selbst kein LDAP um zyklische Abhängigkeiten zu vermeiden und den Administratoren die Arbeit bei einem Ausfall nicht zu blockieren.

4. Integration in bestehende Benutzerverwaltung

Diese Lösung wurde vollständig in die bestehende Benutzerverwaltung und die etablierten Bestellprozesse integriert.

Von der Bestellung eines Zugriffsrechtes ist abgesehen von der Genehmigung durch den Rollenowner per Mausklick keine Interaktion bis zur Provisionierung in den Verzeichnisdienst erforderlich.

Dies gilt ebenso für den HR-Feed falls ein Mitarbeiter neu eingestellt wird oder die Firma verlässt.

Als Schnittstelle zwischen dem intern eingesetzten Control-SA und dem LDAP-Verzeichnis dient ein einfaches Perlskript, dessen Hauptaufgabe die Überprüfung der Eingabeparameter ist.

5. Erreichte Ziele

Alle Anforderungen aus Kapitel wurden erfüllt. Seit Produktionsstart gab es keine geplante und keine ungeplante Downtime.

Für Wartungsarbeiten ist kein Serviceunterbruch erforderlich.

Die Verfügbarkeit seit Oktober 2009 beträgt 100%

Für Betrieb, Engineering und 3rd Level Support werden drei Mitarbeiter zu je 30% eingesetzt.

6. Stolpersteine

Die Unterschiede der eingesetzten Betriebssysteme machten einige Anpassungen erforderlich.

So mussten einige herstellerspezifische LDAP-Schemata erfolgreich intergiert werden und das bestehende LDAP-Schema so erweitert werden, dass für jedes Betriebssystem ein eigener Ort für die Benutzerverzeichnisse angegeben werden kann und jeder Benutzer pro Betriebssystem eine eigene Shell haben kann.

Durch die unterschiedliche Unterstützung von Hashalgorithmen für die Passworte blieb als kleinster gemeinsamer Nenner nur die Möglichkeit simple-authentication zu verwenden.

Bei einem Hersteller verhält sich der LDAP-Client bei einem bestimmten Releasestand nicht korrekt, was zu einer drastischen Erhöhung der Last auf den LDAP-Slaves durch diese Clients geführt hat.

Suboptimal konfigurierte Name-Service-Caches führten zu unnötig vielen Anfragen an den LDAP-Service und einer damit einhergehenden stärkeren Auslastung.

Bestimmte Sonderzeichen in Passwörtern bereiten Probleme. Entsprechend wurde das Schnittstellenskript angepasst.

Eine bleibende Herausforderung bleibt die Analyse neu aufzunehmender sudo-Rollen auf unerwünschte Nebeneffekte, von denen die aus einem Editor zu öffnende root-Shell wohl der bekannteste ist.

7. Ausblick auf die weitere Entwicklung

Eine Erhöhung des Komforts für die stellt Benutzer die Integration der ssh public keys in das LDAP-Verzeichnis dar, die ausserdem die Kosten für die Verwaltung dieser Schlüssel drastisch vermindern wird.

Es gibt die Option für Session-Logging bei der Verwendung von sudo. Möglicherweise ein Thema für Systeme mit erhöhten Sicherheitsanforderungen.

Die Integration von Applikationen ist in Arbeit, die Einführung der LDAP-Authentisierung auf Serviceprozessoren, ALOM, ILOM für die Zukunft geplant.

Im nächsten Jahr wird voraussichtlich ein Hardware LifeCycle durchgeführt werden um die dann sieben Jahre alten Komponenten zu erneuern.

8. Fragen

9. Kontakt

Referent:

Jürgen Sprenger

Swisscom AG

Postfach

3050 Bern

Schweiz