Kerberos und das Oracle – die Nutzung von Kerberos in einer Oracle-Solaris-Umgebung

Veit Jäger
ORDIX AG
Paderborn

Schlüsselworte
Sicherheit, Kerberos, Single-Sign-On, Solaris, SSH, NFS

Einleitung
Das Thema Sicherheit in Unternehmen wird immer wichtiger und soll im Idealfall für den Mitarbeiter transparent via Single-Sign-On (SSO) erfolgen. Durch die Nutzung von Kerberos kann sowohl die Produktivität als auch die Sicherheit in Unternehmen gesteigert werden.

Dieser Vortrag ist ein Erfahrungsbericht über die Verwendung von Kerberos als SSO-Lösung in einer homogenen Solaris-Umgebung. Der Vortrag kann in drei Abschnitte unterteilt werden, wobei der erste Abschnitt grundlegende Sicherheitsaspekte des Betriebssystems und eine anschauliche Einführung in Kerberos beinhaltet. Im folgenden Abschnitt wird detailliert auf die Installation der notwendigen Komponenten und die Konfiguration des Systems eingegangen. Ebenso wird die Kombination von Kerberos mit den verschiedenen Systemdiensten und Applikationen, wie zum Beispiel einer Oracle-Datenbank, dargestellt. Eine Demonstration über den Einsatz von Kerberos im Alltag anhand von typischen Systemdiensten wie zum Beispiel SSH oder NFS runden diesen Vortrag ab.

Sicherheit wird immer wichtiger
Die Nachrichten bringen täglich neue Meldungen über An- und Übergriffe auf Computersysteme. Dadurch wird immer offensichtlicher, dass Unternehmen ihre Sicherheit betrachten und überprüfen müssen. Neben den Zugängen zu den Systemen muss auch die Kommunikation zwischen den Systemen überwacht und abgesichert werden.

Dass die klassischen Dienste wie zum Beispiel „telnet“ unsicher sind und zahlreiche Angriffspunkte darstellen ist inzwischen bekannt. Die Nachfolger zeichnen sich oftmals durch die Eingabe von Kennwörtern aus. Die Probleme dabei sind aber die Anzahl der Kennwörter und das häufig notwendige Wechseln der Kennwörter. Bei der notwendige Länge von Kennwörtern, welche u.a. bedingt wird durch s.g. „Brutforce-Attacken“, werden immer öfter Standardschlüssel verwendet und somit selbst sichere Systeme unterwandert.

Durch die Verwendung von Single-Sign-On kann sowohl der Aufwand für die Anwender als auch die Sicherheit der Systeme erhöht werden. Eine Möglichkeit der sicheren system- und applikationsübergreifenden Authentifizierung bietet Kerberos.

Kerberos, so geht`s
Kerberos ist ein ticketbasiertes Authentifizierungsverfahren. Dies bedeutet, dass sich jeder Beteiligte mit einer Art Ausweis/Ticket authentifizieren muss. Die verschiedenen Tickets sind jeweils mit Hilfe von Schlüsseln geschützt und können nur von den jeweiligen Empfängern verwendet werden.

Um die Funktionsweise von Kerberos erklären zu können, müssen zunächst einige Begriffe eingeführt werden:

a. Das Key Distribution Center (KDC) ist der Überbegriff für den Kerberos Server. Es besteht aus dem AS und dem TGS.
b. Der Authentication Service (AS) ist für die erste Authentifizierung zuständig.
c. Der Ticket Granting Service (TGS) stellt die weiteren Tickets aus.
d. Ein Ticket besteht aus verschlüsselten Session Keys, welche für die Authentifizierung benötigt werden.
e. Das Ticket Granting Ticket (TGT) nimmt eine besondere Position ein. Es wird vom AS ausgestellt und erlaubt dem Client, sich ein Ticket für einen bestimmten Dienst vom TGS zu holen.
f. Kerberos-Objekte sind sowohl die Dienste und Systeme als auch die Anwender (Clients), welche in einem Kerberos Realm bekannt sind.
g. Unter einem Realm versteht man eine Domäne, innerhalb derer sich alle Beteiligten befinden müssen.
h. Principals sind eindeutige Namen für alle Objekte, die in einer Kerberos-Umgebung vorkommen.

Solaris und Kerberos
Solaris biete bereits einige Sicherheitsmechanismen und kann ohne große Probleme mit Kerberos verwendet werden. Kerberos ist in Solaris als Service integriert.

Nach erfolgreicher Konfiguration über die Dateien `/etc/krb5/kdc.conf` und `/etc/krb5/krb5.conf` kann der Service mit `svcadm` gestartet werden. In den Konfigurationsdateien können neben der Verschlüsselungsmethode unter anderem auch die zentralen Server und das sogenannte Realm festgelegt werden.

Ein Kerberos Realm ist die Umgebung, in welcher ein bestimmter Kerberos Server zuständig ist. Man kann mehrere Realms parallel betreiben und untereinander verbinden, zum Beispiel die Solaris Server mit einer Windows-Active-Domain-Umgebung, in welcher sich die Anwender anmelden. Dabei darf jedes System nur einem Realm angehören.

Weiterhin stellt der Service einige Anforderungen an die Serverlandschaft im Unternehmen dar. Damit der Dienst sicher funktioniert wird erwartet, dass die dynamische Namensauflösung (DNS) in einem Unternehmen vollständig implementiert ist. Neben der Namensauflösung sind die verwendeten Tickets nur eine begrenzte Zeit gültig, daher ist auch das Network Time Protokoll (NTP) eine grundlegende Anforderung.

Die Pakete welche sich mit Kerberos und Solaris beschäftigen sind folgende:

system	SUNWkdcr	Kerberos V5 KDC (root)
system	SUNWkdcu	Kerberos V5 Master KDC (user)
system	SUNWkrbr	Kerberos version 5 support (Root)
system	SUNWkrbu	Kerberos version 5 support (Usr)

Auf den Clients ist nur die Installation der Anwenderpakete notwendig.

Was für Möglichkeiten bringt der Dienst?
Die Vorteile einer zentralen Authentifizierung für ein Unternehmen liegen in dem, für den Anwender, einfacheren Zugriff auf Applikationen und natürlich der Verwendung von besseren Kennwörtern. Durch den Umstand, dass nur ein Kennwort vergeben werden muss, kann dieses länger und komplizierter ausfallen ohne, dass die Anwender mit Notizen arbeiten müssen. Durch die Verwendung eines zentralen Schlüssels steigt auch die Produktivität, da die Anwender sich nicht mehr mit dem Eingeben und Administrieren von Kennwörtern aufhalten müssen.

Auf der Seite der Administratoren steigt der Aufwand nur unwesentlich - im Gegenteil, die verschiedenen Zugriffe müssen nicht mehr mit verschiedenen Werkzeugen gepflegt werden. Der Kerberos-Dienst bietet eine zentrale Zugriffskontrolle.

Kerberos und Oracle-Datenbanken
Die Kerberos-Anbindung von Oracle-Datenbanken setzt voraus, dass auf dieser die Option „Oracle Advanced Security“ installiert und aktiviert ist. Erst diese stellt Module für die „starke Authentifikation“ zur Verfügung, welche wiederum mit Kerberos gleichzusetzen ist. Die Option ist für alle Oracle Database Enterprise Editionen verfügbar, muss aber gesondert lizensiert werden.

Die Konfiguration für „Oracle Advanced Security“ liegt in der Datei `sqlnet.ora` vor. Bei gesetzten Oracle-Umgebungsvariablen ist diese im Verzeichnis `$ORACLE_HOME/network/admin` zu finden. In der Konfigurationsdatei werden die Kerberos typischen Informationen hinterlegt, wie zum Beispiel die Verschlüsselung und der Pfad zu den Konfigurationen. Damit sich ein Anwender anmelden kann, muss die Datenbank lernen mit den Kerberos Principal Names umzugehen, also diese beispielsweise einem Datenbankbenutzer zuzuordnen.

Im einfachsten Beispiel wird zu dem Zweck mittels SQL*Plus ein neuer, extern authentifizierter Datenbankbenutzer angelegt:

```
SQL > CREATE USER user IDENTIFIED EXTERNALLY AS 'user@ORDIX .DE ';
SQL > GRANT CREATE SESSION to user;
```

SQL*Plus muss danach beim Start lediglich mitgeteilt werden, dass es eine SQLNet-Authentifizierung durchführen soll. Dies geschieht indem der Aufruf von SQL*Plus wie folgt durchgeführt wird:

```
# sqlplus /@instanz
```

Anstatt _`instanz`_ ist hier der TNS-Name der Instanz einzutragen.

Kerberos und SSH
Um auf ein Unix-System zuzugreifen, wird in der Regel die Secure Shell (SSH) verwendet. SSH bringt bereits eine eigene Methode für die Vereinfachung der Anmeldung mit, allerdings bedeutet diese Methode neben einer bestehenden Kerberos-Umgebung einen extra Aufwand für die Verwaltung.

Die Konfiguration des Dienstes erfolgt in der Datei `/etc/ssh/sshd_config`, bzw. in deren Gegenstück für den Client. Für eine funktionierende Implementierung muss die Kerberos-Konfiguration sowohl auf dem Client als auch auf dem Server hinterlegt sein. Nach der Verteilung der notwendigen Tickets für die Systeme kann der Anwender sich mit seinem persönlichen Ticket anmelden und den Dienst nutzen. Eventuelle Fehlermeldungen und Fehlkonfigurationen tauchen in der Service Management Facility auf und können in der Logdatei des Service nachgelesen werden.

Kerberos und NFS
Das Network Filesystem (NFS) ist in der Unix-Welt sehr weit verbreitet und seit einigen Jahren in der Version 4 verfügbar. NFSv4 ist vorbereitet für die Verwendung von Kerberos. In der Konfiguration muss der Dienst aktiviert werden und greift dann automatisch auf die Kerberos-Konfiguration bzw. den Dienst zu.

Kerberos kann bei NFS in verschiedenen Stufen aktiviert werden. In der einfachsten Variante werden nur die beteiligten Objekte authentifiziert, die beiden folgenden Methoden prüfen zusätzlich explizit die Echtheit der Datenpakete bzw. Verschlüsseln. Durch die Verwendung der Authentifizierung, insbesondere bei der dritten Variante, wird die Performance beeinträchtigt.

Die Absicherung von NFS verläuft im Hintergrund, d.h. sobald Kerberos einmal aktiviert wurde und die Anwender und Systeme eingerichtet sind bemerkt der Anwender nichts mehr von der Sicherheit.

Kleine Stolpersteine
Bei der Verwendung von Kerberos sind neben den bekannten Problemen mit DNS und NTP auch Problematiken mit den locales aufgefallen. Alle beteiligten Systeme sollten hier die gleichen Einstellungen haben oder zumindest die locales installiert haben damit es keine Probleme mit zum Beispiel den Dateinamen unter NFS gibt.

Bei heterogenen Umgebungen mit Windows, Linux bzw. AIX fällt auf, dass das Ziehen von Tickets kein Problem ist, allerdings die unterschiedlichen NFS Implementierungen nicht immer gut miteinander arbeiten.

Sobald Kerberos einmal mit den gewünschten Anwendungen eingerichtet und getestet wurde läuft das System aber erfahrungsgemäß reibungslos.

Abschließende Worte zu Kerberos
Durch die zentrale Aufgabe und Position von einer auf Kerberos basierten Umgebung ist es notwendig, den Server besonders abzusichern. Der Dienst sollte als einzige Applikation auf dem System laufen, um möglichst wenig Schnittstellen und somit Angriffspunkte zu bieten. Durch die Wichtigkeit des Systems sollte auch die Personengruppe der Administratoren, welche Zugriff haben, stark eingeschränkt werden.

Sicherheit ist immer mit einem Aufwand und natürlich auch einem Risiko verbunden. Daher ist es wichtig eine gesunde Relation zu finden.

Kontaktadresse:
Veit Jäger
ORDIX AG
Westermauer 12-16
D-33098 Paderborn

Telefon:	+49 (0) 5251 / 1063-0
Fax:	+49 (0) 180 1 67349 0
E-Mail:	info@ordix.de
Internet:	www.ordix.de