Mark Pröhl

Kerberos

Single Sign-on in gemischten Linux/Windows-Umgebungen

dpunkt.verlag

Mark Pröhl
mark@mproehl.net

Lektorat: René Schönfeldt
Copy-Editing: Ursula Zimpfer, Herrenberg
Satz: Mark Pröhl
Herstellung: Nadine Thiele
Umschlaggestaltung: Helmut Kraus, www.exclam.de
Druck und Bindung: M.P. Media-Print Informationstechnologie GmbH, 33100 Paderborn

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

ISBN 978-3-89864-444-0

1. Auflage 2011

Ringstraße 19 B
69115 Heidelberg

5 4 3 2 1 0

Über dieses Buch

Die Verwaltung von Identitäten und deren Berechtigungen, auch Identity and Access Management genannt, ist eine der Grundlagen für die Sicherheit von IT-Umgebungen. Ein wesentlicher Aspekt dabei ist die Überprüfung und Bestätigung von Anwenderidentitäten, also die Authentisierung bzw. Authentifizierung – ein Bereich, in dem sich das Authentisierungsverfahren Kerberos als Standard durchgesetzt hat. Diese Tatsache erkennt man u.a. daran, dass Kerberos heutzutage Bestandteil aller wichtigen Betriebssysteme ist: Unter den verschiedenen Unix- und Linux-Derivaten war Kerberos schon seit jeher vertreten. Aber auch in der Apple-Welt und insbesondere in Microsofts Active Directory spielt Kerberos eine wesentliche Rolle, wenn es um die Authentifizierung von Anwendern geht. Mindestens ebenso wichtig ist die Unterstützung durch Anwendungen und Netzwerkdienste, die für Kerberos großflächig gegeben ist. Hier kann Kerberos durch echtes Single Sign-on (SSO) weiter punkten. Aber auch andere Aspekte der IT-Sicherheit, wie die Integrität und Vertraulichkeit von Nutzdaten, deckt Kerberos ab.

Gerade in heterogenen IT-Umgebungen eignet sich Kerberos aufgrund seines sehr hohen Verbreitungs- und Standardisierungsgrades als Authentisierungskomponente innerhalb einer zentralen Benutzer- und Berechtigungsverwaltung. Aus diesem Grund befasst sich dieses Buch neben dem Hauptschwerpunkt Kerberos auch mit den Möglichkeiten, Kerberos durch zusätzliche Infrastrukturdienste zu erweitern und so Kerberos-integrierte Netzwerks- und Verwaltungsumgebungen zu schaffen.

Welche Ziele hat dieses Buch?

Dieses Buch möchte dem Leser zunächst ein Verständnis für die Funktionsweise des Kerberos-Protokolls vermitteln. Diese theoretischen Inhalte liefern das nötige Hintergrundwissen für die Praxisteile, in denen der Aufbau und die Verwaltung von Kerberos-Infrastrukturen und die Integration von Anwendungen und Netzwerkdiensten (die »Kerberisierung«) behandelt wird. Dabei soll das Motto gelten: »nicht mehr Theorie als

nötig, aber auch nicht weniger«. An geeigneten Stellen wird auf weiterführende Literatur verwiesen.

Die Praxisteile beschreiben konkrete Implementierungen und sollen dem Leser die Möglichkeit geben, schnell eine funktionierende Kerberos-Umgebung aufsetzen und das theoretisch Gelernte praktisch anwenden zu können.

Für wen ist das Buch?

Dieses Buch richtet sich in erster Linie an Administratoren heterogener Netzwerkumgebungen, die sich eingehend mit Single Sign-on und Kerberos beschäftigen wollen. Für Anwendungsprogrammierer werden vor allem jene Buchteile interessant sein, die die Funktionsweise des Kerberos-Protokolls und die Kerberisierung existierender Netzwerkdienste beschreiben.

Welche Voraussetzungen sollte der Leser mitbringen?

Der Leser sollte über allgemeine Grundkenntnisse der Administration von Linux- und Windows-Systemen verfügen, er sollte sich insbesondere nicht vor dem Einsatz der Kommandozeile scheuen und in der Lage sein, mit einem Texteditor Konfigurationsdateien zu erstellen oder anzupassen. Es wird beispielsweise nicht erklärt, wie man unter Linux ein Terminalfenster oder einen Editor startet. Grundkenntnisse in LDAP sind von Vorteil, obwohl die nötigen Voraussetzungen hier geschaffen werden (siehe Anhang A). Leser, die sich bereits mit den Themengebieten Authentisierung, Autorisierung und Zugriffskontrolle beschäftigt haben, wird der Einstieg in die Materie sicherlich leichter fallen, auch wenn diese Grundlagen hier behandelt werden.

Kenntnisse in Virtualisierungslösungen sind ebenfalls von Vorteil, wenn es darum geht, die hier beschriebenen Beispielszenarien in einer eigenen virtuellen Infrastruktur nachzuvollziehen.

Wie ist das Buch aufgebaut?

Teil I befasst sich mit den theoretischen Grundlagen der Authentisierung in Rechnernetzen mit Kerberos. Um diesen theoretischen Stoff nicht zu trocken zu gestalten, bietet Kapitel 3 einen Eindruck von Kerberos aus der Sicht der Anwender. Danach folgt eine eingehende Beschreibung des

Protokollablaufs, wobei fortgeschrittene Themen (Stichworte: Principal-Aliase, KDC-Referrals und Constrained Delegation) in das abschließende Kapitel 6 ausgelagert sind.

In Teil II lernt der Leser anhand verschiedener Beispielumgebungen, wie man Kerberos-Infrastrukturen aufbaut und verwaltet. Verschiedene Kapitel von Teil II benötigen zusätzliche Komponenten wie NTP, DNS, LDAP und eine PKI, deren Einrichtung daher vorab in Kapitel 7 behandelt wird. Danach werden die Konzepte und Konfigurationsmöglichkeiten anhand der Kerberos-Implementierung des Massachusetts Institute of Technology (MIT Kerberos) sehr detailliert erläutert (Kapitel 8–13). In anschließenden Kapiteln geht es dann um die alternative Implementierung Heimdal und die Möglichkeiten, die Active Directory als Kerberos-Infrastruktur zu bieten hat. Teil II wird von Kapitel 16 abgeschlossen, das sich fortgeschrittenen Themen der Kerberos-Praxis widmet.

In Teil III des Buches geht es darum, wie man Kerberos-Infrastrukturen durch die Integration weiterer Netzwerkdienste erweitern kann. Der Verzeichnisdienst LDAP spielt hier eine tragende Rolle, da dieser Dienst Kerberos um die Verwaltung von Benutzer- und Berechtigungsdaten ergänzt. Ein weiterer Aspekt dabei ist die Integration der Anmeldung am Betriebssystem, wobei LDAP als Namensdienst und Kerberos für die Passwortüberprüfung eingesetzt werden. Dieser Teil beschäftigt sich aber auch grundsätzlich mit dem Vorgang der Kerberisierung von Netzwerkdiensten, die der Leser anhand zahlreicher Beispiele lernen kann.

Der Aufbau des Buches erfolgt in der beschriebenen Reihenfolge, es sollte aber auch möglich sein, einzelne Kapitel zu überspringen oder erst später zu lesen, ohne dabei den Gesamtüberblick zu verlieren.

Die Beispielumgebung

Die Praxisteile II und III beschreiben die verschiedenen Aspekte von Kerberos anhand einer konkreten Beispielumgebung mit dem Namen »EXAMPLE.COM«, die auch aus weiteren Subdomänen besteht. Listing 6.5 auf Seite 109 stellt die Gesamtstruktur dar. Der Aufbau dieser Beispielumgebung wird detailliert beschrieben. Dem Leser steht frei, diese Umgebung oder Teile davon in einem eigenen Testnetz aufzubauen oder nur die Beschreibung zu lesen.

Verwendete Benutzernamen

In den Beispielumgebungen tauchen zwei Benutzer immer wieder auf: Max Mustermann (`maxm`) und Erika Musterfrau (`erim`).

Verwendete Passwörter

In vielen Listings wird das Beispielpasswort »DrPig!« verwendet, das sich aus dem Satz »**D**as **r**oot **P**asswort **i**st **g**eheim!« ableitet. Derartige Passwörter sollten in realen Umgebungen natürlich nicht verwendet werden, machen aber das Leben im Testlabor einfacher. An anderen Stellen dieses Buches wird dagegen mit »richtigen« Passwörtern gearbeitet, die mit einem Passwortgenerator erzeugt werden. Das macht zwar einige Listings etwas unleserlich, soll aber die Sicherheitsrelevanz unterstreichen.

Typografische Konventionen

Im Text

Für die Auszeichnung von Programmein- und -ausgaben, Benutzernamen und Ähnlichem werden verschiedene Schriftarten verwendet, hauptsächlich ist das die `Schreibmaschinenschrift`. Hier ein paar Beispiele:

- Die Ausgabe von textbasierten Computerprogrammen wird so dargestellt: `Dies ist der Output eines Programms`.
- Befehle auf der Kommandozeile werden im Text wie folgt dargestellt: `ssh -l maxm lx01.example.com`.
- Manche Befehle enthalten Platzhalter, die je nach Zusammenhang ersetzt werden müssen. Diese werden *`kursiv`* gesetzt. Beispiel: `ssh -l` *`Benutzer Hostname`*. Dabei wären *`Benutzer`* und *`Hostname`* entsprechend zu ersetzen.
- Benutzernamen: `maxm` und `erim`.
- DNS-Hostnamen: `lx01.example.com`.
- Webadressen (HTTP-URLs): `https://www.example.com`.
- Beschriftungen innerhalb von grafischen Programmelementen. Beispiel: *OK* oder *Cancel*.

In den Listings

Listings werden wie folgt dargestellt:

```
user@lx01:~$ echo 'Hallo Welt'
Hallo Welt
user@lx01:~$
```

Benutzereingaben werden hierbei **fett** gesetzt. Es gibt aber auch unsichtbare Eingaben (beispielsweise Passwörter). Diese werden ***fett-kursiv*** dargestellt:

```
maxm@lx01:~$ kinit maxm@EXAMPLE.COM
Password for maxm@EXAMPLE.COM: DrPig!
maxm@lx01:~$
```

Listings mit zu langen Zeilen müssen umgebrochen dargestellt werden. Der Umbruch wird dann mit dem Zeichen »➘« markiert:

```
user@lx01:~$ echo 'Diese Zeile ist zu lang für ein dpunkt-Buch, ➘
daher wird sie automatisch umgebrochen'
Diese Zeile ist zu lang für ein dpunkt-Buch, daher wird sie auto ➘
matisch umgebrochen
user@lx01:~$
```

Sehr lange Listings können verkürzt dargestellt werden. Das wird dann durch die Zeichenfolge *[...]* angedeutet. Beispiel:

```
user@lx01:~$ ls -la
total 24
drwxr-xr-x 2 user user 4096 2011-08-07 08:56 .
drwxr-xr-x 5 root root 4096 2011-08-07 08:55 ..
-rw------- 1 user user   35 2011-08-07 08:56 .bash_history
-rw-r--r-- 1 user user  220 2010-04-18 18:51 .bash_logout
-rw-r--r-- 1 user user 3360 2011-04-17 12:30 .bashrc
-rw-r--r-- 1 user user  675 2010-04-18 18:51 .profile
[...]
```

Die gleiche Zeichenfolge wird auch verwendet, um Kommentare in die Listings einzubauen. Im folgenden Beispiel soll zwischen zwei Kommandos neun Minuten gewartet werden:

```
[...]
user@lx01:~$ klist -f
[...]
[...9 Minuten warten...]
user@lx01:~$ kinit  -R
user@lx01:~$ klist -f
[...]
```

Der Text *[...9 Minuten warten...]* ist also kein Teil einer Programmausgabe, sondern ein Kommentar.

Der Prompt hängt vom Betriebssystem ab. Befehlszeilen unter Linux werden durch einen Prompt wie dem folgenden eingeleitet:

```
user@lx01:~$
```

unter Windos geschieht das in dieser Art:

```
C:\>
```

Danksagung

Mein Dank gilt in erster Linie meiner Frau und meinen Kindern, ohne deren Unterstützung ich dieses Werk nicht hätte fertigstellen können. Vielen Dank auch an Freunde und Arbeitskollegen für viele anregende Diskussionen.

Oliver Tennert gilt ein besonderer Dank für Anregungen und Diskussionen während der Entstehung dieses Buches. Vielen Dank auch an Markus Widmer und Heiko Hütter für Tests der beschriebenen Infrastrukturen und ihre Rückmeldungen zu den LDAP-spezifischen Teilen. René Schönfeldt und dem Team beim dpunkt.verlag sowie allen Gutachtern ebenfalls ein herzliches Dankeschön für die Unterstützung bei der Realisierung dieses Buchprojektes.

Kontakt

Für Fragen, Anregungen, Kritik und Feedback jeglicher Art ist der Autor unter seiner E-Mail-Adresse `mark@mproehl.net` zu erreichen.

Im Internet

www.kerberos-buch.de

Unter `http://www.kerberos-buch.de` befindet sich die Homepage dieses Buches. Dort finden Sie Informationen rund um das Kerberos-Buch, insbesondere sind dort sämtliche Listings und Errata verfügbar.