

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 Identitäten, 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 Nutzer:innen 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 User- 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 Netzwerk- und Verwaltungsumgebungen zu schaffen.

Welche Ziele hat dieses Buch?

Dieses Buch möchte Ihnen 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 werden. 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 Ihnen 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 Administrator:innen heterogener Netzwerkumgebungen, die sich eingehend mit Single Sign-on und Kerberos beschäftigen wollen. Für Anwendungsprogrammierer:innen werden vor allem jene Buchteile interessant sein, die die Funktionsweise des Kerberos-Protokolls und die Kerberisierung existierender Netzwerkdienste beschreiben.

Welche Voraussetzungen sollten Sie mitbringen?

Unsere Leser:innen sollten über allgemeine Grundkenntnisse der Administration von Linux- und Windows-Systemen verfügen, 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). Wenn Sie sich bereits mit den Themengebieten Authentisierung, Autorisierung und Zugriffskontrolle beschäftigt haben, wird Ihnen 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:innen. 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 lernen Sie anhand verschiedener Beispielumgebungen, wie man Kerberos-Infrastrukturen aufbaut und verwaltet. Verschiedene Kapitel von Teil II benötigen zusätzliche Komponenten wie NTP, DNS und LDAP sowie eine Infrastruktur für X.509-Zertifikate, 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. Kapitel 15 behandelt dabei die Microsoft-Implementierung von Active Directory, Kapitel 16 die dazu kompatible, freie Alternative des Samba-Projekts. Eine konzeptionell ähnliche integrierte Lösung speziell für Linux-Umgebungen ist FreeIPA, das Kapitel 17 im Detail vorstellt. Teil II wird von Kapitel 18 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 User- 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 unsere Leser:innen anhand zahlreicher Beispiele lernen können.

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.

Diese Leseprobe haben Sie beim
 edv-buchversand.de heruntergeladen.
Das Buch können Sie online in unserem
Shop bestellen.

[Hier zum Shop](#)