Linux mit dem Active Directory verbinden

Eingehakt

Udo Seidel

Einen Linux-Server ans Active Directory (AD) anzubinden, ist heutzutage eigentlich kein Problem mehr. Allerdings gibt es verschiedene Möglichkeiten dafür, was etwas verwirrend sein kann.

Soll ein Linux-System Dienste eines Active Directory nutzen, lassen sich zunächst zwei Kategorien unterscheiden: die Verwendung von Bordmitteln der Distribution und die Anschaffung eines entsprechenden Dritthersteller-Produktes wie Centrify, PowerBroker Identity Services oder der nun zu Dell gehörenden Software von Quest (siehe „Alle Links“).

Entscheidet man sich fürs Verwenden von Linux-Bordmitteln, gibt es mehrere Wege. Im einfachsten Fall geht es nur darum, die Benutzer- und Passwortverwaltung an das Active Directory auszulagern. Dies geschieht über Kerberos und LDAP (Lightweight Directory Access Protocol) beziehungsweise die entsprechenden Client-Programme. Für den Anwender fügt anschließend PAM (Pluggable Authentication Module) alles zusammen – dazu später mehr.

Moderner SSSD oder Urgestein NSCD

Das Kerberos-Modul ist für die Authentisierung zuständig, das LDAP-Pendant stellt die Namensauflösung zur Verfügung. Eventuell kommt noch ein Caching-Mechanismus über NSCD (Name Service Caching Daemon) zum Einsatz. Moderne Linux-Distributionen bringen geeignete Werkzeuge für die (interaktive) Konfiguration von Kerberos, LDAP und PAM mit. Wer das selbst erledigen möchte, muss die Dateien */etc/nsswitch.conf*, */etc/krb5.conf* und */etc/nslcd.conf* sowie die PAM-Konfiguration in */etc/pam.conf* oder */etc/pam.d* bearbeiten.

Auf modernen Linux-Systemen ist NSCD oft durch SSSD (System Security Services Daemon) abgelöst. Dieser hat ein fürs AD spezifiziertes Modul, das beispielsweise das Zwischenspeichern von Log-in-Informationen erlaubt. So kann sich der Linux-Anwender anmelden, wenn der Rechner gerade keine Verbindung zum Domänencontroller hat. Ein weiterer Vorteil ist die Möglichkeit zur Verschlüsselung von Authentisierung und Namensauflösung. Wer auf die Verwendung der Distributionswerkzeuge verzichtet, muss statt */etc/nslcd.conf* die Datei */etc/sssd.conf* anpassen, dazu die oben erwähnten anderen Dateien.

Neben der Authentisierung gibt es einen weiteren Grund, dass ein Linux-Rechner einer AD-Domäne beitritt: den Zugriff auf Netzlaufwerke und Drucker. Dazu muss Linux das SMB-Protokoll beziehungsweise dessen Dialekt CIFS beherrschen. Hier kommt Samba ins Spiel und ist damit eine Pflicht-Komponente für diese Anwendungsfälle – genau genommen dessen Bestandteil *winbind*. Er übernimmt die Authentisierung und die Namensauflösung, ist modular aufgebaut und verfügt über mehrere Backends. Eines interagiert mit Kerberos, das im Hintergrund gegen das AD authentisiert. Ein anderes übernimmt das ID-Mapping. In den vorigen Anwendungsfällen war dies nicht nötig. Für den problemlosen Zugriff auf Netzressourcen wie Dateiserver-Freigaben oder Drucker ist eine eindeutige Zuordnung der UNIX-Informationen wie UID und GID zu den Windows Security Identifiers (SID) jedoch notwendig.

Auch hier hat der Anwender Wahlmöglichkeiten: Der einfachere Fall sind statische (unveränderbare) User-Attribute im AD. Pfade zum persönlichen Verzeichnis oder zur Log-in-Shell sind für alle Linux-Benutzer von derselben Struktur. Die Konfiguration von *winbind* ist etwas einfacher als die von SSSD und benutzt das Backend *idmap_rid*. Der Linux-Server kann in der Domäne auch Dateifreigaben und Drucker ansprechen – anders als SSSD beherrscht Samba das SMB-/CIFS-Protokoll und damit einiges mehr als nur Authentisierung über das AD. Diese Einbindung erfordert kaum Zusatzaufwand von den AD-Administratoren.

Anders sieht es aus, wenn die Log-in-Shells oder die Struktur der persönlichen Verzeichnisse nicht einheitlich sind. Die zugehörigen Einträge im AD müssen dann entsprechend konfigurierbar sein. Alte Hasen erinnern sich hier sicherlich an die Schemaerweiterung von Microsofts SFU (Services for UNIX). Die moderne Variante heißt: Unterstützung für RFC2307-Attribute (siehe „Alle Links“). *winbind* verwendet das darauf zugeschnittene Backend *idmap_ad*. Idealerweise stellt der Linux-Dienstleister gute Konfigurationswerkzeuge zur Verfügung. Für die manuelle Konfiguration muss der Administrator die Dateien */etc/nsswitch.conf*, */etc/samba/smb.conf* und */etc/krb5.conf* anpassen, dazu die beiden oben erwähnten PAM-Konfigurationsdateien.

Zum Schluss ein paar Worte zu den Pluggable Authentication Modules (PAM). Die PAM-Bibliotheken sind eine Abstraktionsschicht [1]. Sie bietet eine einheitliche Schnittstelle für Anwendungen, die Authentisierung benötigen, und kann im Hintergrund auf zahlreiche Infrastrukturen beziehungsweise Anbieter zurückgreifen. Die Umsetzung einer bestimmten Technik für PAM manifestiert sich als eine PAM-Bibliothek. Bei Centrify heißt sie *pam_centrifydc.so*, bei Winbind *pam_winbind.so*, und für SSSD gibt es *pam_sss.so*. (tiw)

Udo Seidel

arbeitet als Chief Architect und Digital Evangelist bei der Amadeus Data Processing GmbH in Erding.

Literatur

[1] Udo Seidel; Authentifizierung; Zuspiel; Kurz erklärt: PAM; *iX* 1/2015, S. 117

Alle Links: www.ix.de/ix1610150