10.7 Verzeichnisdienste, Netzwerkmanagement und Zeitdienste: LDAP, SNMP und NTP

LDAP, SNMP und NTP gehören zur OSI-Schicht 7.

Sie erfüllen unterschiedliche Aufgaben in Netzwerken:

```
LDAP:
Verzeichnisdienste abfragen und verwalten

SNMP:
Netzwerkgeräte überwachen und verwalten

NTP:
Uhrzeit synchronisieren
```

Diese Dienste sind besonders in Unternehmensnetzwerken wichtig.

Merksatz:

```
LDAP verwaltet Verzeichnisinformationen.
SNMP überwacht Geräte.
NTP synchronisiert Zeit.
```

Grundidee

In Netzwerken müssen nicht nur Daten übertragen werden.

Es müssen auch Dienste bereitstehen für:

```
- Benutzerinformationen
- Gruppen
- Geräteinformationen
- zentrale Anmeldung
- Monitoring
- Zustandsabfragen
- Zeitabgleich
- Protokollierung
```

- Authentifizierung

LDAP, SNMP und NTP unterstützen genau solche Verwaltungsaufgaben.

Merksatz:

> Schicht 7 enthält viele Verwaltungs- und Infrastrukturprotokolle.

Einordnung im OSI-Modell

Thema	Schicht
LDAP	7
SNMP	7
NTP	7
TCP-/UDP-Port	4
IP-Adresse	3
TLS bei LDAPS	6 mit Schicht-7-Bezug
Benutzer- und Gruppendaten	7 / Verzeichnisdienst
Monitoringdaten	7 / Managementdienst

Merksatz:

> Dienstprotokoll = Schicht 7.
> Port = Schicht 4.

LDAP

LDAP steht für:

> Lightweight Directory Access Protocol

LDAP dient dazu, Informationen aus einem Verzeichnisdienst abzufragen oder zu verwalten.

Typische Informationen:

- Benutzer
- Gruppen
- Computer
- Organisationseinheiten
- E-Mail-Adressen
- Telefonnummern
- Rollen
- Berechtigungsbezüge

Merksatz:

LDAP = Zugriff auf Verzeichnisdienste.

Was ist ein Verzeichnisdienst?

Ein Verzeichnisdienst speichert strukturierte Informationen über Objekte in einer Organisation.

Beispiele für Objekte:

- Benutzerkonto
- Gruppe
- Computer
- Drucker
- Dienstkonto
- Kontakt
- Organisationseinheit

Der Verzeichnisdienst ermöglicht zentrale Verwaltung.

Merksatz:

Verzeichnisdienst = zentrale Datenbank für Identitäten und Objekte.

Typische Verzeichnisdienste

Typische Verzeichnisdienste sind:

- Microsoft Active Directory
- OpenLDAP
- FreeIPA
- Samba AD
- cloudbasierte Identitätsdienste mit LDAP-Anbindung

Besonders wichtig im FISI-Umfeld ist:

Active Directory

Merksatz:

Active Directory ist ein sehr verbreiteter Verzeichnisdienst.

LDAP und Active Directory

Active Directory nutzt LDAP für viele Abfragen.

Beispiele:

Benutzer anmelden
Gruppenmitgliedschaften prüfen
Benutzerobjekte suchen
Computerobjekte verwalten
Verzeichnisinformationen abfragen

Wichtig:

Active Directory besteht nicht nur aus LDAP.
Es nutzt auch DNS, Kerberos, Gruppenrichtlinien und weitere Dienste.

Merksatz:

LDAP ist ein wichtiger Teil von Active Directory,
aber nicht das ganze Active Directory.

LDAP-Ports

Wichtige LDAP-Ports:

Dienst	Protokoll	Port
LDAP	TCP / UDP	389
LDAPS	TCP	636

LDAP über Port 389 kann zusätzlich mit STARTTLS abgesichert werden.

LDAPS nutzt direkt TLS.

Merksatz:

> LDAP = 389.
> LDAPS = 636.

LDAP und LDAPS unterscheiden

Begriff	Bedeutung
LDAP	Verzeichniszugriff, klassisch Port 389
LDAPS	LDAP über TLS, klassisch Port 636
LDAP mit STARTTLS	startet auf 389 und schaltet auf TLS um

Wichtig:

> Für Anmeldedaten und sensible Informationen sollte verschlüsselte Kommunikation genutzt werden.

Merksatz:

> LDAPS schützt LDAP-Kommunikation mit TLS.

LDAP-Baumstruktur

LDAP-Daten sind hierarchisch organisiert.

Man kann sich das wie einen Baum vorstellen.

Beispiel:

```
Firma
├── Benutzer
├── Gruppen
├── Computer
└── Drucker
```

Jedes Objekt hat eine Position im Verzeichnisbaum.

Merksatz:

```
LDAP ist hierarchisch aufgebaut.
```

Distinguished Name

Ein Distinguished Name beschreibt die eindeutige Position eines Objekts im LDAP-Verzeichnis.

Kurz:

```
DN
```

Beispiel:

```
CN=Felix Ulrich,OU=Benutzer,DC=firma,DC=local
```

Bedeutung:

```
CN = Common Name
OU = Organizational Unit
DC = Domain Component
```

Merksatz:

```
DN = eindeutiger LDAP-Pfad eines Objekts.
```

Common Name

CN steht für:

```
Common Name
```

CN bezeichnet häufig den Namen eines Objekts.

Beispiel:

```
CN=Felix Ulrich
```

Merksatz:

```
CN = Name eines LDAP-Objekts.
```

Organizational Unit

OU steht für:

```
Organizational Unit
```

Eine OU ist eine Organisationseinheit.

Beispiel:

```
OU=Benutzer
OU=Computer
OU=Berlin
OU=Ausbildung
```

OUs helfen, Objekte zu strukturieren und zu verwalten.

Merksatz:

```
OU = Organisationseinheit im Verzeichnis.
```

Domain Component

DC steht für:

```
Domain Component
```

DC bildet Teile des Domänennamens ab.

Beispiel:

```
firma.local
```

wird zu:

```
DC=firma,DC=local
```

Merksatz:

```
DC bildet den Domänennamen im LDAP-Pfad ab.
```

LDAP-Attribute

LDAP-Objekte haben Attribute.

Beispiele für Benutzerattribute:

```
- cn
- givenName
- sn
- mail
- telephoneNumber
- memberOf
- userPrincipalName
- sAMAccountName
```

Diese Attribute beschreiben das Objekt genauer.

Merksatz:

```
LDAP-Attribute speichern Eigenschaften eines Objekts.
```

LDAP-Suche

Eine LDAP-Suche fragt Objekte aus dem Verzeichnis ab.

Typische Suchfragen:

```
Gibt es diesen Benutzer?
Welche Gruppen hat der Benutzer?
Welche E-Mail-Adresse hat der Benutzer?
Welche Computer gehören zu einer OU?
Welche Benutzer sind deaktiviert?
```

Merksatz:

```
LDAP-Suche findet Objekte und Attribute im Verzeichnis.
```

LDAP-Filter

LDAP-Filter grenzen Suchergebnisse ein.

Beispiel sinngemäß:

```
Suche Benutzer mit bestimmtem Namen.
```

Oder:

```
Suche alle Benutzer in einer bestimmten Gruppe.
```

Filter sind wichtig, damit Abfragen gezielt und effizient sind.

Merksatz:

```
LDAP-Filter bestimmen,
welche Objekte gesucht werden.
```

Bind

Bind bedeutet bei LDAP:

```
Anmeldung oder Authentifizierung am Verzeichnisdienst.
```

Ein Client verbindet sich mit dem LDAP-Server und authentifiziert sich.

Mögliche Varianten:

```
- anonym
- Benutzername und Passwort
- Dienstkonto
- Kerberos in AD-Umgebungen
```

Merksatz:

```
LDAP Bind = Anmeldung am Verzeichnisdienst.
```

LDAP und Authentifizierung

Viele Anwendungen nutzen LDAP, um Benutzer gegen ein zentrales Verzeichnis zu prüfen.

Beispiel:

```
Benutzer meldet sich an Anwendung an.
Anwendung prüft Benutzer über LDAP.
LDAP bestätigt oder lehnt ab.
Anwendung prüft zusätzlich Gruppen oder Rollen.
```

Merksatz:

```
LDAP kann zentrale Anmeldung und Gruppenprüfung unterstützen.
```

LDAP und Autorisierung

LDAP kann Gruppeninformationen liefern.

Beispiel:

```
Benutzer ist Mitglied der Gruppe:
IT-Admins
```

Eine Anwendung kann daraus ableiten:

```
Benutzer darf Adminbereich öffnen.
```

Wichtig:

```
LDAP liefert Informationen.
Die Anwendung entscheidet oft,
welche Rechte daraus entstehen.
```

Merksatz:

```
LDAP liefert Identitäts- und Gruppeninformationen.
```

Typische LDAP-Fehler

Typische Fehler sind:

```
- falscher LDAP-Server
- falscher Port
- DNS-Name nicht auflösbar
- falscher Bind-Benutzer
- falsches Passwort
- Benutzer nicht gefunden
- falscher Base-DN
- falscher Suchfilter
- TLS-Zertifikatsfehler bei LDAPS
- Firewall blockiert Port 389 oder 636
```

Merksatz:

```
LDAP-Fehler betreffen oft Server,
Port,
Bind,
```

```
Base-DN
oder Zertifikat.
```

Fehlerbild: Anmeldung über LDAP funktioniert nicht

Mögliche Ursachen:

```
- Benutzername falsch
- Passwort falsch
- Benutzerkonto gesperrt
- LDAP-Server nicht erreichbar
- falscher LDAP-Port
- falscher Base-DN
- falscher Suchfilter
- Gruppe fehlt
- LDAPS-Zertifikat ungültig
- Anwendung nutzt falsches Dienstkonto
```

Merksatz:

```
LDAP-Anmeldefehler mit Konto,
Server,
Suche
und Gruppen prüfen.
```

SNMP

SNMP steht für:

```
Simple Network Management Protocol
```

SNMP wird zur Überwachung und Verwaltung von Netzwerkgeräten genutzt.

Typische Geräte:

```
- Switches
- Router
- Firewalls
```

- Drucker
- Server
- USV-Anlagen
- Access Points
- NAS-Systeme

Merksatz:

SNMP = Netzwerkgeräte überwachen und verwalten.

Was kann man mit SNMP abfragen?

Mit SNMP kann man viele Geräteinformationen abfragen.

Beispiele:

- Gerätename
- Uptime
- CPU-Auslastung
- RAM-Auslastung
- Interface-Status
- Traffic pro Port
- Fehlerzähler
- Temperatur
- Tonerstand
- Lüfterstatus
- Seriennummer

Merksatz:

SNMP liefert Messwerte und Zustandsinformationen.

SNMP-Manager und SNMP-Agent

Bei SNMP gibt es meist:

SNMP-Manager
SNMP-Agent

SNMP-Manager:

Monitoring-System,
das Werte abfragt.

SNMP-Agent:

Dienst auf dem überwachten Gerät,
der Informationen bereitstellt.

Beispiel:

Monitoring-Server fragt Switch ab.
Switch-Agent liefert Interface-Daten.

Merksatz:

Manager fragt.
Agent antwortet.

SNMP-Ports

Wichtige SNMP-Ports:

Funktion	Protokoll	Port
SNMP-Abfragen	UDP	161
SNMP-Traps	UDP	162

Merksatz:

SNMP-Abfrage = UDP 161.
SNMP-Trap = UDP 162.

SNMP-Abfrage

Bei einer SNMP-Abfrage fragt der Manager gezielt einen Wert ab.

Beispiel:

```
Wie hoch ist die CPU-Auslastung?
Ist Port 5 am Switch aktiv?
Wie viele Fehler gab es auf Interface 1?
```

Der Agent antwortet mit dem passenden Wert.

Merksatz:

```
SNMP-Abfrage = Manager fragt Gerät nach Wert.
```

SNMP-Trap

Ein SNMP-Trap ist eine Meldung, die ein Gerät von sich aus an den Manager sendet.

Beispiele:

```
Link down
Lüfter ausgefallen
Temperatur zu hoch
USV läuft auf Batterie
Gerät startet neu
```

Merksatz:

```
Trap = Gerät meldet Ereignis selbstständig.
```

MIB

MIB steht für:

```
Management Information Base
```

Die MIB beschreibt, welche Informationen ein Gerät per SNMP bereitstellt.

Sie enthält eine strukturierte Sammlung von verwaltbaren Objekten.

Merksatz:

MIB beschreibt verfügbare SNMP-Informationen.

OID

OID steht für:

Object Identifier

Eine OID ist eine eindeutige Nummer für einen bestimmten SNMP-Wert.

Beispiel sinngemäß:

OID für Gerätenamen
OID für Interface-Traffic
OID für CPU-Auslastung

Merksatz:

OID = eindeutige Kennung eines SNMP-Werts.

SNMP-Versionen

Wichtige SNMP-Versionen:

Version	Kurzinfo
SNMPv1	alt, einfach
SNMPv2c	verbreitet, Community-String
SNMPv3	sicherer mit Authentifizierung und Verschlüsselung

Für moderne Umgebungen ist SNMPv3 vorzuziehen.

Merksatz:

SNMPv3 ist sicherer als SNMPv1/v2c.

Community-String

Bei SNMPv1 und SNMPv2c wird ein Community-String verwendet.

Er wirkt wie ein einfaches Passwort.

Beispiele:

```
public
private
```

Problem:

```
Community-Strings werden bei alten SNMP-Versionen nicht sicher geschützt.
```

Merksatz:

```
Community-String ist kein starker Schutz.
```

SNMPv3

SNMPv3 bietet bessere Sicherheitsfunktionen.

Dazu gehören:

```
- Authentifizierung
- Verschlüsselung
- Benutzerkonzept
- Integritätsschutz
```

Damit ist SNMPv3 deutlich sicherer als ältere Varianten.

Merksatz:

```
SNMPv3 für sichere Überwachung bevorzugen.
```

SNMP und Monitoring

Monitoring-Systeme nutzen SNMP, um Geräte regelmäßig abzufragen.

Beispiele für Monitoring:

- Ist Gerät erreichbar?
- Ist ein Port down?
- Wie hoch ist die Auslastung?
- Gibt es Fehler auf Interfaces?
- Wird Speicher knapp?
- Gibt es Temperaturprobleme?

Merksatz:

SNMP ist wichtig für Netzwerkmonitoring.

Typische SNMP-Fehler

Typische Fehler sind:

- SNMP-Agent deaktiviert
- falsche SNMP-Version
- falscher Community-String
- falsche SNMPv3-Zugangsdaten
- Firewall blockiert UDP 161 oder 162
- Monitoring-Server nicht erlaubt
- Gerät unterstützt OID nicht
- MIB fehlt im Monitoring-System
- ACL auf Gerät blockiert Zugriff

Merksatz:

SNMP-Fehler betreffen oft Version,
Zugangsdaten,
Firewall
oder OID.

Fehlerbild: Monitoring zeigt Gerät als down

Mögliche Ursachen:

```
- Gerät wirklich offline
- IP-Adresse falsch
- DNS falsch
- ICMP blockiert
- SNMP-Agent aus
- Firewall blockiert
- falsche SNMP-Zugangsdaten
- falsche SNMP-Version
- Monitoring fragt falsche Schnittstelle
```

Merksatz:

```
Monitoring-Fehler erst mit Erreichbarkeit und SNMP prüfen.
```

NTP

NTP steht für:

```
Network Time Protocol
```

NTP dient zur Zeitsynchronisation von Systemen.

Typischer Port:

```
UDP 123
```

Korrekte Zeit ist in IT-Systemen sehr wichtig.

Merksatz:

```
NTP = Zeitsynchronisation über Netzwerk.
```

Warum ist korrekte Zeit wichtig?

Korrekte Zeit wird benötigt für:

- Zertifikate
- Kerberos
- Active Directory
- Logs
- Fehlersuche
- Backup-Zeitpunkte
- Monitoring
- Dateisynchronisation
- Datenbanktransaktionen
- Sicherheitsereignisse

Schon wenige Minuten Abweichung können Probleme verursachen.

Merksatz:

> Falsche Uhrzeit kann viele IT-Probleme verursachen.

NTP-Client und NTP-Server

Bei NTP gibt es:

> NTP-Client
> NTP-Server

NTP-Client:

> fragt Zeit ab.

NTP-Server:

> liefert Zeitinformationen.

In Unternehmen synchronisieren Clients oft gegen interne Zeitserver.

Merksatz:

> NTP-Client fragt Zeit vom NTP-Server ab.

NTP-Stratum

NTP nutzt sogenannte Stratum-Werte.

Sie beschreiben die Entfernung zur ursprünglichen Zeitquelle.

Beispiel:

```
Stratum 0:
direkte Zeitquelle, zum Beispiel Atomuhr oder GPS

Stratum 1:
Server direkt an Stratum-0-Quelle

Stratum 2:
Server synchronisiert von Stratum 1
```

Je kleiner der Stratum-Wert, desto näher an der ursprünglichen Zeitquelle.

Merksatz:

```
Stratum beschreibt die Nähe zur Zeitquelle.
```

NTP und Active Directory

In Active-Directory-Umgebungen ist Zeit besonders wichtig.

Grund:

```
Kerberos ist empfindlich gegenüber Zeitabweichungen.
```

Wenn Client und Domänencontroller zu stark unterschiedliche Zeiten haben, kann Anmeldung fehlschlagen.

Merksatz:

```
AD und Kerberos brauchen korrekte Zeit.
```

NTP und Zertifikate

Zertifikate haben Gültigkeitszeiträume.

Wenn die Systemzeit falsch ist, kann ein eigentlich gültiges Zertifikat als ungültig erscheinen.

Beispiel:

```
Client-Uhr geht ein Jahr falsch.
Browser meldet Zertifikatsfehler.
```

Merksatz:

```
Falsche Uhrzeit kann Zertifikatswarnungen verursachen.
```

NTP und Logs

Logs sind nur sinnvoll, wenn Zeitstempel stimmen.

Bei Fehlersuche muss man Ereignisse zeitlich zusammenbringen können.

Beispiele:

```
Firewall-Log
Server-Log
Anwendungslog
Authentifizierungslog
```

Wenn Systeme unterschiedliche Uhrzeiten haben, wird die Analyse erschwert.

Merksatz:

```
Ohne korrekte Zeit sind Logs schwer auswertbar.
```

NTP und Sicherheit

NTP sollte sicher und sinnvoll konfiguriert werden.

Wichtige Punkte:

- vertrauenswürdige Zeitquellen nutzen
- interne Zeitserver verwenden
- keine unnötig offenen NTP-Server betreiben
- Firewall-Regeln kontrollieren
- Zeitabweichungen überwachen
- Manipulation vermeiden

Merksatz:

Zeit ist sicherheitsrelevant.

Typische NTP-Fehler

Typische Fehler sind:

- NTP-Server nicht erreichbar
- UDP 123 blockiert
- falscher Zeitserver eingetragen
- große Zeitabweichung
- falsche Zeitzone
- Systemzeit driftet
- virtuelle Maschinen synchronisieren falsch
- mehrere Zeitquellen widersprechen sich
- DNS-Name des Zeitservers nicht auflösbar

Merksatz:

NTP-Fehler betreffen Zeitserver,
UDP 123,
DNS
oder Systemkonfiguration.

Fehlerbild: Zertifikate wirken ungültig

Mögliche Ursache:

Systemzeit ist falsch.

Prüfung:

```
Datum prüfen.
Uhrzeit prüfen.
Zeitzone prüfen.
NTP-Status prüfen.
Zeitquelle prüfen.
```

Merksatz:

```
Bei vielen Zertifikatsfehlern auch Uhrzeit prüfen.
```

Fehlerbild: Anmeldung an Domäne schlägt fehl

Mögliche Ursache:

```
Zeitabweichung zwischen Client und Domänencontroller.
```

Besonders relevant:

```
Kerberos
```

Prüfung:

```
Clientzeit prüfen.
Domänencontrollerzeit prüfen.
NTP-Konfiguration prüfen.
Zeitzone prüfen.
```

Merksatz:

```
Domänenanmeldung braucht passende Zeit.
```

Fehlerbild: Logs passen zeitlich nicht zusammen

Mögliche Ursachen:

- falsche Systemzeit
- falsche Zeitzone
- NTP gestört
- Zeitquelle falsch
- Sommerzeitproblem
- Container oder VM nutzt falsche Zeitbasis

Merksatz:

Log-Auswertung braucht synchronisierte Zeit.

LDAP, SNMP und NTP vergleichen

Protokoll	Hauptaufgabe	typischer Port
LDAP	Verzeichnisdienstzugriff	TCP/UDP 389
LDAPS	LDAP über TLS	TCP 636
SNMP	Netzwerkmanagement	UDP 161
SNMP-Trap	Ereignismeldung	UDP 162
NTP	Zeitsynchronisation	UDP 123

Merksatz:

LDAP 389/636,
SNMP 161/162,
NTP 123.

Sicherheitsvergleich

Protokoll	Sicherheitsaspekt
LDAP	Anmeldedaten schützen, LDAPS oder STARTTLS nutzen
SNMP	SNMPv3 bevorzugen, Community-Strings schützen
NTP	vertrauenswürdige Zeitquellen und Zugriffsbeschränkung
LDAPS	Zertifikate korrekt prüfen
SNMPv1/v2c	möglichst vermeiden oder stark einschränken

Merksatz:

Infrastrukturprotokolle müssen ebenfalls abgesichert werden.

Fehlersuche allgemein

Eine sinnvolle Reihenfolge:

1. Namensauflösung prüfen.
2. IP-Erreichbarkeit prüfen.
3. Port prüfen.
4. Dienst läuft?
5. Zugangsdaten korrekt?
6. Verschlüsselung oder Zertifikat korrekt?
7. Berechtigungen korrekt?
8. Logs prüfen.

Merksatz:

Auch Verwaltungsdienste nach Schichten prüfen.

Was LDAP, SNMP und NTP nicht machen

LDAP macht nicht automatisch:

Berechtigungen in jeder Anwendung korrekt.

SNMP macht nicht automatisch:

Fehlerbehebung,
sondern liefert Informationen.

NTP macht nicht automatisch:

Zeitzonenlogik oder Zertifikatsverwaltung korrekt.

Alle drei Dienste brauchen korrekte Konfiguration und passende Sicherheit.

Merksatz:

Infrastrukturprotokolle unterstützen Administration,
ersetzen aber keine saubere Konfiguration.

Einordnung in typische Unternehmensnetze

In Unternehmen sieht man häufig:

LDAP / AD:
zentrale Benutzer und Gruppen

SNMP:
Monitoring von Switches, Routern und Servern

NTP:
einheitliche Zeit für Clients, Server und Logs

Diese Dienste sind nicht immer sichtbar für Benutzer, aber wichtig für stabilen Betrieb.

Merksatz:

LDAP, SNMP und NTP sind Grundlagen für Betrieb und Verwaltung.

Typische IHK-Fragen

In AP1 und AP2 kann zum Beispiel gefragt werden:

- Wofür steht LDAP?
- Wofür wird LDAP verwendet?
- Was ist ein Verzeichnisdienst?
- Was ist LDAPS?
- Welche Ports nutzen LDAP und LDAPS?
- Was ist ein Distinguished Name?
- Was ist ein LDAP Bind?
- Wofür steht SNMP?
- Wofür wird SNMP verwendet?
- Was sind SNMP-Manager und SNMP-Agent?
- Was ist ein SNMP-Trap?
- Welche Ports nutzt SNMP?

- Warum ist SNMPv3 sicherer?
- Wofür steht NTP?
- Warum ist korrekte Zeit wichtig?
- Welche Probleme können durch falsche Uhrzeit entstehen?

Typische Prüfungsfallen

LDAP gehört zu Schicht 7.

LDAP ist nicht das gesamte Active Directory.

LDAP nutzt typischerweise Port 389.

LDAPS nutzt typischerweise Port 636.

DN ist der eindeutige LDAP-Pfad.

Bind bedeutet LDAP-Anmeldung.

SNMP gehört zu Schicht 7.

SNMP nutzt UDP.

SNMP-Abfragen nutzen UDP 161.

SNMP-Traps nutzen UDP 162.

SNMPv1/v2c mit Community-String sind unsicherer.

SNMPv3 ist sicherer.

NTP gehört zu Schicht 7.

NTP nutzt UDP 123.

Falsche Zeit kann Zertifikatsfehler verursachen.

Falsche Zeit kann Kerberos-Probleme verursachen.

Logs brauchen synchronisierte Zeit.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
LDAP	Protokoll für Verzeichnisdienste
LDAPS	LDAP über TLS
Verzeichnisdienst	zentrale Verwaltung von Identitäten und Objekten
Active Directory	verbreiteter Microsoft-Verzeichnisdienst
DN	eindeutiger LDAP-Pfad
CN	Common Name eines Objekts
OU	Organisationseinheit
DC	Domain Component
Attribut	Eigenschaft eines LDAP-Objekts
Bind	Anmeldung am LDAP-Server
SNMP	Protokoll für Netzwerkmanagement
SNMP-Manager	fragt Gerätewerte ab
SNMP-Agent	liefert Gerätewerte
Trap	Gerät sendet Ereignis selbstständig
MIB	Beschreibung verfügbarer SNMP-Werte
OID	eindeutige Kennung eines SNMP-Werts
Community-String	einfacher Zugriffstext bei SNMPv1/v2c
SNMPv3	sicherere SNMP-Version
NTP	Protokoll zur Zeitsynchronisation
Stratum	Nähe zur Zeitquelle
Zeitserver	Server, der Uhrzeit bereitstellt

IHK-sichere Kurzformulierung

LDAP, SNMP und NTP sind Protokolle der Anwendungsschicht. LDAP steht für Lightweight Directory Access Protocol und dient dem Zugriff auf Verzeichnisdienste wie Active Directory. Es wird zum Suchen und Verwalten von Benutzern, Gruppen und anderen Objekten verwendet. SNMP steht für Simple Network Management Protocol und wird zur Überwachung von Netzwerkgeräten genutzt. Dabei fragt ein SNMP-Manager Werte von einem SNMP-Agenten ab oder empfängt Traps. NTP steht für Network Time Protocol und synchronisiert die Uhrzeit von Systemen. Korrekte Zeit ist wichtig

für Zertifikate, Kerberos, Logs und Fehlersuche.

Merksätze

LDAP = Lightweight Directory Access Protocol.

LDAP gehört zu Schicht 7.

LDAP greift auf Verzeichnisdienste zu.

Active Directory nutzt LDAP,
ist aber mehr als LDAP.

LDAP = Port 389.

LDAPS = Port 636.

DN = eindeutiger LDAP-Pfad.

Bind = Anmeldung am LDAP-Server.

SNMP = Simple Network Management Protocol.

SNMP gehört zu Schicht 7.

SNMP überwacht Netzwerkgeräte.

SNMP-Manager fragt.

SNMP-Agent antwortet.

SNMP-Abfrage = UDP 161.

SNMP-Trap = UDP 162.

MIB beschreibt verfügbare Werte.

OID kennzeichnet einen SNMP-Wert.

SNMPv3 ist sicherer als SNMPv1/v2c.

NTP = Network Time Protocol.

NTP gehört zu Schicht 7.

NTP nutzt UDP 123.

NTP synchronisiert Uhrzeit.

Korrekte Zeit ist wichtig für Zertifikate.

Korrekte Zeit ist wichtig für Kerberos.

Korrekte Zeit ist wichtig für Logs.

Infrastrukturprotokolle müssen ebenfalls abgesichert werden.