10.11 Merksätze und Prüfungswissen zu OSI-Schicht 7

Diese Seite fasst die wichtigsten Inhalte zur OSI-Schicht 7 zusammen.

OSI-Schicht 7 heißt:

```
Anwendungsschicht
```

Die Hauptaufgabe von Schicht 7 ist:

```
Netzwerkdienste für Anwendungen bereitstellen.
```

Typische Protokolle und Dienste sind:

```
- HTTP
- HTTPS
- DNS
- DHCP
- SMTP
- POP3
- IMAP
- FTP
- SFTP
- FTPS
- SMB
- LDAP
- SNMP
- NTP
- SSH
- RDP
- Telnet
- APIs
```

Merksatz:

```
Schicht 7 = Netzwerkdienste für Anwendungen.
```

Grundidee von Schicht 7

Schicht 7 ist die oberste Schicht des OSI-Modells.

Sie ist die Schicht, die Anwendungen am nächsten ist.

Wichtig:

> Die Anwendungsschicht ist nicht einfach das Programm selbst.

Besser:

> Anwendungen nutzen Protokolle der Anwendungsschicht.

Beispiel:

> Browser = Anwendung
>
> HTTP / HTTPS = Protokolle der Anwendungsschicht

Merksatz:

> Schicht 7 beschreibt Protokolle und Dienste,
> die Anwendungen für Netzwerkkommunikation verwenden.

Schicht 7 im OSI-Modell

Schicht	Name	Kerngedanke
7	Anwendungsschicht	Netzwerkdienste für Anwendungen
6	Darstellungsschicht	Daten darstellen, codieren, komprimieren, verschlüsseln
5	Sitzungsschicht	Sitzungen aufbauen, verwalten und beenden
4	Transportschicht	TCP, UDP, Ports
3	Vermittlungsschicht / Netzwerkschicht	IP, Routing
2	Sicherungsschicht	Frames, MAC-Adressen, VLAN
1	Bitübertragungsschicht	Bits, Signale, Medien

Merksatz:

```
Schicht 7 nutzt alle darunterliegenden Schichten.
```

Schicht 7 und Schicht 4 unterscheiden

Ein häufiger Prüfungsfehler ist, Ports und Protokolle zu vermischen.

Beispiel:

```
TCP 443 = Schicht 4

HTTPS = Schicht 7 mit TLS-Bezug
```

Oder:

```
UDP 53 / TCP 53 = Schicht 4

DNS = Schicht 7
```

Merksatz:

```
Port = Schicht 4.
Dienstprotokoll = Schicht 7.
```

Wichtige Standardports

Dienst	Protokoll	typischer Port
HTTP	TCP	80
HTTPS	TCP	443
DNS	UDP / TCP	53
DHCP-Server	UDP	67
DHCP-Client	UDP	68
SMTP	TCP	25
Submission	TCP	587
SMTPS	TCP	465

Dienst	Protokoll	typischer Port
POP3	TCP	110
POP3S	TCP	995
IMAP	TCP	143
IMAPS	TCP	993
FTP	TCP	21
SFTP	TCP	22
SSH	TCP	22
Telnet	TCP	23
SMB	TCP	445
LDAP	TCP / UDP	389
LDAPS	TCP	636
SNMP	UDP	161
SNMP-Trap	UDP	162
NTP	UDP	123
RDP	TCP	3389

Merksatz:

> Standardports helfen bei Prüfung und Fehlersuche,
> gehören aber zur Transportschicht.

HTTP und HTTPS

HTTP steht für:

> Hypertext Transfer Protocol

HTTPS steht für:

> Hypertext Transfer Protocol Secure

HTTP wird für Webkommunikation genutzt.

HTTPS ist:

HTTP über TLS

Typische Ports:

HTTP:
TCP 80

HTTPS:
TCP 443

Merksatz:

HTTP = Web ohne TLS.
HTTPS = Web mit TLS.

HTTP-Request und HTTP-Response

HTTP arbeitet mit:

Request
Response

Request:

Anfrage des Clients

Response:

Antwort des Servers

Beispiel:

Browser fordert Webseite an.
Webserver liefert Antwort.

Merksatz:

HTTP arbeitet mit Anfrage und Antwort.

HTTP-Methoden

Wichtige HTTP-Methoden:

Methode	Bedeutung
GET	Daten abrufen
POST	Daten senden oder erstellen
PUT	Ressource vollständig ersetzen
PATCH	Ressource teilweise ändern
DELETE	Ressource löschen
HEAD	nur Kopfzeilen abrufen
OPTIONS	Möglichkeiten abfragen

Merksatz:

GET liest.
POST sendet.
PUT ersetzt.
PATCH ändert teilweise.
DELETE löscht.

HTTP-Statuscodes

HTTP-Statuscodes zeigen das Ergebnis einer Anfrage.

Bereich	Bedeutung
1xx	Information
2xx	Erfolg
3xx	Weiterleitung
4xx	Clientfehler
5xx	Serverfehler

Wichtige Beispiele:

Statuscode	Bedeutung

200	OK
301	dauerhaft weitergeleitet
302	vorübergehend weitergeleitet
400	fehlerhafte Anfrage
401	nicht authentifiziert
403	verboten
404	nicht gefunden
500	interner Serverfehler
502	Bad Gateway
503	Dienst nicht verfügbar
504	Gateway Timeout

Merksatz:

```
2xx = Erfolg.
4xx = Clientproblem.
5xx = Serverproblem.
```

---

401 und 403 unterscheiden

401 bedeutet:

```
nicht authentifiziert
```

Der Benutzer ist nicht angemeldet oder die Anmeldung ist ungültig.

403 bedeutet:

```
verboten
```

Der Benutzer ist möglicherweise angemeldet, hat aber keine Berechtigung.

Merksatz:

```
401 = Wer bist du?
403 = Du darfst das nicht.
```

DNS

DNS steht für:

```
Domain Name System
```

DNS löst Namen in IP-Adressen auf.

Beispiel:

```
www.example.com
→ IP-Adresse
```

DNS gehört zur Anwendungsschicht, nutzt aber UDP oder TCP auf Port 53.

Merksatz:

```
DNS = Name zu IP-Adresse.
```

Wichtige DNS-Records

Record	Bedeutung
A	Name zu IPv4-Adresse
AAAA	Name zu IPv6-Adresse
CNAME	Alias auf anderen Namen
MX	Mailserver einer Domain
NS	zuständiger Nameserver
TXT	Textinformationen
PTR	Reverse-DNS-Eintrag
SRV	Dienststandort
SOA	Verwaltungsdaten einer Zone

Merksatz:

```
A = IPv4.
AAAA = IPv6.
MX = Mailserver.
```

```
PTR = Reverse Lookup.
```

Forward Lookup und Reverse Lookup

Forward Lookup bedeutet:

```
Name zu IP-Adresse
```

Beispiel:

```
server01.firma.local
→ 192.168.10.20
```

Reverse Lookup bedeutet:

```
IP-Adresse zu Name
```

Beispiel:

```
192.168.10.20
→ server01.firma.local
```

Merksatz:

```
Forward = Name zu IP.
Reverse = IP zu Name.
```

DNS-TTL

TTL steht für:

```
Time To Live
```

Die TTL gibt an, wie lange ein DNS-Eintrag zwischengespeichert werden darf.

Folge:

```
DNS-Änderungen sind nicht immer sofort überall sichtbar.
```

Merksatz:

```
TTL steuert DNS-Caching.
```

DHCP

DHCP steht für:

```
Dynamic Host Configuration Protocol
```

DHCP verteilt automatisch Netzwerkkonfigurationen.

Ein Client kann erhalten:

```
- IP-Adresse
- Subnetzmaske
- Standard-Gateway
- DNS-Server
- Domain-Suffix
- Lease-Zeit
```

DHCP gehört zur Anwendungsschicht, liefert aber wichtige Schicht-3-Konfiguration.

Merksatz:

```
DHCP = automatische IP-Konfiguration.
```

DHCP-DORA

Der klassische DHCP-Ablauf heißt:

```
DORA
```

DORA steht für:

```
Discover
Offer
Request
Acknowledge
```

Ablauf:

```
Client sucht DHCP-Server.
Server bietet Konfiguration an.
Client fordert Angebot an.
Server bestätigt Vergabe.
```

Merksatz:

```
DHCP-Ablauf = DORA.
```

DHCP-Relay

DHCP startet häufig mit Broadcast.

Router leiten Broadcasts normalerweise nicht einfach weiter.

Wenn DHCP-Client und DHCP-Server in verschiedenen Netzen liegen, braucht man:

```
DHCP-Relay
```

Bei manchen Herstellern heißt das:

```
IP Helper Address
```

Merksatz:

```
DHCP-Relay bringt DHCP-Anfragen über Netzgrenzen.
```

APIPA

Wenn ein Windows-Client keine DHCP-Adresse erhält, kann er sich selbst eine Adresse aus diesem Bereich geben:

```
169.254.0.0/16
```

Das nennt man:

```
APIPA
```

Typisches Fehlerbild:

```
Client hat 169.254.x.x
```

Mögliche Ursache:

```
DHCP fehlgeschlagen
```

Merksatz:

```
169.254.x.x deutet oft auf DHCP-Probleme hin.
```

E-Mail-Protokolle

Die wichtigsten E-Mail-Protokolle sind:

```
SMTP
POP3
IMAP
```

Grundregel:

```
SMTP sendet.
POP3 und IMAP empfangen.
```

Merksatz:

```
SMTP raus.
POP3/IMAP rein.
```

SMTP

SMTP steht für:

```
Simple Mail Transfer Protocol
```

SMTP wird verwendet für:

```
- E-Mail senden
- E-Mail zwischen Mailservern weiterleiten
```

Typische Ports:

```
TCP 25:
Mailserver zu Mailserver

TCP 587:
Submission, also authentifiziertes Einreichen durch Clients

TCP 465:
SMTPS, also SMTP direkt über TLS
```

Merksatz:

```
SMTP = E-Mail senden und transportieren.
```

POP3

POP3 steht für:

```
Post Office Protocol Version 3
```

POP3 dient zum Abrufen von E-Mails.

Typische Ports:

```
POP3:
TCP 110
```

```
POP3S:
TCP 995
```

POP3 lädt E-Mails eher einfach ab und ist weniger gut für mehrere Geräte geeignet.

Merksatz:

```
POP3 = E-Mail abrufen.
```

IMAP

IMAP steht für:

```
Internet Message Access Protocol
```

IMAP dient zum Abrufen und Verwalten von E-Mails auf dem Server.

Typische Ports:

```
IMAP:
TCP 143

IMAPS:
TCP 993
```

IMAP eignet sich gut für mehrere Geräte, weil E-Mails und Ordner synchronisiert werden.

Merksatz:

```
IMAP = E-Mails auf dem Server verwalten und synchronisieren.
```

SPF, DKIM und DMARC

Diese Verfahren helfen bei E-Mail-Sicherheit.

Verfahren	Hauptaufgabe
SPF	legt erlaubte sendende Server fest

Verfahren	Hauptaufgabe
DKIM	signiert E-Mails kryptografisch
DMARC	legt Umgang mit SPF-/DKIM-Fehlern fest

Merksatz:

```
SPF erlaubt.
DKIM signiert.
DMARC entscheidet.
```

FTP, SFTP und FTPS

Diese Protokolle dienen der Dateiübertragung.

Protokoll	Bedeutung	Sicherheit
FTP	File Transfer Protocol	klassisch unverschlüsselt
SFTP	SSH File Transfer Protocol	über SSH verschlüsselt
FTPS	FTP mit TLS	über TLS geschützt

Typische Ports:

```
FTP:
TCP 21

SFTP:
TCP 22

FTPS implizit:
TCP 990
```

Merksatz:

```
FTP unverschlüsselt.
SFTP über SSH.
FTPS über TLS.
```

SFTP und FTPS nicht verwechseln

SFTP ist:

```
Dateiübertragung über SSH
```

FTPS ist:

```
FTP mit TLS
```

Das sind unterschiedliche Protokolle.

Merksatz:

```
SFTP ist nicht FTPS.
```

SMB

SMB steht für:

```
Server Message Block
```

SMB dient für:

```
- Datei-Freigaben
- Drucker-Freigaben
- Netzlaufwerke
- NAS-Freigaben
- Windows-Freigaben
```

Typischer Port:

```
TCP 445
```

Beispiel für einen UNC-Pfad:

```
\\server01\freigabe
```

Merksatz:

SMB = Datei- und Druckerfreigaben.

SMB-Berechtigungen

Bei SMB sind meist zwei Ebenen wichtig:

Freigabeberechtigungen
Dateisystemberechtigungen

Beispiel:

Freigabe erlaubt Vollzugriff.
Dateisystem erlaubt nur Lesen.

Ergebnis:

Benutzer kann nur lesen.

Merksatz:

Die strengere Berechtigung begrenzt den Zugriff.

LDAP

LDAP steht für:

Lightweight Directory Access Protocol

LDAP dient dem Zugriff auf Verzeichnisdienste.

Typische Nutzung:

- Benutzer suchen
- Gruppen prüfen
- Anmeldungen unterstützen
- zentrale Identitätsinformationen abfragen

Wichtige Ports:

```
LDAP:
TCP/UDP 389

LDAPS:
TCP 636
```

Merksatz:

```
LDAP = Zugriff auf Verzeichnisdienste.
```

Active Directory und LDAP

Active Directory nutzt LDAP, ist aber nicht nur LDAP.

Active Directory nutzt außerdem unter anderem:

```
- DNS
- Kerberos
- Gruppenrichtlinien
- Verzeichnisdatenbank
- Replikation
```

Merksatz:

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

SNMP

SNMP steht für:

```
Simple Network Management Protocol
```

SNMP dient zur Überwachung und Verwaltung von Netzwerkgeräten.

Typische Geräte:

```
- Switches
- Router
- Firewalls
- Drucker
- Server
- USV
- Access Points
```

Wichtige Ports:

```
SNMP-Abfrage:
UDP 161

SNMP-Trap:
UDP 162
```

Merksatz:

```
SNMP = Netzwerkgeräte überwachen.
```

SNMPv3

SNMPv3 ist sicherer als ältere SNMP-Versionen.

SNMPv3 kann bieten:

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

Ältere Varianten mit Community-String sind weniger sicher.

Merksatz:

```
SNMPv3 bevorzugen.
```

NTP

NTP steht für:

```
Network Time Protocol
```

NTP synchronisiert die Uhrzeit von Systemen.

Typischer Port:

```
UDP 123
```

Korrekte Zeit ist wichtig für:

```
- Zertifikate
- Kerberos
- Logs
- Monitoring
- Fehlersuche
- Backups
- Authentifizierung
```

Merksatz:

```
NTP = Zeitsynchronisation.
```

SSH

SSH steht für:

```
Secure Shell
```

SSH dient sicherer Fernadministration über eine Kommandozeile.

Typischer Port:

```
TCP 22
```

SSH wird häufig genutzt für:

```
- Linux-Server
- Netzwerkgeräte
- Firewalls
- NAS-Systeme
- SFTP
- Automatisierung
```

Merksatz:

```
SSH = sicherer Fernzugriff auf die Shell.
```

RDP

RDP steht für:

```
Remote Desktop Protocol
```

RDP dient grafischem Fernzugriff.

Typischer Port:

```
TCP 3389
```

RDP ist besonders bei Windows-Systemen verbreitet.

Wichtig:

```
RDP sollte nicht ungeschützt direkt aus dem Internet erreichbar sein.
```

Merksatz:

```
RDP = grafischer Fernzugriff.
```

Telnet

Telnet ist ein älteres Fernzugriffsprotokoll.

Typischer Port:

```
TCP 23
```

Problem:

```
Telnet ist unverschlüsselt.
```

Benutzername, Passwort und Befehle können im Klartext übertragen werden.

Merksatz:

```
Telnet vermeiden.
SSH verwenden.
```

Authentifizierung

Authentifizierung bedeutet:

```
Identität prüfen.
```

Frage:

```
Wer bist du?
```

Beispiele:

```
- Benutzername und Passwort
- SSH-Schlüssel
- Zertifikat
- Smartcard
- MFA-Code
- Token
```

Merksatz:

```
Authentifizierung = Identität prüfen.
```

Autorisierung

Autorisierung bedeutet:

> Rechte prüfen.

Frage:

> Was darfst du?

Beispiele:

> - Datei lesen
> - Datei ändern
> - Adminbereich öffnen
> - API verwenden
> - Benutzer anlegen
> - Server verwalten

Merksatz:

> Autorisierung = Rechte prüfen.

Authentifizierung und Autorisierung unterscheiden

Begriff	Frage	Beispiel
Authentifizierung	Wer bist du?	Benutzer meldet sich an
Autorisierung	Was darfst du?	Benutzer darf bestimmten Ordner öffnen

Merksatz:

> Angemeldet bedeutet nicht automatisch berechtigt.

MFA

MFA steht für:

```
Multi-Faktor-Authentifizierung
```

Dabei werden mehrere Faktoren kombiniert.

Beispiele:

```
- Passwort
- Smartphone-App
- Hardware-Token
- Fingerabdruck
- Smartcard
```

Merksatz:

```
MFA schützt zusätzlich,
wenn ein Passwort gestohlen wurde.
```

SSO

SSO steht für:

```
Single Sign-on
```

SSO bedeutet:

```
Einmal anmelden,
mehrere Dienste nutzen.
```

Typische Bestandteile:

```
- Identity Provider
- Service Provider
- Token
- zentrale Identität
```

Merksatz:

SSO = einmal anmelden,
mehrere Dienste nutzen.

Token und Session

Token:

digitaler Zugriffsnachweis

Session:

Sitzung zwischen Client und Anwendung

Session-Cookie:

Cookie zur Zuordnung einer Sitzung

Wichtig:

Tokens und Session-Cookies müssen geschützt werden,
weil sie Zugriff ermöglichen können.

Merksatz:

Token und Session-Cookie wie Zugangsdaten schützen.

Least Privilege

Least Privilege bedeutet:

Benutzer und Dienste erhalten nur die Rechte,
die sie wirklich benötigen.

Beispiel:

Dienst braucht nur Leserechte.
Dann bekommt er keine Schreibrechte.

Merksatz:

Nur so viele Rechte wie nötig,
so wenige wie möglich.

Typische Schicht-7-Fehler

Typische Fehler auf Schicht 7 sind:

- DNS löst falsch auf
- HTTP 404
- HTTP 500
- HTTP 502
- Login funktioniert nicht
- Zugriff verweigert
- API lehnt Anfrage ab
- falscher Content-Type
- ungültiges JSON
- Mail kommt nicht an
- Mail landet im Spam
- SMB-Freigabe verweigert Zugriff
- LDAP-Bind schlägt fehl
- SNMP-Werte fehlen
- NTP synchronisiert nicht
- SSH Permission Denied
- RDP-Anmeldung abgelehnt

Merksatz:

Schicht-7-Fehler betreffen Dienst,
Inhalt,
Anmeldung
oder Rechte.

Fehlersuche auf Schicht 7

Eine sinnvolle Reihenfolge:

1. Fehlermeldung genau lesen.
2. Betroffene Benutzer und Systeme eingrenzen.
3. Dienst und Protokoll bestimmen.
4. DNS und Hostname prüfen.
5. IP-Erreichbarkeit prüfen.
6. Port prüfen.
7. TLS oder Zertifikat prüfen.
8. Dienststatus prüfen.
9. Anmeldung prüfen.
10. Berechtigung prüfen.
11. Datenformat prüfen.
12. Logs prüfen.
13. letzte Änderungen prüfen.

Merksatz:

Erst eingrenzen,
dann Schicht für Schicht prüfen.

Wichtigste Abgrenzung zu unteren Schichten

Aussage	Einordnung
Kabel steckt nicht	Schicht 1
VLAN falsch	Schicht 2
Gateway falsch	Schicht 3
Port blockiert	Schicht 4
TLS-Zertifikat ungültig	Schicht 6
HTTP 404	Schicht 7
Login falsch	Schicht 7
Rechte fehlen	Schicht 7
DNS-Record falsch	Schicht 7

Merksatz:

Schicht 7 beginnt dort,
wo der konkrete Dienstinhalt geprüft wird.

Typische Prüfungsfallen

Schicht 7 heißt Anwendungsschicht.

Schicht 7 ist nicht einfach das Programm selbst.

Anwendungen nutzen Schicht-7-Protokolle.

Port gehört zu Schicht 4.

Dienstprotokoll gehört zu Schicht 7.

DNS gehört zu Schicht 7.

DHCP gehört zu Schicht 7,
obwohl es IP-Konfiguration verteilt.

HTTP gehört zu Schicht 7.

HTTPS ist HTTP über TLS.

SMTP sendet E-Mails.

POP3 und IMAP empfangen E-Mails.

POP3 lädt eher herunter.

IMAP synchronisiert besser.

FTP ist klassisch unverschlüsselt.

SFTP ist nicht FTPS.

SMB nutzt TCP 445.

LDAP ist nicht das ganze Active Directory.

SNMPv3 ist sicherer als SNMPv1/v2c.

NTP-Probleme können Zertifikats- und Loginprobleme verursachen.

SSH ist sicherer als Telnet.

RDP nicht ungeschützt ins Internet öffnen.

Authentifizierung ist nicht Autorisierung.

Anmeldung bedeutet nicht automatisch Berechtigung.

Offener Port bedeutet nicht automatisch,
dass die Anwendung funktioniert.

Wichtige Begriffe kurz erklärt

Begriff	Kurze Erklärung
Anwendungsschicht	OSI-Schicht 7
Dienst	Netzwerkfunktion für Anwendungen
Protokoll	Regelwerk für Kommunikation
HTTP	Webprotokoll
HTTPS	HTTP über TLS
DNS	Namensauflösung
DHCP	automatische IP-Konfiguration
SMTP	E-Mail senden
POP3	E-Mail abrufen
IMAP	E-Mail abrufen und verwalten
FTP	klassische Dateiübertragung
SFTP	Dateiübertragung über SSH
FTPS	FTP mit TLS
SMB	Datei- und Druckerfreigaben
LDAP	Verzeichnisdienstzugriff
SNMP	Netzwerkmanagement

Begriff	Kurze Erklärung
NTP	Zeitsynchronisation
SSH	sicherer Shell-Zugriff
RDP	grafischer Fernzugriff
Telnet	altes unverschlüsseltes Fernzugriffsprotokoll
API	Schnittstelle zwischen Anwendungen
Authentifizierung	Identität prüfen
Autorisierung	Rechte prüfen
MFA	Multi-Faktor-Authentifizierung
SSO	Single Sign-on
Token	digitaler Zugriffsnachweis
Session	Sitzung zwischen Client und Anwendung
Least Privilege	nur notwendige Rechte vergeben

IHK-sichere Gesamtformulierung

Die Anwendungsschicht ist Schicht 7 des OSI-Modells. Sie stellt Netzwerkdienste für Anwendungen bereit. Typische Protokolle sind HTTP, HTTPS, DNS, DHCP, SMTP, POP3, IMAP, FTP, SFTP, FTPS, SMB, LDAP, SNMP, NTP, SSH, RDP und Telnet. Die Anwendungsschicht ist nicht das Programm selbst, sondern beschreibt die Protokolle und Dienste, die Anwendungen zur Kommunikation verwenden. Ports gehören zur Transportschicht, während die eigentlichen Dienstprotokolle zur Anwendungsschicht gehören. Fehler auf Schicht 7 betreffen häufig DNS, HTTP-Statuscodes, Anmeldungen, Berechtigungen, APIs, Datenformate, Maildienste, Dateifreigaben oder Dienstlogs.

Wichtigste Merksätze

```
Schicht 7 = Anwendungsschicht.

Schicht 7 = Netzwerkdienste für Anwendungen.

Anwendung nutzt Protokoll.

Protokoll gehört zu Schicht 7.

Port gehört zu Schicht 4.

HTTP = Webprotokoll.
```

HTTPS = HTTP über TLS.

DNS = Name zu IP-Adresse.

DHCP = automatische IP-Konfiguration.

SMTP sendet.

POP3 ruft ab.

IMAP synchronisiert.

FTP ist klassisch unverschlüsselt.

SFTP läuft über SSH.

FTPS nutzt TLS.

SMB = Datei- und Druckerfreigaben.

LDAP = Verzeichnisdienstzugriff.

SNMP = Netzwerküberwachung.

NTP = Zeitsynchronisation.

SSH = sicherer Fernzugriff.

RDP = grafischer Fernzugriff.

Telnet ist unsicher.

Authentifizierung = Wer bist du?

Autorisierung = Was darfst du?

Anmeldung ist nicht gleich Berechtigung.

MFA erhöht die Sicherheit.

Least Privilege immer beachten.

Offener Port heißt nicht:
Anwendung funktioniert.

Schicht-7-Fehler mit Dienst,
Protokoll,
Anmeldung,
Rechten,
Daten
und Logs prüfen.