M127 – Server betreiben

1 Serverarten

1.1 Dateiserver

Sobald der Server für andere Benutzer im Netzwerk Dateien in freigegebenen Ordnern bereitstellt, fungiert er als Dateiserver. Zu konfigurieren sind dazu Freigaben mit den entsprechenden Sicherheitseinstellungen für die Benutzer und Gruppen.

1.2 Druckserver

Die am häufigsten genutzten Dienste eines Servers sind die zur zentralen Bereitstellung und Verwaltung von Druckern. Dieser Dienst ist mit W2k3 Server noch einfacher geworden

1.3 Anwendungsserver

Über die Anwendungsdienste können Server miteinander kommunizieren beziehungsweise spezielle Funktionen als Clients bereitstellen. Sie sind beim W2k3 Server in den Internet Information Services (IIS) verankert.
Für einen normalen Serverbetrieb im Netzwerk, bei dem die zentrale Verwaltung der Benutzerkonten und Ressource (Daten, Drucker, etc.) im Vordergrund steht, sind diese Anwendungsdienste nicht relevant.

1.4 Mailserver

Mit W2k3 Server kann man einen einfachen, aber voll funktionsfähigen Mailserver betreiben.

1.5 Terminalserver

Über den Terminalserver werden Clients virtuelle Windows-Computer zur Verfügung gestellt. Alle Anwendungen und Systemeinstellungen werden am Terminalserver vorgenommen. Die Benutzer greifen auf diese dann über eine spezifische Clientsoftware zu. Bei einem leistungsfähigen Terminalrechner mit einer schnellen Netzwerkanbindung sind Performance-Unterschiede zu einem lokal arbeitenden Windows kaum noch auszumachen.

1.6 RAS/VPN Server

Ein RAS/VPN-Server fungiert heute oft nicht nur im lokalen Netzwerk, sondern soll aus verschiedenen Gründen über eine direkte Datenfernverbindung oder mit Hilfe des Internets als Transortmedium erreichbar sein. Die Remote Access Services (RAS) stellen dazu die benötigten Funktionen bereit.

1.7 Domänencontroller

Die Domänencontroller verwalten die Verzeichnisdatenbank der Domäne, in der unter anderem alle Benutzer, Sicherheitsgruppen und Computer erfasst sind (→ Active Directory)

1.8 DNS-Server

Das Domain Name System (DNS) dient der Namensauflösung im Internet oder im LAN.
Bei Active Directory wird DNS vorausgesetzt.
IP-Adresse ←→ Namen

1.9 DHCP-Server

Mithilfe des Dynamic Host Configuration Protocol (DHCO`P) werden IP-Adressen an Clientcomputer automatisch durch einen zentralen DHCP-Server verteilt.

1.10 Streaming-Media-Server

Grundlegende Funktionen für die zentrale Bereitstellung von multimedialen Inhalten im Netzwerk.

1.11 WINS-Server

WINS (Windows Internet Name Service) wurde ursprünglich für die Namensauflösung in Windows-Netzwerken entwickelt. Übernimmt eine ähnliche Rolle wie der DNS-Server.

2 Dateiserver-Funktionen

(siehe Aufgaben)

3 Kommandointerpreter

(siehe Aufgaben)

4 Massenspeicherverwaltung

(siehe Aufgaben)

4.1 Convert-Befehl

Bei W2k3-Server kann man mi diesem Befehl FAT- und FAT32-Dateisysteme nach NTFS umwandeln.

4.2 Dynamic Volumes – Dynamische Datenträger

4.2.1 Mirrored: gespiegelt

Daten auf einem Datenträger werden parallel auf einen andren Datenträger gespiegelt. Die Daten sind doppelt vorhanden. Beim Ausfall einer HD sind die Daten immer noch verlustfrei verfügbar.

4.2.2 Striped

Mehrere Festplatten werden zu „einer“ zusammengeschlossen, was den Datendurchsatz pro integrierter Festplatte erhöht.

4.3 Festplatte, Volume und Datenträger
Mit Festplatte und Datenträger werden physische Festplatten bezeichnet.
Der Begriff „Volume“ wird hingegen für logische Einheiten auf den Festplatten benutzt.

4.4 Boot.ini
In der Datei „Boot.ini“ sind die Starteinträge für installierte Betriebssysteme hinterlegt, die im Startmenü zur Auswahl angeboten werden können.

4.5 Unterschied zwischen einem Basisdatenträger und einem dynamischen Datenträger?
Basisdatenträger werden durch die Komponente „ftdisk (Fault Tolerance Disk Driver)“ angesteuert. Diese Kompabilitätsfunktion wurde bei Windows Server 2003 gekappt, um den Umstieg auf die dynamische Danteträgerverwaltung zu erzwingen. Mit der dynamischen Datenträgerverwaltung kann die Grösse des Speichervolumens ohne neue Gesamtformatierung angepasst werden.

4.6 Volumenschattenkopie
Bei einer Volumenschattenkopie können generell auf alle Dateien, die auf dem Volume gespeichert sind, zugegriffen werden. Dies wird erreicht, indem die Dateien gesichert und alle Versionen archiviert werden.

4.7 EFS-Verschlüsselung
EFS - Verschlüsselung bedeutet Encrypting File System und bildet ein verschlüsseltes Dateisystem. Die Handhabung ist dabei für den Benutzer sehr einfach. Durch eine solche Verschlüsselung können die Daten auf der Festplatte bei einem Diebstahl nicht mehr gelesen werden.

4.8 verteiltes Dateisystem (DFS)
Das verteilte Dateisystem (DFS) ist ein spezieller Serverdienst, mit dem Daten auf unterschiedlichen Servern zu einem einheitlichen Namen zusammengefasst werden können.

4.9 Remotespeicher
Ein Remotespeicher ermöglicht die Verwendung von Bandspeichermedien als Erweiterungen von NTFS-Datenträgern.

4.10 Defragmentierung
Durch Defragmentierung erfolgt eine Umformung des Speichers, wobei alle belegten Speicherinhalte dicht ans Ende des Speichers verschoben werden. Damit werden am Anfang des Speichers wieder viele Speicherstellen frei.
So kann die Laufwerkszugriffszeit verringert werden, womit sich eine Performancesteigerung ergibt.

4.11 MBR (Master Boot Record)
MBR (Master Boot Record) ist ein logischer Sektor eines bootsfähigen Mediums wie z.B. Festplatte oder Diskette. Der Bootssektor beinhaltet die Bootdateien bzw. die Verzeichnisse zu den Bootfiles, er ist somit nichts anderes als ein ausführbares Programm bzw. der Verweis auf eins solches.

4.12 RAID-Level
- RAID 0: Striping: Mehrere Festplatten werden zu „einer“zusammengeschlossen, was den Datendurchsatz pro integrierter Festplatte faktorisiert
- RAID 1: Mirroring: Die Daten werden von der einen Festplatte auf die andere gespiegelt. Sollte eine dieser beiden Festplatten ausfallen, sind die Daten weiterhin verlustfrei verfügbar.
- RAID 5: Bei der Version „Performance + Parität“ werden die Daten sowohl gespiegelt, als auch über mehrere Fesplatten verteilt. Beim Ausfall einer der beteiligten Festplatten sind die Daten weiterhin verfügbar. Es müssen mindestens drei Festplatten zusammengeschlossen werden.

5 Releases, Upgrades und Updates
(siehe Aufgaben)

5.1 Upgrade
Wenn z.B. ein neues Betriebssystem auf den Mark kommt, so kann, sofern der Vorgänger bereits installiert ist, ein Upgrade auf das neue gemacht werden. Ein Upgrade bedeutet also, dass ein altes Produkt auf den Stand eines neuen gebracht wird. Beispiel eines Upgrades ist, wenn ein bestehendes Windows XP auf Windows Vista upgegraded wird

5.2 Update
Ein Update ist eine neue Subversion, meist um Programmfehler zu beheben und kleinere Erweiterungen einzuführen. Z.B. von Windows XP 1.0.0.2 auf Windows XP 1.0.0.3.! Beispiel ist, wenn eine Virensoftware fast täglich ein Update mit den neusten Viren erhält, welche in Umlauf gekommen sind, damit es einen optimalen Schutz bietet.

5.3 Release

Ein Betriebssystemrelease bedeutet, dass ein neues Betriebssystem erschienen
ist. Es gibt auch sogenannte Releasecandidats. Dies sind Betaversionen im Endstadium,
die zum offiziellen Betriebssystem werden. Ein Release ist also keine Erweiterung
(Update), sondern ein komplettes System.

5.4 Warum ist eine Registrierung des verwendeten Betriebssystems von Vorteil?

Dadurch enthält man (laut Verpackung) Support und die neusten Updates und Sicherheitspatches.

5.5 Was ergibt sich, wenn man Windows Server 2003 aktiviert?

Man erhält die neusten Updates und Sicherheitspatches. Dadurch wird das System auf dem Laufenden gehalten.

5.6 Betriebssystem-Dokumentation

- **Installierte Software:** Systemsteuerung → SW
- **Benutzerkonten:** Systemsteuerung → Benutzerkonten
- **HW:** Verwalten → Gerätemanager
- **Belegter und freier Speicher auf HD und RAM:** Partitionseigenschaften
- **RAM-Auslastung:** Taskmanager
- **NW-Einstellungen:** ipconfig
- **Vorhandene Fehler:** Computerverwaltung → Ereignisanzeige (eventlog)

Eine BS-Dokumentation muss immer aktuell sein, damit bei einem Ausfall die letzte, lauffähige Version immer bekannt ist und damit wieder hergestellt werden kann.
Eine Betriebssystemdokumentation muss die eingesetzten Werkzeuge und definierten User, deren Konfiguration, Adressen und Rechte genau definieren.

5.7 Microsoft-Update

Updates werden je nach Einstellung automatisch installiert. Ansonsten können unter http://update.microsoft.com/microsoftupdate/v6/default.aspx?ln=de die neusten Updates bezogen werden. Diese Updates sollte man regelmässig durchführen, da sie das Betriebssystem verbessern und auch Gratis von Microsoft zur Verfügung gestellt werden.

5.8 Automatische Updates

Start → Einstellungen → Systemsteuerung → „Automatische Updates“.

5.9 Was tun, wenn PC nach Update etc nicht mehr bootet?

Wenn der PC nicht starten, würde ich zuerst versuche, im abgesicherten Modus zu starten. Danach nach „Systemsteuerung / Software“ wechseln und „Update“ aktivieren. Nun das letzte Update anklicken und auf „Deinstallieren“ klicken. Nun einen Neustart machen und hoffen, dass es wieder funktioniert.

5.10 Fehlerberichterstattung an Microsoft

Microsoft will die Fehler erkennen können und Updates bereitstellen, damit dieser Fehler nicht mehr auftritt. Mit „Fehlerbericht senden“ wird ein Bericht über den Fehler, wo er wann und wieso aufgetreten ist, und viele Informationen über den Computer, damit Microsoft den Fehler rekonstruieren können. Support wird man aber leider nicht erhalten. Aus Ressourcengründen ist dies gar nicht vertretbar. Fehler passieren zu tausendsten.

6 Systemausfälle und Gegenmassnahmen

(siehe Aufgaben)

7 Reparatur und Datenwiederherstellung

(siehe Aufgaben)

7.1 Hauptunterschied zwischen Abgesichertem Modus und Wiederherstellungskonsole:

Der abgesicherte Modus startet den Server mit einer Reihe von Standardtreibern, während die Wiederherstellungskonsole eine eigene Miniversion von Windows Server 2003 zum Start verwendet. Die Wiederherstellungskonsole unterstützt nur ein paar Kommandozeilenbefehle.

7.2 NTBackup

- **Normal:** Alle Dateien werden gesichert. Das Archivbit wird dabei zurückgesetzt und der Sicherungsstatus der Dateien wird nicht verwendet.
- **Kopieren:** Alle Dateien werden gesichert, das Archivbit jedoch nicht zurückgesetzt. Der Sicherungsstatus der Dateien bleibt also unberührt.
- **Differenz:** Es werden nur die Dateien gesichert, deren Archivbit gesetzt ist. Das

sind also jene Dateien, die seit der letzten normalen Sicherung geändert wurden
- **Inkrementell:** Hier werden ebenfalls nur die Dateien gesichert, deren Archivbit gesetzt ist. Doch wird hier dann das Archivbit zurückgesetzt.
- **Täglich:** Bei dieser Sicherungsart werd das Archivbit weder beachtet noch geändert. Es werden einfach alle Dateien gesichert.

7.3 Welche Sicherungstypen verändern das Archivbit nicht?

Die Sicherungstypen Kopieren-, Differenz- und tägliche Sicherungen ändern das Archivbit nicht.

Administratoren-Gruppe und Sicherungsoperatoren erhalten automatisch Sicherungs- und Wiederherstellungsrechte.

7.4 ASR (Automated System Recovery)

Die automatische Systemwiederherstellung erfordert:
- Windows Server 2003-CD-Rom
- Diskette und
- Sicherungsmedium, das bei der ASR-Sicherung erzeugt wurde.

Mit ASR kann man das System auf einen zuletzt hoffentlich noch funktionsfähigen Stand zurückführen.

7.5 Wiederherstellungskonsole

Mit der Wiederherstellungskonsole können grundlegende Reparaturarbeiten durchgeführt werden. Die Anzeige bleibt dabei auf den Textmodus beschränkt und die grafischen Dienstprogramme sind damit für die Anwendung gesperrt.
Die Wiederherstellungskonsole lässt sich auch von der Windows-Server-2003- CD starten!

7.6 Generationsprinzip bei Datensicherung

Es werden mehrere Medien eingesetzt, auf die jeweils zu einem bestimmten Zeitpunkt alle Dateien gesichert werden. Ziel ist es, im Notfall auf einen Datenbestand in der Vergangenheit zurückgreifen zu können.

7.7 F8-Menü (erw. Startoptionen)

Dieses Menü erscheint, wenn Sie unmittelbar bei Beginn des Systemstarts oder im Startmenü die F8-Taste betätigen. Sie erhalten dann verschiedene Optionen zur Auswahl, die u.a. besondere Startmodi für die Fehlerbehebung bieten.

8 Geräte und Dienste

(siehe Aufgaben)

9 Client-Systeme

(siehe Aufgaben)

10 Routing und RAS-Funktionen

(siehe Aufgaben)

11 Server-Hardware

(siehe Aufgaben)

12 Theorie-Fragen

12.1 Rückblicksübungen

Kernel-Modus ist ein mit umfassenden Rechten ausgestatteter Betriebsmodus. Jede Komponente und jeder Dienst, der im Kernel-Modus ausgeführt wird. kann auf die HW sowie den gesamten Speicher zugreifen.

Benutzermodus
Anwendungsprogramme und gemeinsame Komponenten werden im Benutzermodus ausgeführt. In diesem Modus haben die Programme eingeschränkte Rechte, lediglich Zugriff auf den eigenen Programmspeicher, nicht jedoch auf den Speicher des Kernel-Modus und den zugehörigen Code.

CLR = Common Language Runtime (Laufzeitumgebung)
Verwaltung und Ausführung von Code….
CTS = Common Type System
Einheitliche Datentypen
→ Sprach- und Plattformunabhängigkeit

Was bedeutet LDM und für was dient diese?
LDM (Logical Disk Manager) stellt die Verwaltungsschnittstelle für dynamische Datenträger bereit. LDM enthält eine Datenträgerverwaltungsdatenbank.

Sind Volumenschattenkopien ein Ersatz für die Datensicherung?
Ähnlich einer nach dem Generationsprinzip durchgeführten Datensicherung kann über Volumenschattenkopien ebenfalls auf ältere Dateiversionen zurückgegriffen werden. Ein Ersatz für eine Dateisicherung ist dies jedoch nicht. Diese sollte auf jeden Fall zusätzlich vorgenommen werden.

Dateisystemfehler und fehlerhafte Sektoren auf der Festplatte des Computers wiederherstellen.
→ Chkdsk (Datenüberprüfung)

Systemaktualisierung
1. Updates suchen (Microsoft Update)
2. Updates überprüfen und installieren

SUS-Komponente
Microsoft *Software Update Services* (SUS) sind kostenlose Tools, die die Windows-Update Funktionalität im Unternehmen verfügbar machen – allerdings nur für die Betriebssysteme Windows 2000, XP, Server 2003. Dabei werden die Updates und Patches auf einen internen Update-Server heruntergeladen, getestet und freigegeben. Die Clients wiederum installieren die Updates vom internen SUS-Server.

Lizenzmodi bei W2k3-Server
- ✓ pro Server
- ✓ pro Gerät oder pro Benutzer

Sicherheitsfeatures
1. **Core Security:**
   Sicherheitsmerkmale von AD (Zugriffsberechtigungen wie Kerberos, Smartcards, Public-Key-Infrastruktur)
2. **Network Security**
   Netzwerkprotokolle IPSec, VPN, Erweiterungen von WLAN und weitere Massnahmen zur Verbesserung der Sicherheit der NW-Kommunikation
3. **Computing Device Security**
   Massnahmen zur Sicherung der Server, Clients und Notebooks sowie EFS.
4. **Application Security**
   Schutz vor Viren und Trojanern….

Öffentlicher und privater Schlüssel (Sicherheit)
Die Funktionsweise einer PKI basiert auf der Verwendung eines Schlüsselpaares. Informationen werden unter Verwendung eines Schlüssels verschlüsselt und können dann nur mithilfe des anderen Schlüssels entschlüsselt werden.
➔ RSA
Einsatzgebiete: Verschlüsselung und Signatur

Arten von Angriffen auf Kennwörter
1. **Mangelnde Sorgfalt der Anwender** (Bsp. Passwort am Bildschirm angeklebt etc)
2. **Social Engineering:** Angreifer täuscht vor, er sei Administrator
3. **NetzwerkSniffer:** Protokollierung von Datenpaketen in schlecht gesicherten NWs
4. T**rojaner**

Arten von Angriffen auf Daten

1. Versehentliche Zuweisung von umfangreichen Berechtigungen
2. Mitlesen von Datenübertragungen durch NW-Sniffer

Unterschied HW und SW-Firewall

HW-Firewalls (sog. Appliances) haben den Vorteil, sehr schnell zu sein, denn sie sind nicht mit dem Overhead eines BS belastet. Allerdings sind sie weniger gut in die Benutzerverwaltung des AD integriert.
SW-Firewalls können den Zugriff aif Basis von AD-Benutzer und Gruppen regeln.

MessageBlock

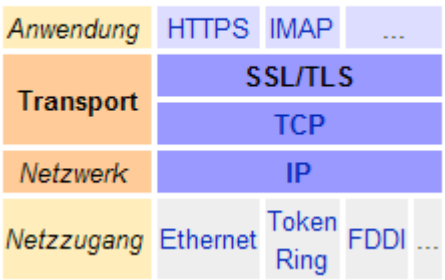
Das Server MessageBlock-Protokoll (SMB) dient der Kommunikation zwischen Windows-Dateiserver und –Client, die als SERVER bzw. ARBEITSSTATIONSDIENST implementiert sind. Alle netzwerkfähigen Windows-Versionen enthalten SMB-Protokoll.

IPSec besteht aus den beiden Protokollen AH (Authentificated Header) und ESP (Encapsulating Securtiy Payload).

SSL

Transport Layer Security (TLS) oder Secure Sockets Layer (SSL) ist ein hybrides Verschlüsselungsprotokoll für Datenübertragungen im Internet. TLS 1.0, 1.1 und 1.2 sind die standardisierten Weiterentwicklungen von SSL 3.0 (TLS 1.0 steht neu für SSL 3.1). SSL wird also nun unter dem Namen TLS weiterentwickelt. Hier wird die Abkürzung SSL für beide Bezeichnungen verwendet.

SSL im TCP/IP-Protokollstapel



NetBIOS ist eine Schnittstelle zum Auffinden von Rechnern und deren Dienste. NetBIOS arbeitet mit 16-Byte langen Rechnernamen, wovon 15-Byte frei wählbar sind und das 16.Byte den Dienste bezeichnet, den ein Rechner anbietet.

EMS (Emergency Management System) erlaubt eine Out-of-Band-Verbindung zum Server über den seriellen Port, wenn ein Server nicht mehr übers NW erreicht wird.

12.2 Prüfungen

Mit welchem Befehl kann man de Freigabe von „Test$“ unter dem Server „SRV01“ auf dem Laufwerk „X“ mappen?

net use X: \\SRV01\Test$

Was braucht es für Anforderungen, um einen Server zu betreiben?

- hohe Ausfallsicherheit
- Datensicherung (Backup)
- Benutzerverwaltung → Berechtigungen
- Serverbetriebssystem, z.B. W2k3-Server (erlaubt mehr Connections als ein gewöhnliches OS)
- Firewall (Schutz vor Viren, Trojaner, Rootkits

Unterschied zwischen der Hardware eines normalen PC’s und eines wichtigen Betriebs-Servers:

- höhere Ausfallsicherheit: gespiegelte Festplatten
- mehr Speicher, RAM, CPU Taktfrequenz, da der Server eine höhere Leistung erbringen muss
- Backup auf Bandspeichermedium

Was tun wenn sich ein Server nicht mehr hochfahren lässt:

1. Problemanalyse, wieso geht nichts mehr?
2. evtl. abgesicherter Modus, Systemwiederherstellung
3. evtl. defekt HW auswechseln

Nachteile, wenn man die Ressourcen für Hardwaregeräte manuell konfiguriert:

Wenn man an der HW des Os „herumspielt“, kann es irgendwann mal vorkommen, dass ein Bluescreen erscheint und der PC nicht mehr korrekt bootet.

Dann muss man das System wiederherstellen.., was unter Umständen Zeit in Anspruch nimmt. Ausserdem verschwinden die „Plug and Play“-Vorteile

Probleme mit Hardware und Treibern kann man im Gerätemanager gut erkennen und behandeln.