iSCSI (Internet Small Computer System Interface)

iSCSI je síťový protokol pro přenos dat na úrovni bloků (block-level), který zapouzdřuje příkazy protokolu SCSI do paketů TCP/IP. To umožňuje serverům přistupovat k úložným zařízením přes standardní ethernetovou síťovou infrastrukturu (kabely, switche, routery).

Z pohledu operačního systému se disk připojený přes iSCSI jeví jako lokálně připojený pevný disk, přestože se fyzicky nachází na vzdáleném úložném serveru.

Základní komponenty iSCSI

Architektura iSCSI využívá model klient-server, ale s jinou terminologií:

1. iSCSI Initiator (Klient)

Software nebo hardware na straně serveru, který „iniciuje“ spojení. Initiator posílá SCSI příkazy přes síť.

- **Software Initiator:** Běžný program v OS (součást Windows, Linuxu i macOS). Využívá výkon CPU serveru.
- **Hardware Initiator:** Specializovaná karta HBA, která odlehčuje procesoru (TCP Offload).

2. iSCSI Target (Server/Úložiště)

Cílové zařízení, které poskytuje úložný prostor. Může to být:

- Dedikované diskové pole (SAN).
- Běžný server se softwarem (např. Linux s balíčkem `targetcli` nebo TrueNAS).
- NAS zařízení s podporou iSCSI (Synology, QNAP).

Identifikace a adresace (IQN)

Protože iSCSI běží v síti, potřebuje unikátní jména pro identifikaci zařízení. Nejčastějším formátem je **IQN** (iSCSI Qualified Name).

Příklad formátu IQN:

```
''iqn.2026-01.com.priklad:uloziste.disk01''
* **iqn:** Konstanta.
* **2026-01:** Datum registrace domény.
* **com.priklad:** Obrácená doména vlastníka.
```

```
* **uloziste.disk01:** Volitelný název konkrétního cíle.
```

Výhody a nevýhody

Výhody	Nevýhody
Nízké náklady: Využívá stávající ethernetové switche a kabely.	**Zátěž sítě:** Může zpomalit běžný síťový provoz (proto se doporučuje oddělená VLAN).
Dosah: Data lze přenášet na velké vzdálenosti přes IP sítě.	**Režie (Overhead):** Zapouzdření do TCP/IP přidává malou latenci oproti Fibre Channel.
Snadná správa: Administrátoři nemusí znát FC technologie, stačí znalost TCP/IP.	**Závislost na CPU:** Software iniciátory zatěžují procesor serveru.

Zabezpečení v iSCSI

Jelikož data tečou po běžné síti, je zabezpečení kritické:

- **CHAP (Challenge Handshake Authentication Protocol):** Ověřování jménem a heslem mezi iniciátorem a cílem.
- **ACL (Access Control Lists):** Target dovolí připojení pouze konkrétním IQN jménům.
- **VLAN / Izolace:** iSCSI provoz by měl běžet ve vlastní fyzické nebo virtuální síti, oddělené od internetu a uživatelů.

Praktické využití

- **Virtualizace:** Propojení hypervisorů (VMware, Proxmox) se sdíleným úložištěm pro umožnění **Live Migration** (přesun běžícího VM mezi servery).
- **Clustery:** SQL servery nebo souborové servery v clusteru potřebují přístup ke stejnému disku (LUN).
- **Zálohování:** Připojení vzdálených páskových knihoven.

— **Související termíny:** SAN, SCSI, LUN, HBA, NAS, Multipathing.