

Disaster Recovery (DR)

Disaster Recovery (Obnova po havárii) je soubor politik, nástrojů a postupů, které umožňují obnovu nebo pokračování vitální technologické infrastruktury a systémů po přírodní nebo člověkem způsobené katastrofě. Zatímco vysoká dostupnost (HA) se zaměřuje na předcházení výpadkům, DR se zaměřuje na to, jak se vrátit do provozu, když už k výpadku došlo.

Základem DR je existence sekundární lokality (DR Site), která je geograficky oddělená od hlavní lokality.

Klíčové metriky DR: RPO a RTO

Úspěšnost strategie Disaster Recovery se měří dvěma parametry, které určují, kolik dat a času si firma může dovolit ztratit.

- **RPO (Recovery Point Objective):** Maximální přípustné stáří dat, která mohou být ztracena. Pokud zálohujete jednou za 24 hodin, vaše RPO je 24 hodin.
- **RTO (Recovery Time Objective):** Maximální přípustný čas, za který musí být služby po havárii opět funkční. Pokud obnovení trvá 4 hodiny, vaše RTO je 4 hodiny.

Typy Disaster Recovery lokalit

Podle toho, jak rychle je záložní lokalita schopna převzít provoz, rozlišujeme:

- **Cold Site (Studená):** Záložní prostor s infrastrukturou (elektřina, chlazení), ale bez nainstalovaného hardwaru a dat. Obnova trvá dny až týdny. (Nejlevnější)
- **Warm Site (Teplá):** Hardware je připraven a nakonfigurován, ale data nejsou aktuální (obnovují se např. jednou denně ze záloh). Obnova trvá hodiny.
- **Hot Site (Horká):** Plně funkční kopie produkčního prostředí. Data jsou synchronizována v reálném čase. Přejechod je téměř okamžitý. (Nejdražší)

Strategie přenosu dat

Aby bylo možné v záložní lokalitě začít pracovat, musí tam být data. Toho se docílí pomocí:

1. ****Zálohování (Backup):**** Pravidelné kopírování dat na pásky, disky nebo do cloudu.
2. ****Replikace:**** Kontinuální kopírování dat mezi úložnými systémy ([[san|SAN]]).
 - * ****Synchronní:**** Každý zápis musí být potvrzen v obou lokalitách (nulové RPO, ale vyžaduje extrémně rychlé spojení a malou vzdálenost).
 - * ****Asynchronní:**** Data se posílají s mírným zpožděním (vhodné pro velké vzdálenosti).
3. ****Cloud DR (DRaaS):**** Využití cloudového poskytovatele jako záložní

lokality, což eliminuje potřebu vlastnit druhý fyzický serverový sál.

DR Plán (DRP - Disaster Recovery Plan)

DR není jen o technologiích, ale především o procesech. Kvalitní plán musí obsahovat:

- **Analýzu dopadů (BIA):** Které systémy jsou nejdůležitější?
- **Krizové kontakty:** Kdo má pravomoc spustit DR proces?
- **Postupy krok za krokem:** Jak nastartovat servery v záložní lokalitě v určitém pořadí (např. nejdřív databáze, pak aplikace).
- **Pravidelné testování:** Neotestovaný DR plán je neexistující plán.

Moderní trendy v DR

- **Immutable Backups:** Zálohy, které nelze změnit ani smazat (ochrana proti Ransomware).
- **Orchestrace:** Nástroje (např. VMware SRM nebo Veeam), které automaticky provedou stovky kroků k oživení datacentra po stisknutí jediného tlačítka.

— **Související termíny:** [Failover](#), [High Availability](#), [Zálohování](#), [IaaS](#), [iSCSI](#).

From:

<https://www.serviceit.cz/> - IT ENCYKLOPEDIE

Permanent link:

https://www.serviceit.cz/doku.php?id=disaster_recovery

Last update: **2026/01/03 18:11**

