Průřezové služby Objednatele

Specifikace průřezových služeb poskytovaných Objednatelem

Příloha č. 3

Table of Contents

[Průřezové služby infrastruktury Objednatele 3](#_Toc158972357)

[1. IDM 3](#_Toc158972358)

[2. DNS 3](#_Toc158972359)

[3. NFS 3](#_Toc158972360)

[4. DHCP 3](#_Toc158972361)

[5. Mailové služby 3](#_Toc158972362)

[6. VPN 3](#_Toc158972363)

[7. LoadBalancing 4](#_Toc158972364)

[8. Firewall 4](#_Toc158972365)

[9. Proxy 4](#_Toc158972367)

[Architektonické principy 4](#_Toc158972368)

[10. Škálovatelnost 5](#_Toc158972369)

[11. Standardizace procesů rozvoje a podpory 5](#_Toc158972371)

[12. Náklady na vlastnictví a provoz 5](#_Toc158972373)

[13. Základní rysy architektury 6](#_Toc158972374)

[Dostupnost 6](#_Toc158972375)

[Zálohování a obnova 6](#_Toc158972376)

[Preferované architektonické patterny 6](#_Toc158972377)

[Samostatný virtuální server 6](#_Toc158972378)

[Předpoklady 6](#_Toc158972379)

[Popis architektury 6](#_Toc158972380)

[Vysoká dostupnost mezi datovými centry 7](#_Toc158972381)

[Předpoklady 7](#_Toc158972382)

[Popis STOR 8](#_Toc158972383)

[Fyzická vrstva 8](#_Toc158972384)

## Průřezové služby infrastruktury Objednatele

Tato kapitola popisuje průřezové služby infrastruktury, které poskytují technické nebo aplikační funkcionality, obvykle nezbytné pro definici architektury implementovaného řešení.

Služby jsou součástí služeb DC

### IDM

Služby IDM jsou poskytovány systémem IdM společnosti Autocont (AC identita). Další specifikace je obsažena v příloze č. 4 kapitole Autentizace.

### DNS

Služby DNS jsou poskytovány automaticky pro všechny rozsahy adres, přístupné z externích prostředí.

Pro interní komunikaci v rámci navrhovaného řešení je třeba zajistit nastavení na úrovni příslušného OS (hosts), případně nastavení DNS služby v rámci aplikace.

### NFS

Služby NFS nejsou centrálně poskytovány, případné sdílení filesystémů v rámci řešení je nutné řešit jako součást dodávané architektury aplikace prostředky příslušného OS nebo jako součást aplikace.

### DHCP

V rámci DC jsou poskytovány výhradně služby provozu serverových řešení, kterým jsou přidělovány pevné adresy z rozsahů definovaných Poskytovatelem infrastruktury. Služby dynamického přidělování adres tedy nejsou poskytovány.

Výjimkou jsou služby kontejnerizace, kde je adresa přidělena jako součást parametrů kontejneru při jeho spuštění.

### Mailové služby

Mailové služby jsou poskytovány ve formě SMTP serveru, výhradně pro odchozí mailovou komunikaci (notifikace).

### VPN

Služby VPN jsou poskytovány v rámci služeb DC Poskytovatele infrastruktury výhradně pro potřeby vzdálené administrace, zpravidla pro potřeby Dodavatele, a to jak pro fázi implementací, tak pro fázi provozní podpory.

Součástí služby je vytvoření specifické skupiny uživatelů Dodavatele, která zajišťuje oprávnění přístupu ke službám, jež jsou součástí služeb řešení. Skupina VPN klientů není vnitřně diverzifikovaná.

### LoadBalancing

LoadBalancing není v infrastruktuře poskytované Objednatelem poskytován. LoadBalancing na L7 dodá Dodavatel.

### Firewall

Zabezpečení je realizované pomocí firewallových pravidel. Veškerá síťová komunikace podléhá pravidlům pro komunikaci.

Aplikace, resp. řešení Dodavatele musí být navržena s ohledem na možnost monitorovat, resp. řídit komunikaci. Základním předpokladem je rozvrstvení aplikace do vrstev (segmentů), které mají společné vlastnosti, požadavky na infrastrukturu, monitoring nebo procesy podpory. Optimálně je pro návrh aplikace využito rozdělení na tyto vrstvy:

* databázová vrstva, která je zodpovědná za persistenci dat;
* aplikační vrstva, která je zodpovědná za procesní a funkční zpracování dat;
* vrstva uživatelského rozhraní, která je zodpovědná za poskytnutí uživatelského rozhraní;
* pro návrh řešení a síťového prostředí pak platí následující pravidla:
  + veškerá komunikace (externí i interní, tedy mezi komponentami řešení) musí být šifrovaná;
  + komunikace mezi vrstvami (segmenty) je kontrolována firewallem, v rámci vrstvy (segmentu) neprochází kontrolou firewallu;

### Proxy

Služby proxy serveru, stejně jako služby reverzní proxy, nejsou centrálně poskytovány. Pokud jsou tyto služby vyžadovány, musí být zabezpečeny jako součást řešení (např. s využitím služeb OS).

### Architektonické principy

IS jsou investice, které si Objednatel pořizuje s cílem zajistit požadované funkcionality a procesy, a to s výhledem na řadu let provozu. Zároveň obvykle řešení prochází během svého životního cyklu (a často i během implementace) řadou změn, kdy je nutné reagovat na změny podmínek, požadavků nebo technických komponent. Řešení tedy musí být navrženo takovým způsobem, aby bylo flexibilní a umožnilo Objednateli pružně reagovat na výzvy během produktivního provozu aplikace. Předpokladem je minimálně splnění následujících podmínek:

* veškerá (nevýhradní) práva jsou součástí plnění a přecházejí na Objednatele;
* pokud je to možné, jsou implementované procesy a funkcionality řešeny tak, aby byly bez vazby na konkrétní technologie;
* maximální podpora virtualizace a virtuálního datového centra, bez úzké vazby na HW platformu;
* využívání otevřených řešení, u kterých je zaručena dlouhodobá stabilita při podpoře a dalším rozvoji;
* maximální podpora virtualizace včetně kontejnerizace a virtuálního datového centra, bez úzké vazby na HW platformu;
* podpora flexibilního prostředí s maximální možnou dynamikou;

### Škálovatelnost

Navrhovaná architektura bude schopna pokrýt vzrůstající počet uživatelů, funkcionalit a dat, spravovaných v rámci systému. Škálovatelnost se v tomto smyslu netýká jen růstu počtu uživatelů a množství dat, resp. požadavku na výpočetní výkon, ale i možnosti nasazení distribuovaných aplikací. Cílem je architektura, která neobsahuje úzká místa a dovolí růst od malých nebo pilotních řešení ke komplexnímu celostátnímu nasazení.

### Standardizace procesů rozvoje a podpory

Standardizace procesů administrace, podpory a správy softwaru je základním předpokladem pro úspěšný a bezproblémový chod IS. Navrhované řešení musí podporovat standardní nástroje pro tyto oblasti a zajistit podporu procesům spojených s provozem celého řešení.

* požadována je 3vrstvá architektura s oddělením databázové, aplikační a prezentační vrstvy;
* celkové řešení architektury a procesů podpory zahrnuje oddělené produkční a neprodukční prostředí;
* topologie a architektura produkčního a testovacího prostředí musí být identická, odlišovat se může v sizingu testovacího prostředí;
* řešení je řádně dokumentované

### Náklady na vlastnictví a provoz

Řešení musí zohlednit, zejména z dlouhodobého hlediska, cenově nejpříznivější variantu (samozřejmě s ohledem na zajištění požadovaných procesů a funkcionalit). Při návrhu musí být respektován nejen výchozí a požadovaný stav, ale také náročnost údržby a obnovy.

Preferovány jsou takové alternativy architektury, které zajistí minimalizaci rozsahu používaných technologií, usnadní správu technologického portfolia a umožní opakování ověřených jednoduchých návrhových vzorů.

Řešení také musí zajistit bezproblémový chod ve virtualizovaném prostředí a v cloudu, které umožní Objednateli volit optimální model provozu řešení.

Cílem je dosažení co nejnižších celkových nákladů na vlastnictví (TCO).

### Základní rysy architektury

Navrhovaná architektura musí splňovat následující požadavky a vlastnosti.

#### Dostupnost

Zajištění kontinuity služeb a tedy vysoké dostupnosti je základním předpokladem provozu většiny moderních IS. Způsobů zajištění je celá řada a záleží na Dodavateli, aby kombinací vhodných aplikačních funkcí a služeb infrastruktury navrhl řešení, které bude splňovat parametry a kritéria požadovaná zadávací dokumentací.

Architektura bude důsledně respektovat požadavky na potřebnou dostupnost klíčových komponent. Řešení v tomto případě zahrnuje nejen vhodně volené prostředky IT, ale také určení procesů a prostředků údržby, zálohování, krizových procesů aj. Cílem je zajistit kontinuitu procesů a služeb směrem ke koncovým uživatelům.

#### Zálohování a obnova

Součástí navrženého řešení bude integrace na centrální systém pro zálohování a obnovu dat. Řešení bude obsahovat podrobné postupy pro zálohování a obnovu každé komponenty řešení, stejně jako plán obnovy celkové architektury řešení s ohledem na používaný zálohovací software.

### Preferované architektonické patterny

Tato kapitola popisuje základní doporučované přístupy k návrhu technické architektury a jejího začlenění do prostředí DC Provozovatele infrastruktury.

#### Samostatný virtuální server

##### Předpoklady

Předpoklady architektury samostatného virtuálního serveru:

* základní, nereplikované virtuální servery;
* dostupné všechny typy diskových služeb (STOR1 i STOR2);
* dostupné všechny služby jednoho (obvykle Primárního) DC;
* přístup Administrátora je povolen prostřednictvím VPN na úroveň virtuálního serveru.

##### Popis architektury

Pattern je založen na využití nereplikovaných virtuálních serverů, které jsou provozovány vždy v jednom (obvykle Primárním) DC. V Záložním DC je alokován příslušný výpočetní výkon, ovšem standardně není utilizován. Data jsou replikována prostředky diskového pole.

Umístění virtuálního serveru (tedy to, v jakém DC je virtuální server provozován) nemá vliv na jeho konektivitu nebo na dostupnost průřezových služeb infrastruktury.

Stejně tak dostupnost zálohovacích technologií je transparentní a nezávisí na DC, ve kterém je virtuální server provozován (nezávisle na tom, zda se jedná o backup nebo restore).

Vysoká dostupnost je založena na službách příslušné virtualizační platformy. Pokud je to možné, virtuální server je automaticky zprovozněn v DC, ve kterém je provozován v rámci garantované SLA. Poskytovatel infrastruktury garantuje přístupnost funkcionalit, které jsou součástí služby infrastruktury. Dostupnost aplikačních služeb garantuje Dodavatel.

#### Vysoká dostupnost mezi datovými centry

##### Předpoklady

Předpoklady architektury virtuálního serveru replikovaného přes 2 datová centra:

* aplikační služby jsou pro uživatele dostupné pouze přes VIP (virtual IP);
* využití replikovaných virtuální serverů;
* diskové služby kategorie STOR1. Datový obsah je replikován:
  + synchronně prostředky SAN;
* diskové služby kategorie STOR2. Datový obsah je replikován:
  + asynchronně prostředky SAN
* přístup uživatele je povolen s ohledem na zvolené a schválené politiky konektivity. Doporučuje se použití služeb Load Balanceru (buď dostupné služby infrastruktury, nebo jako vlastnost nasazované aplikace);
* přístup Administrátora je povolen prostřednictvím VPN na úroveň virtuálního serveru, a to do obou DC (samozřejmě že v Záložním DC je server dostupný po jeho převedení a aktivaci);
* pro návrh infrastruktury jsou dostupné všechny služby obou DC.
* služba STOR1 - replikace probíhá:
  + synchronně prostředky SAN;
* služba STOR2 - přičemž replikace probíhá:
  + synchronně prostředky SAN;
  + asynchronně pro virtualizační platformu VMware (x64);

Umístění virtuálního serveru (tedy to, v jakém DC v konkrétním okamžiku běží virtuální server) nemá vliv na jeho konektivitu nebo na dostupnost průřezových služeb infrastruktury (viz. kapitola ). Stejně tak dostupnost zálohovacích technologií je transparentní a nezávisí na DC, ve kterém je virtuální server v daném okamžiku provozován (nezávisle na tom, zda se jedná o backup nebo restore).

Vysoká dostupnost je založena na službách příslušné virtualizační platformy. Pokud je to možné, je virtuální server automaticky zprovozněn v Primárním DC. Pokud je Primární DC, nebo část jeho infrastruktury nedostupná, je virtuální server zprovozněn v Záložním DC. To je provedeno automaticky virtualizační platformou na základě rozhodnutí operátora.

Poskytovatel infrastruktury garantuje přístupnost funkcionalit, které jsou součástí služby infrastruktury. Dostupnost aplikačních služeb garantuje Dodavatel.

##### Popis STOR

Provozovatel infrastruktury zajišťuje provoz diskových služeb STOR1 a STOR2.

Parametry služeb:

* STOR1 - synchronně replikováno mezi lokalitami prostředky SAN, rychlá disková oblast (SSD), určená pro databáze;
* STOR2 - asynchronně replikováno mezi lokalitami pro virtualizační platformu VMware (x64).

##### Fyzická vrstva

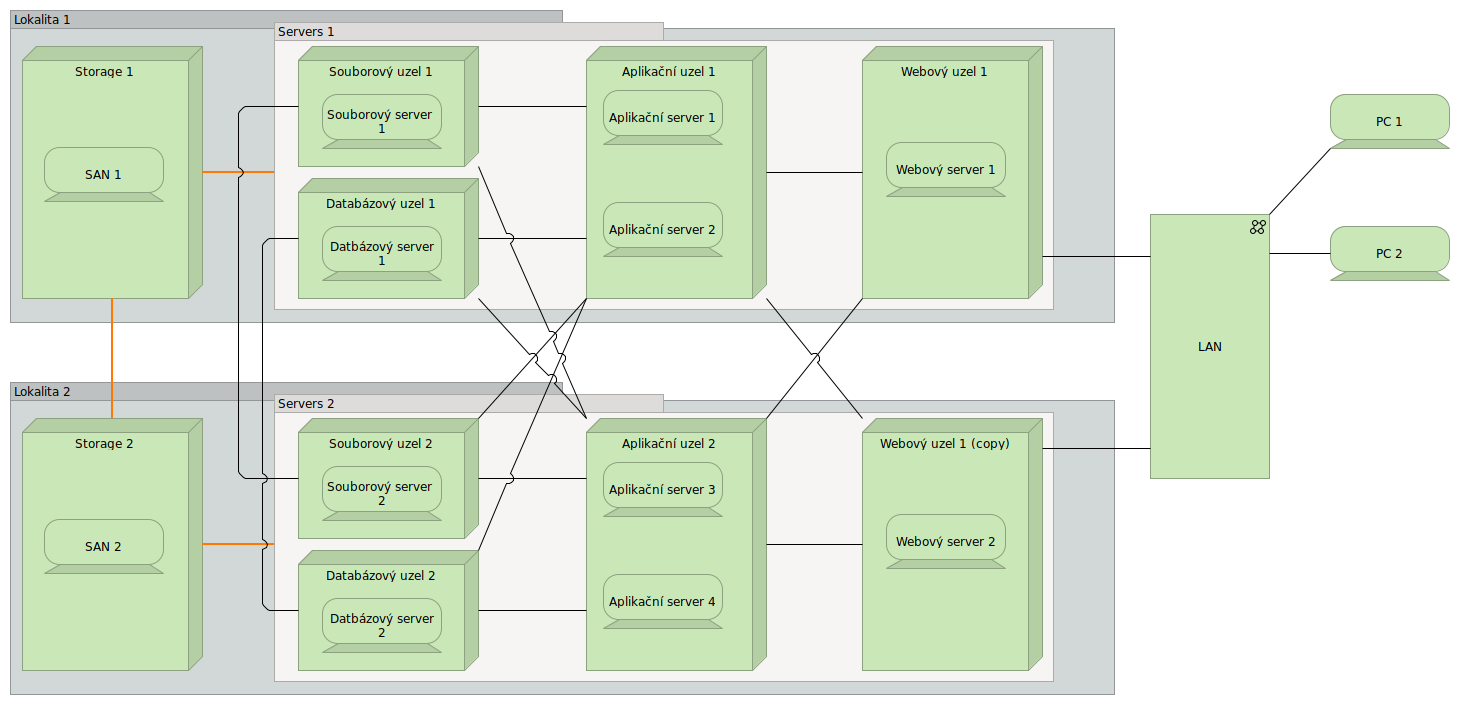
Fyzická vrstva se skládá z:

Servery

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Označení | svr\_1.1 | svr\_1.2 | svr\_2.1 | svr\_2.2 |
| Lokalita | 1 | 1 | 2 | 2 |
| CPU | 1 | 1 | 1 | 1 |
| CORE | 32 | 32 | 32 | 32 |
| RAM [TB] | 1 | 1 | 1 | 1 |
| Dual CPU PassMark | 66 000 | 66 000 | 66 000 | 66 000 |

SAN storage připojený přes FC

|  |  |  |
| --- | --- | --- |
| Označení | san\_1.1 | san\_2.1 |
| Lokalita | 1 | 2 |
| STOR1 [TB] | 9 | 9 |
| STOR2 [TB] | 96 | 96 |

Figure 1: Technologická vrstva