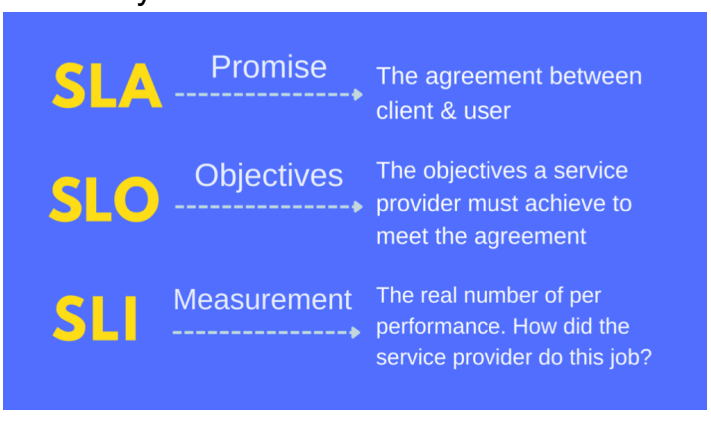
Webový server - logování, zabezpečení, monitoring

Monitoring

- **Je klíčový pro:**
  - Zajištění dostupnosti a rychlé reakce na incidenty
  - Zvýšení bezpečnosti a optimalizaci výkonu
  - Minimalizaci dopadů výpadků
- **Klíčové principy monitoringu:**
  - Sledování metrik (latence, dostupnost, chybovost)
  - Automatizovanou detekci a notifikaci incidentů
  - Analýza logů a provozních dat
- **Přínos:** rychlá reakce a udržení vysoké kvality služby
- **Site Reliability Engineering (SRE):**
  - **Definice:**
    - Je praxe, která integruje principy softwarového inženýrství do provozních procesů
    - Cílem je zvýšit spolehlivost, škálovatelnost a efektivitu provozu systému
  - **Klíčové principy:**
    - **Automatizace**: Minimalizace manuálních zásahů pomocí skriptů a nástrojů
    - **Měřitelnost**: Definice Service Level Objectives (SLO) a Service Level Indicators (SLI) pro sledování výkonů
    - **Incident Management**: Rychlá detekce, řešení incidentů a následná post-mortem analýza



- **Měření a metriky**:
  - **Uptime a dostupnost**: Procentuální dostupnost systému
  - **Latence**: Měření doby odezvy na požadavky
  - **MTTR** (Mean Time to Recovery): Průměrná doba obnovy po incidentu
  - **Chybovost**: Počet incidentů či chyb v daném časovém období

- **Technologie a nástroje:**
  - **Prometheus** - sběr metrik a alerting
  - **Grafana** - vizualizace metrik a dashboardy pro SLO
  - **PagerDuty** - automatizovaná notifikace a eskalace incidentů
  - **ELK Stack** - centralizovaná správa a analýza logů

Logování

- **Logy jsou záznamy událostí generované:**
  - Webovým serverem (Apache, Nginx)
  - Operačním systémem (syslog)
  - Aplikačními frameworky
- Slouží k diagnostice, analýze výkonu a bezpečnostnímu auditu
- **Poskytují:**
  - Historický záznam událostí
  - Podklady pro analýzu incidentů
  - Možnost prediktivní údržby
- Umožňují sledovat trendy a identifikovat problémy dříve, než ovlivní provoz
- **Nástroje**:
  - **Rozlišujeme:**
    - **Lokální nástroje**: Syslog, logrotate
    - **Centralizovaná řešení**: ELK, Stack, Splunk, Graylog
  - Centralizace umožňuje efektivní analýzu a vizualizaci
  - **Praktický postup:**
    - Konfigurace lobovacích služeb ve webovém serveru
    - Použití logrotate k automatické rotaci a archivaci
    - Agregace logů pomocí Logstash a vizualizace v Kibana

Bezpečnost

- Development vs Production servery

- Nikdy nepoužívat development server v produkci! Je pomalý, nezabezpečený a nestabilní
- **Production server:**
  - Optimalizovaný výkon
  - SSL/TLS
  - Komprese, caching
- **Development server:**
  - Volná bezpečnost
  - Není optimalizovaný
  - Debugging tools

- Bezpečnost HTTPS/SSL/TLS

- **HTTPS:**
  - Je rozšíření HTTP s vrstvou zabezpečení
  - Pro zabezpečení přenos dat mezi klientem a serverem
  - Používá SSL/TLS protokoly
- **SSL:**
  - Protokol pro zabezpečení komunikace na internetu
- **TLS:**
  - Následník SSL, modernější a bezpečnější

SSL konfigurace v Nginx

```
server {
    listen 443 ssl http2;
    server_name example.com;
    # SSL certifikáty
    ssl_certificate /etc/letsencrypt/live/example.com/fullchain.pem;
    ssl_certificate_key /etc/letsencrypt/live/example.com/privkey.pem;
    # SSL protokoly a šifry (moderní konfigurace)
    ssl_protocols TLSv1.2 TLSv1.3;
    ssl_ciphers HIGH:!aNULL:!MD5;
    ssl_prefer_server_ciphers on;
    # OCSP stapling
    ssl_stapling on;
    ssl_stapling_verify on;
    # Root a další konfigurace...
}
```

- **HTTPS - Let's Encrypt:**
  - **Let's Encrypt - zdarma SSL certifikáty:**
    - Automatizované vystavení certifikátů (Certbot)
    - 90 dní platnost - automatizovaná obnova
    - Domain validation (DV) - ověření vlastnictví domény
    - Podporování všemi moderními prohlížeči
- **Security headers:**
  - Chrání před útoky

Bezpečnostní hlavičky v Nginx

```
# Ochrana proti clickjackingu
add_header X-Frame-Options "SAMEORIGIN" always;
# Ochrana proti MIME sniffing
add_header X-Content-Type-Options "nosniff" always;
# Content Security Policy (ochrana proti XSS)
add_header Content-Security-Policy "default-src 'self';
# HSTS (HTTP Strict Transport Security)
add_header Strict-Transport-Security "max-age=31536000; includeSubDomains" always;
# XSS Protection (legacy, ale stále užitečné)
add_header X-XSS-Protection "1; mode=block" always;
# Referrer Policy
add_header Referrer-Policy "strict-origin-when-cross-origin" always;
```