Manuál konfigurácie služby **unattended-upgrades**

Nastavenie automatickej aplikácie bezpečnostných záplat na systémoch Debian/Ubuntu a RHEL.

OBSAH

Úvod

Zastaraný softvér je najčastejším vstupným bodom útočníkov. Pravidelná aplikácia bezpečnostných záplat je preto jedným z najúčinnejších opatrení, ktoré môže organizácia prijať, a zároveň jedným z najčastejšie zanedbávaných, pretože si vyžaduje pravidelnú pozornosť správcu systému.

Tento dokument opisuje nastavenie automatickej aplikácie bezpečnostných záplat bez nutnosti manuálneho zásahu. Na systémoch Debian a Ubuntu sa na tento účel používa nástroj **unattended-upgrades**, na systémoch RHEL, CentOS a Fedora nástroj **dnf-automatic**. Oba nástroje fungujú na rovnakom princípe, pravidelne kontrolujú dostupnosť aktualizácií a bezpečnostné záplaty aplikujú automaticky.

Čo automatické aktualizácie riešia a čo nie

Automatické aktualizácie pokrývajú balíky spravované systémovým správcom balíkov, teda samotný operačný systém, NGINX, databázový server a podobné systémové komponenty. **Nepokrývajú** aplikačnú vrstvu: WordPress pluginy a témy, PHP závislosti spravované Composerom, Node.js balíky a podobné. Pre tieto komponenty sú potrebné samostatné procesy aktualizácie.

Pred začatím

> ⚠️ **PRED AKÝMIKOĽVEK ZMENAMI SI VYTVORTE ZÁLOHU**
>
> Pred nastavením automatických aktualizácií sa uistite, že máte funkčnú zálohu systému. Hoci je aplikácia bezpečnostných záplat štandardnou operáciou, každá zmena systému nesie určitú mieru rizika. Záloha je vaša sieť bezpečnosti.

Čo budete potrebovať

- Prístup k serveru
- Základnú znalosť práce s príkazovým riadkom

Distribúcie

Distribúcia	Nástroj
Ubuntu, Debian	`unattended-upgrades`
RHEL, CentOS, AlmaLinux, Rocky Linux, Fedora	`dnf-automatic`

Každá sekcia tohto návodu je rozdelená na paralelné časti pre obe distribúcie. Postupujte len podľa časti zodpovedajúcej vašemu systému.

01

KAPITOLA PRVÁ

Inštalácia a spustenie

Inštalácia nástroja a spustenie automatických aktualizácií ako systémovej služby.

1 Inštalácia nástroja

Debian / Ubuntu

Na väčšine moderných Ubuntu a Debian inštalácií je `unattended-upgrades` predvolene nainštalovaný. Overte to príkazom:

```
dpkg -l unattended-upgrades
```

Ak balík nie je nainštalovaný, nainštalujte ho spolu s nástrojom `apt-listchanges`, ktorý zaznamenáva popis každej aplikovanej zmeny:

```
sudo apt update
sudo apt install unattended-upgrades apt-listchanges -y
```

RHEL

Na systémoch RHEL, CentOS, AlmaLinux a Rocky Linux nainštalujte `dnf-automatic`:

```
sudo dnf install dnf-automatic -y
```

2 Spustenie a povolenie služby

Debian / Ubuntu

Spustite sprievodcu základnou konfiguráciou. Na otázku o automatických aktualizáciách odpovedzte **Yes**:

```
sudo dpkg-reconfigure -plow unattended-upgrades
```

Overte, že služba je spustená:

```
sudo systemctl status unattended-upgrades
```

Výstup by mal obsahovať `Active: active (running)`.

RHEL

Povolte a spustite časovač pre automatické aplikovanie aktualizácií:

```
sudo systemctl enable --now dnf-automatic-install.timer
```

Overte, že časovač je spustený:

```
sudo systemctl status dnf-automatic-install.timer
```

Výstup by mal obsahovať `Active: active (waiting)`.

> 📋 **ROZDIELY MEDZI ČASOVAČMI NA RHEL**
>
> Na RHEL sú dostupné tri časovače: `dnf-automatic-install.timer` (automaticky inštaluje aktualizácie - odporúčané), `dnf-automatic-download.timer` (len stiahne, nenainštaluje) a `dnf-automatic-notifyonly.timer` (len upozorní). Pre účely tohto návodu používajte `dnf-automatic-install.timer`.

02

KAPITOLA DRUHÁ

Konfigurácia

Nastavenie toho, čo sa aktualizuje, čo nie, a ako sa systém správa po aktualizácii jadra.

3 Povolené zdroje aktualizácií

Pre väčšinu organizácií odporúčame automaticky aplikovať len **bezpečnostné záplaty**, teda aktualizácie opravujúce zraniteľnosti. Všeobecné aktualizácie (nové funkcie, zmeny správania) je bezpečnejšie aplikovať manuálne a pred nasadením otestovať.

Debian

Otvorte súbor `/etc/apt/apt.conf.d/50unattended-upgrades`:

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Nájdite sekciu `Unattended-Upgrade::Origins-Pattern`. Na Debian 12 sú správne bezpečnostné zdroje už predvolene odkomentované. Overte si, že nasledujúce tri riadky sú aktívne (bez `//` na začiatku):

```
Unattended-Upgrade::Origins-Pattern {
    "origin=Debian,codename=${distro_codename},label=Debian";
    "origin=Debian,codename=${distro_codename},label=Debian-Security";
    "origin=Debian,codename=${distro_codename}-security,label=Debian-Security";
};
```

Riadky pre `-updates` a `-proposed-updates` nechajte zakomentované (`//` na začiatku). Tie pokrývajú všeobecné aktualizácie, nie len bezpečnostné.

> 📋 **AKO FUNGUJÚ KOMENTÁRE V TOMTO SÚBORE**
>
> Riadky začínajúce `//` sú zakomentované a ignorované. Ak chcete nejaký zdroj zakázať, pridajte pred riadok `//`. Ak chcete povoliť, `//` odstráňte.

Ubuntu

Otvorte súbor `/etc/apt/apt.conf.d/50unattended-upgrades`:

```
sudo nano /etc/apt/apt.conf.d/50unattended-upgrades
```

Na Ubuntu sa sekcia volá `Unattended-Upgrade::Allowed-Origins` a používa iný formát. Overte, že je aktívny len bezpečnostný zdroj:

```
Unattended-Upgrade::Allowed-Origins {
    "${distro_id}:${distro_codename}-security";
    // "${distro_id}:${distro_codename}-updates";  // zakomentované = vypnuté
};
```

RHEL

Otvorte súbor `/etc/dnf/automatic.conf`:

```
sudo nano /etc/dnf/automatic.conf
```

V sekcii `[commands]` nastavte typ aktualizácií na `security`:

```
[commands]
upgrade_type = security
```

Predvolená hodnota je `default`, ktorá aplikuje všetky aktualizácie. Zmeňte ju na `security`.

4 Vylúčenie balíkov z automatickej aktualizácie

Niektoré balíky môžu byť kritické pre prevádzku a ich automatická aktualizácia môže narušiť funkčnosť. Takéto balíky je možné vylúčiť.

Debian / Ubuntu

V súbore `/etc/apt/apt.conf.d/50unattended-upgrades` nájdite sekciu `Package-Blacklist`, predvolene je prázdna a všetky riadky sú zakomentované. Pridajte balíky, ktoré chcete vylúčiť:

```
Unattended-Upgrade::Package-Blacklist {
    "mysql-server";
    "php.*";
};
```

⚠ **BLACKLIST POUŽÍVA PYTHON REGULÁRNE VÝRAZY**

Názvy balíkov v blackliste sú Python regulárne výrazy. Bežné vzory: `"mysql-server"` presná zhoda, `"php.*"` všetky balíky začínajúce na `php`, `"libc6$"` presná zhoda na konci názvu. Nesprávny vzor môže spôsobiť, že balík nebude vylúčený aj keď si to myslíte.

RHEL

V súbore `/etc/dnf/dnf.conf`, v sekcii `[main]`, pridajte:

```
[main]
excludepkgs=mysql-server php*
```

⚠ **VYLÚČENÉ BALÍKY ZOSTÁVAJÚ NEZÁPLATOVANÉ**

Každý balík vylúčený z automatickej aktualizácie musí byť aktualizovaný manuálne. Zaraďte kontrolu vylúčených balíkov do mesačného plánu auditu a aplikujte záplaty ručne.

5 Automatický reštart po aktualizácii jadra

Niektoré bezpečnostné aktualizácie, najmä aktualizácie jadra operačného systému, vyžadujú reštart servera, aby sa záplata skutočne aktivovala.

⚠ **AUTOMATICKÝ REŠTART PRODUKČNÉHO SERVERA - ZVÁŽTE DÔSLEDKY**

Automatický reštart servera môže spôsobiť krátkodobú nedostupnosť služby. Pred povolením zvážte: má vaša stránka stanovené servisné okno? Ovplyvní výpadok niekoľkých minút používateľov? Ak si nie ste istí, nastavte reštart na čas s najnižšou návštevnosťou a vopred informujte zainteresovaných.

Debian / Ubuntu

V súbore `/etc/apt/apt.conf.d/50unattended-upgrades` nájdite zakomentované riadky pre automatický reštart a odkomentujte ich:

```
// Povolenie automatického reštartu
Unattended-Upgrade::Automatic-Reboot "true";

// Čas reštartu - odporúčame mimo prevádzkových hodín
Unattended-Upgrade::Automatic-Reboot-Time "03:00";
```

📋 **ALTERNATÍVA BEZ AUTOMATICKÉHO REŠTARTU**

Ak nechcete automatický reštart, nechajte `Automatic-Reboot "false"` a zaraďte do týždenných úloh kontrolu, či systém čaká na reštart:

```
cat /var/run/reboot-required
```

Ak súbor existuje, naplánujte reštart manuálne na vhodný čas.

RHEL

Na RHEL automatický reštart nie je priamo súčasťou `dnf-automatic`. Overte, či systém potrebuje reštart:

```
sudo needs-restarting -r
```

Ak príkaz indikuje potrebu reštartu, naplánujte ho manuálne na vhodný čas.

03

KAPITOLA TRETIA

Logovanie

Logovanie automatických aktualizácií je nielen dobrá prax, ale pre mnohé organizácie zákonná povinnosť. Táto kapitola pokrýva overenie logov, retenciu, zabezpečenie a monitoring.

6 Overenie a umiestnenie logov

Automatické aktualizácie zaznamenávajú každé spustenie, každú aplikovanú záplatu aj každú chybu. Bez pravidelnej kontroly logov nemáte istotu, že systém skutočne funguje. Zlyhanie môže prebehnúť potichu.

Debian / Ubuntu

Hlavný log `unattended-upgrades` sa nachádza v súbore `/var/log/unattended-upgrades/unattended-upgrades.log`. Overte, že existuje a obsahuje záznamy:

```
sudo tail -50 /var/log/unattended-upgrades/unattended-upgrades.log
```

Úspešná aplikácia aktualizácie vyzerá takto:

```
INFO Packages that will be upgraded: nginx
INFO Packages that were successfully upgraded: nginx
```

Hľadajte riadky obsahujúce `ERROR` alebo `WARNING`, tie indikujú problém vyžadujúci pozornosť.

RHEL

Logy `dnf-automatic` sú súčasťou systemd journal. Pre zobrazenie posledných záznamov:

```
sudo journalctl -u dnf-automatic-install -n 50
```

Pre sledovanie v reálnom čase počas manuálneho spustenia:

```
sudo journalctl -u dnf-automatic-install -f
```

7 Retencia logov

Uchovávanie logov po dostatočne dlhú dobu je pre mnohé organizácie zákonnou povinnosťou. Konkrétna požadovaná doba retencie závisí od legislatívy aplikovateľnej na vašu organizáciu.

Debian / Ubuntu - predĺženie retencie

Predvolená retencia logov `unattended-upgrades` je riadená nástrojom `logrotate`. Overte aktuálnu konfiguráciu:

```
cat /etc/logrotate.d/unattended-upgrades
```

Ak chcete predĺžiť retenciu, upravte hodnotu `rotate` v súbore `/etc/logrotate.d/unattended-upgrades`. Príklad pre 365-dňovú retenciu pri dennej rotácii:

```
sudo nano /etc/logrotate.d/unattended-upgrades
```

```
/var/log/unattended-upgrades/unattended-upgrades.log {
    rotate 365
    daily
    compress
    missingok
    notifempty
}
```

RHEL - retencia journal logov

Na RHEL sú logy uložené v systemd journal. Nastavte maximálnu veľkosť alebo dobu uchovávania v súbore `/etc/systemd/journald.conf`:

```
sudo nano /etc/systemd/journald.conf
```

```
[Journal]
MaxRetentionSec=365day
SystemMaxUse=500M
```

Po zmene reštartujte journald:

```
sudo systemctl restart systemd-journald
```

8 Zabezpečenie a zálohovanie logov

Logy uložené len na tom istom serveri, ktorý monitorujú, majú obmedzenú hodnotu. Správne musia byť logy uložené oddelene od systému, ktorý ich generuje.

Oprávnenia log súborov

Overte, že log súbory majú správne oprávnenia, čitateľné len pre `root` a skupinu `adm`:

```
ls -la /var/log/unattended-upgrades/
```

Štandardné oprávnenia sú `640`. Ak sú iné, opravte ich. Príkaz pokryje všetky súbory vrátane komprimovaných archívov:

```
sudo find /var/log/unattended-upgrades/ \
  -exec chmod 640 {} \; -exec chown root:adm {} \;
```

Zálohovanie logov na oddelené úložisko

Logy pravidelne kopírujte na server alebo úložisko oddelené od produkčného systému. Pred spustením rsync je potrebné nastaviť prihlasovanie cez SSH kľúče bez hesla. Váš IT správca vám s tým pomôže, alebo si nastavenie vykonajte podľa dokumentácie `ssh-keygen` a `ssh-copy-id`.

Príkaz spúšťajte ako bežný používateľ, nie ako root. Váš používateľ musí byť členom skupiny `adm` pre čítanie log adresára. Nahraďte `pouzivatel`, `zalohovaci-server`, port SSH a `hostname` hodnotami pre váš systém:

```
rsync -av --no-times -e "ssh -p 22" \
  /var/log/unattended-upgrades/ \
  pouzivatel@zalohovaci-server:/logs/hostname/unattended-upgrades/
```

Ak váš zálohovací server používa iný port SSH, nahraďte `22` správnym číslom portu. Po overení, že príkaz funguje, ho zaraďte do cron úlohy pre pravidelné automatické kopírovanie. Cron úlohu vytvorte bez sudo, rsync musí byť spustený pod vašim používateľom, ktorý má SSH kľúč nakonfigurovaný:

```
crontab -e
```

```
# Denné zálohovanie logov o 04:00
0 4 * * * rsync -aq --no-times -e "ssh -p 22" \
  /var/log/unattended-upgrades/ \
  pouzivatel@zalohovaci-server:/logs/hostname/unattended-upgrades/
```

Overte, že cron úloha bola uložená:

```
crontab -l
```

> 📋 **AK NEMÁTE ZÁLOHOVACÍ SERVER**
>
> Ak vaša organizácia nemá dedikovaný zálohovací server, logy je možné kopírovať na NAS, externé úložisko alebo do cloudového úložiska (S3, Azure Blob). Minimálnym prijateľným riešením je manuálne kopírovanie logov na externé médium raz mesačne. Nie je ideálne, ale lepšie ako žiadna záloha. Riešenie konzultujte so svojím nadriadeným alebo IT oddelením.

9 Monitoring logov - logwatch

Nástroj `logwatch` automaticky analyzuje systémové logy a generuje prehľadný denný súhrn vrátane aplikovaných aktualizácií, chýb a ďalších systémových udalostí. Je výrazne jednoduchší než sledovanie surových log súborov a nevyžaduje externý e-mailový server.

Debian / Ubuntu

```
sudo apt install logwatch -y
```

Manuálne spustenie a zobrazenie súhrnu priamo v termináli:

```
sudo logwatch --output stdout --range today
```

Pre denný automatický súhrn uložený do súboru, ktorý si môžete pozrieť kedykoľvek:

```
crontab -e
```

```
# Denný súhrn logwatch o 06:00, uložený do súboru
0 6 * * * logwatch --output file --filename /var/log/logwatch-daily.log --range yesterday
```

RHEL

```
sudo dnf install logwatch -y
```

Použitie je rovnaké ako na Debian/Ubuntu, príkazy sú identické.

✅ **ZARAĎTE KONTROLU LOGOV DO TÝŽDENNEJ RUTINY**

Automatické aktualizácie a logwatch fungujú bez vašej pozornosti, ale logy je potrebné pravidelne čítať. Zaraďte nasledujúce príkazy do týždenného plánu auditu:

```
# Posledné záznamy unattended-upgrades
sudo tail -50 /var/log/unattended-upgrades/unattended-upgrades.log

# Dnešný logwatch súhrn
sudo logwatch --output stdout --range today
```

04

KAPITOLA ŠTVRTÁ

Overenie funkčnosti

Automatická aktualizácia, ktorú ste nikdy neoverili, nie je zárukou.

10 Manuálny test - dry run

Dry run simuluje celý proces automatickej aktualizácie bez skutočnej inštalácie čohokoľvek.

Debian / Ubuntu

```
sudo unattended-upgrade --dry-run --debug
```

Výstup ukáže, ktoré balíky by boli aktualizované a z akých zdrojov. Ak výstup hlási `No packages found that can be upgraded unattended`, systém je aktuálny, to je správny výsledok.

RHEL

```
sudo systemctl start dnf-automatic-install
```

11 Overenie stavu služby

Overte, že automatické aktualizácie sú spustené ako plánovaná úloha.

Debian / Ubuntu

```
# Stav služby
sudo systemctl status unattended-upgrades

# Kedy bola služba naposledy spustená
sudo systemctl list-timers | grep apt
```

RHEL

```
# Stav časovaču
sudo systemctl status dnf-automatic-install.timer

# Kedy bol časovač naposledy spustený
sudo systemctl list-timers | grep dnf
```

✅ **ČO HĽADAŤ VO VÝSTUPE LIST-TIMERS**

Príkaz `list-timers` zobrazí stĺpec `LAST` (kedy bol časovač naposledy spustený) a `NEXT` (kedy bude spustený nasledujúce). Ak stĺpec `LAST` zobrazuje `n/a`, časovač ešte nebol spustený, to je normálne hneď po konfigurácii. Ak hodnota `n/a` pretrváva aj po dni, skontrolujte logy.

12 Riešenie bežných problémov

Aktualizácie sa nespúšťajú

Overte, že časovač je aktívny:

```
# Debian/Ubuntu
sudo systemctl is-active unattended-upgrades

# RHEL
sudo systemctl is-active dnf-automatic-install.timer
```

Ak je výstup `inactive`, spustite a povolte službu znova podľa sekcie 2.

Chyba pri aktualizácii konkrétneho balíka

Niekedy aktualizácia zlyhá kvôli konfliktu závislostí alebo poškodenej lokálnej cache. Vyskúšajte manuálnu opravu:

Debian / Ubuntu

```
sudo apt --fix-broken install
sudo apt update && sudo apt upgrade -y
```

RHEL

```
sudo dnf clean all
sudo dnf update -y
```