

# Manuál pre prevádzku

Verzia: 2025.0.1 23.02.2025 16:44:38

# Obsah

---

- Bezpečnosť
  - [Bezpečnostné testy](#)
  - [Kontrola zraniteľností knižníc](#)
  - [Aktualizácia WebJETu](#)
- Audit
  - [Audit](#)
  - [Zoznam notifikácií](#)
  - [Zmenené stránky](#)
  - [Čaká na publikovanie](#)
  - [Úrovne logovania](#)
  - [Log súbory](#)
  - [Posledné logy](#)
- Prevádzka
  - [Výkon servera](#)
  - [Monitorovanie servera](#)
  - [Reštartovať](#)
  - [Výmena údajov uzlov clustra](#)
  - [Mazanie dát](#)
- Súbory
  - [Zálohovanie systému](#)

# 1. Bezpečnostné testy

Zabezpečenie WebJET CMS je podmienené jeho korektnou konfiguráciou a korektným nastavením prístupových práv. Informácie na tejto stránke je potrebné nastaviť pred spustením do produkčnej prevádzky a následne kontrolovať minimálne na kvartálnej báze a vždy pred vykonaním bezpečnostných testov.

## 1.1. Nastavenie systému

### 1.1.1. Skupiny práv

Cez WebJET CMS je možné upravovať aj programové súbory, preto je potrebné pred penetračnými testami nastaviť obmedzenia práv. Odporúčame vytvoriť nižšie uvedené [skupiny práv](https://docs.webjetcms.sk/latest/sk/admin/users/perm-groups) (<https://docs.webjetcms.sk/latest/sk/admin/users/perm-groups>). **Iné skupiny používateľov, alebo priamo používatelia, by nižšie uvedené jednotkové práva nemali mať povolené.**

#### Správa používateľov

Skupina obsahuje práva, ktoré umožňujú modifikovať oprávnenia. Používateľ s takouto skupinou práv musí byť dostatočne obozretný a musí mu byť jasné, že má najvyššie možnosti práv (pretože dokáže nastavovať práva sám sebe, alebo iným používateľom).

Používateľ s takýmto právom dokáže kompromitovať celý systém (napr. dokáže si nastaviť oprávnenia tak, že dokáže zmazať všetky web stránky, alebo všetky súbory).

Skupine práv nastavte nasledovné práva:

- správa administrátorov - právo umožňuje nastavovať oprávnenia používateľom v administrácii
- Skupiny práv - právo umožňuje nastavovať oprávnenia na skupiny

#### Programátor

Štandardné nastavenie by malo byť také, že používatelia (redaktori) nemôžu nahrávať a modifikovať programové súbory. Programátor ale často potrebuje vykonať rýchlu zmenu ( `hotfix` ) programového kódu a potrebuje teda modifikovať aj programové súbory. Zároveň má pridané práva pre zmenu všetkých konfiguračných premenných a editáciu všetkých prekladových textov.

Používateľ s takýmto právom dokáže kompromitovať celý systém (napr. dokáže nahráť škodlivý kód, ktorý na serveri môže vykonať ľubovoľnú operáciu vrátane zmazania súborov na serveri, alebo kompletného zmazania databázy).

- Neobmedzené nahrávanie súborov (prípony a veľkosti)
- Konfigurácia - zobrazenie všetkých premenných
- Editácia textov - zobrazenie všetkých textov

Poznámka: zoznam konf. premenných bez oprávnenia "Konfigurácia - zobrazenie všetkých premenných" sa nastavuje v konf. premennej `configEnabledKeys`, zoznam prekladových kľúčov bez oprávnenia "Editácia textov - zobrazenie všetkých textov" v konf. premennej `propertiesEnabledKeys`. V prekladových kľúčoch sa zároveň filtruje HTML kód, pravidlá nastavenia sú opísané nižšie v sekcii `Stored XSS cez úpravu prekladových kľúčov`.

Okrem oprávnení je potrebné povoliť prístup na zápis do adresárov súborového systému:

- `/apps` - obsahuje kód aplikácií
- `/components` - obsahuje kód aplikácií
- `/templates` - obsahuje dizajnové šablóny

Ak je prostredie nasadzované priamo z GIT repozitára a nepredpokladáte vykonanie `hot-fixov` priamo cez WebJET CMS nemusíte vyššie uvedené práva na zápis do súborového systému nastavovať. Navyše pre tento prípad odporúčame nastaviť na súborovom systéme oprávnenia zápisu len pre adresáre (ostatné adresáre a súbory majú oprávnenia len na čítanie):

- `/images` - obsahuje obrázky nahraté redaktormi CMS

- `/files` - obsahuje súbory nahraté redaktormi CMS
- `/shared` - obsahuje obrázky a súbory nahraté redaktormi CMS zdieľané medzi doménami
- `/WEB-INF/tmp` - obsahuje dočasné súbory CMS
- `/WEB-INF/imgcache` - obsahuje generované zmenšeniny a výrezy obrázkov pre použitie cez `/thumb` prefix
- `/WEB-INF/formfiles` - obsahuje súbory nahraté cez formuláre na web stránke vytvorené cez aplikáciu Formuláre

### 1.1.2. Konfigurácia

Nastavte a skontrolujte nasledovné konfiguračné premenné (v administrácii Nastavenia->Konfigurácia):

- `defaultDisableUpload=true` - aktivuje režim, v ktorom má používateľ práva na súborový systém len pre nastavené adresáre. Ak nemá nastavený žiaden adresár nebude mať právo zápisu súboru do žiadneho adresára.
- `emailProtectionSenderEmail` - nastavte vhodnú emailovú adresu typu `noreply@domena.sk`, ktorá sa použije ako email adresa odosielaných emailov (pôvodná hodnota sa nastaví do `Reply-To` hlavičky emailu).
- `adminEnabledIPs` - obsahuje čiarkou oddelený zoznam IP adries, z ktorých je povolený prístup do `/admin` časti.
- `multidomainAdminHost` - umožňuje nastaviť samostatnú doménovú adresu pre prístup do `/admin` časti, napr. `cms.domena.sk`. Po nastavení bude volanie `/admin` adresy na ostatných doménach vracať chybu 404 - Stránka neexistuje.
- `serverBeyondProxy` - ak je aplikačný server za Load Balancerom / proxy je potrebné nastaviť hodnotu na `true` (inak nastavte hodnotu `false`). Load Balancer musí následne posilať v HTTP hlavičke `x-forwarded-for` IP adresu návštevníka web stránky a v hlavičke `x-forwarded-proto` protokol (`http` alebo `https`). Overtvorte v audite (napr. po vyplnení formuláru na web stránke) korektné zaznamenanie IP adresy návštevníka web stránky.
- `serverName` - predvolene `unknown` - nastavuje hodnotu HTTP hlavičky `Server` pri HTTP odpovedi. Ak máte aplikačný server za Load Balancerom/proxy overte v HTTP odpovedi hodnotu tejto hlavičky a prípadne ju nastavte na Load Balanceri/proxy serveri na vhodnú neznámu hodnotu.

Obmedzenia pre nahrávané súbory redaktormi v administrácii:

- `FCKConfig.UploadMaxSize[Default][image]` - predvolene 0 - limit veľkosti v kB pre nahrávanie **obrázkov**, odporúčame nastaviť na hodnotu napr. 10000 pre nahranie max 10 MB obrázka
- `FCKConfig.UploadMaxSize[Basic][image]` - predvolene 2048 - limit veľkosti v kB pre nahrávanie **obrázkov** pre používateľov, ktorý **nemajú právo Kompletné menu v editore**
- `FCKConfig.UploadMaxSize[Default][file]` - predvolene 0 - limit veľkosti v kB pre nahrávanie **súborov**, odporúčame nastaviť na hodnotu napr. 50000 pre nahranie max 50 MB súboru
- `FCKConfig.UploadMaxSize[Basic][file]` - predvolene 2048 - limit veľkosti v kB pre nahrávanie **súborov** pre používateľov, ktorý **nemajú právo Kompletné menu v editore**
- `FCKConfig.UploadFileTypes[Default][image]` - predvolene prázdne = bez obmedzení - limity typov **obrázkov**, odporúčame nastaviť na hodnotu `jpg,jpeg,png,gif,svg,mp3,mp4`. Možnosť povolenia prípony SVG je potrebné zvážiť, vid' potencionálne riziko nižšie v bloku **Stored XSS cez SVG obrázok**.
- `FCKConfig.UploadFileTypes[Basic][image]` - predvolene `jpg,jpeg,png,gif,mp4` - limity typov **obrázkov** pre používateľov, ktorý **nemajú právo Kompletné menu v editore**
- `FCKConfig.UploadFileTypes[Default][file]` - predvolene prázdne = bez obmedzení - limity typov **súborov**, odporúčame nastaviť na hodnotu `pdf,docx,xlsx,pptx,pps,zip,rtf`
- `FCKConfig.UploadFileTypes[Basic][file]` - predvolene `doc,docx,xls,xlsx,pdf,zip,rtf` - limity typov **súborov** pre používateľov, ktorý **nemajú právo Kompletné menu v editore**

Môžete skontrolovať ešte nasledovné konf. premenné:

- `overviewJsonUrl` - definuje URL adresu, z ktorej sa číta zoznam noviniek vo WebJETe. Ak používatelia nemajú dostupný internet z prehliadača, môžete nastaviť na hodnotu `/admin/v9/json/` pre čítanie z lokálnej inštancie. Používatelia ale nebudú vidieť novinky v nových verziách WebJET CMS.
- `springSecurityAllowedAuths` - zoznam povolených metód autorizácie pre REST služby, predvolene `basic,api-token`. Ak projekt nepotrebuje iné ako štandardné prihlásenie cez formulár, nastavte na prázdnu hodnotu. Po zmene hodnoty je potrebné reštartovať aplikačný server.

### 1.1.3. HTTP hlavičky

V aplikácii Konfigurácia môžete nastaviť hodnoty bezpečnostných hlavičiek:

- `contentSecurityPolicy` - nastavenie hlavičky `Content-Security-Policy`. Obmedzenie ako má stránka načítavať rôzne zdroje. Ak máte httpS certifikát môžete nastaviť na hodnotu:  
`default-src 'none'; script-src https: blob: data: 'unsafe-inline' 'unsafe-eval'; worker-src https: blob:; child-src https:`  
Predvolene prázdne (hlavička sa nenastavuje).
- `contentSecurityPolicySvg` - špecifické obmedzenie pre SVG obrázky z dôvodu ich iného spracovania v Internet Explorer.
- `featurePolicyHeader` - hodnota HTTP hlavičky `Feature-Policy/Permissions-Policy` (napr.:  
`microphone 'none'; geolocation 'none'`), viac na: [https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature\\_Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy)  
([https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature\\_Policy](https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy)). Predvolene prázdne.
- `referrerPolicy` - nastavenie HTTP hlavičky `Referrer-Policy`, odporúčame nastaviť na hodnotu `same-origin`. Predvolene `same-origin`.
- `serverName` - hodnota hlavičky `Server` v HTTP odpovediach. Predvolene `unknown`. Nie je možné nastaviť na prázdnu hodnotu, pretože potom tam vloží hlavičku aplikačný server.
- `strictTransportSecurity` - predvolene prázdne - nastavuje HTTP hlavičku [Strict-Transport-Security](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) ([https://en.wikipedia.org/wiki/HTTP\\_Strict\\_Transport\\_Security](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security)) v HTTP odpovediach, čo zabezpečí presmerovanie HTTP požiadaviek na zabezpečený httpS, odporúčame nastaviť na hodnotu: `max-age=31536000 ; includeSubDomains`. Vyžaduje, aby aplikačný server bol dostupný cez zabezpečený httpS protokol.
- `xContentTypeOptions` - hodnota hlavičky `X-Content-Type-Options` pre nastavenie určovania typov súborov podľa obsahu (ignorovanie prípony). Predvolene `nosniff`.
- `xFrameOptions` - hodnota hlavičky `X-Frame-Options` pre ochranu pred CSRF útokom. Predvolene `SAMEORIGIN`.
- `xRobotsTagValue` - hodnota hlavičky `X-Robots-Tag` pre URL adresy nastavené v premennej `xRobotsTagUrls`. Predvolene `noindex, nofollow`.
- `xRobotsTagUrls` - zoznam začiatkov URL adries oddelených čiarkou pre nastavenie hlavičky `X-Robots-Tag`. Ak zoznam obsahuje hodnotu `NOT_SEARCHABLE_PAGE` nastaví sa hlavička aj pre stránky, ktoré majú vypnuté vyhľadávanie. Predvolene `/components/,NOT_SEARCHABLE_PAGE`.
- `xXssProtection` - hodnota hlavičky `X-XSS-Protection` pre ochranu pred XSS útokom. Predvolene `1; mode=block`.

Nastavenie hlavičky `Access-Control` pre prístup k REST službám z iných serverov:

- `accessControlAllowOriginValue` - hodnota hlavičky `Access-Control-Allow-Origin` pre URL nastavené v premennej `accessControlAllowOriginUrls`. V hodnote môžete použiť makro (viď nižšie). Predvolene nastavené na `{HTTP_PROTOCOL}://{SERVER_NAME}:{HTTP_PORT}`.
- `accessControlAllowOriginUrls` - zoznam začiatkov URL adries oddelených čiarkou pre nastavenie hlavičky `Access-Control-Allow-Origin`. Predvolene nastavené na `/rest/,/private/rest/,/admin/rest/`.
- `accessControlAllowHeaders` - hodnota pre nastavenie hlavičky `Access-Control-Allow-Headers`, nastavuje sa len pri generovaní hlavičky `Access-Control-Allow-Origin`. Predvolene `Origin, Accept, X-Requested-With, Content-Type, Access-Control-Request-Method, Access-Control-Request-Headers, x-csrf-token`.
- `accessControlAllowMethods` - hodnota pre nastavenie hlavičky `Access-Control-Allow-Methods`, nastavuje sa len pri generovaní hlavičky `Access-Control-Allow-Origin`. Predvolene `HEAD,POST,GET,OPTIONS,PUT`.
- `accessControlMaxAge` - hodnota pre nastavenie hlavičky `Access-Control-Max-Age`, nastavuje sa len pri generovaní hlavičky `Access-Control-Allow-Origin`. Predvolene `1800`.
- `accessControlAllowedOrigins` - ak nie je prázdne, vyžaduje pri požiadavke hlavičku `origin`, ktorej hodnota sa musí nachádzať v tomto zozname (čiarkou/novým riadkom oddelený zoznam). Nastavuje sa len pri generovaní hlavičky `Access-Control-Allow-Origin`. Predvolene prázdne.

Ak potrebujete nastaviť inú HTTP hlavičku môžete použiť aplikáciu [HTTP hlavičky](https://docs.webjetcms.sk/latest/sk/admin/settings/response-header/README) (<https://docs.webjetcms.sk/latest/sk/admin/settings/response-header/README>) v sekcii Nastavenia.

V hodnote môžete použiť makro `{HTTP_PROTOCOL}`, `{SERVER_NAME}/{DOMAIN_NAME}/{DOMAIN_ALIAS}`, `{HTTP_PORT}`, ktoré bude nahradené za hodnotu získanú na serveri. `SERVER_NAME` je doménové meno z `request.getServerName()`, `DOMAIN_NAME` a `DOMAIN_ALIAS` sú hodnoty domén alebo alias-u nastavené vo web stránkach. Hodnota `{INSTALL_NAME}` reprezentuje meno inštalácie. Hodnota `{HEADER_ORIGIN}` obsahuje hodnotu HTTP hlavičky `origin`.

V starších inštaláciach bolo možné nastaviť HTTP hlavičky aj cez konf. premennú `responseHeaders` v ktorej viete nastaviť hlavičku pre URL prefix (začiatok URL adresy). Na každý riadok zadáte hodnotu vo formáte: `url-prefix:hlavička:hodnota`, napríklad:

```
/admin:X-Accel-Buffering:no
/rest/calculators/:Access-Control-Allow-Origin:*
/rest/calculators/:Access-Control-Allow-Headers:origin,x-requested-with,access-control-request-headers,content-type,access-control-request-method,accept,x-csrf-token
/rest/calculators/:Access-Control-Allow-Methods:GET,OPTIONS
```

Hodnoty nastavené cez konf. premennú `responseHeaders` sú globálne bez ohľadu na aktuálnu doménu.

#### 1.1.4. Pravidlá hesiel

Pravidlá pre heslá je možné nastaviť cez nasledovné konfiguračné premenné (pri premennej je v zátvorke uvedená štandardná hodnota):

- `passwordAdminMinLength` - Určuje minimálne akej dĺžky ma byť heslo pre administrátora (5).
- `passwordAdminMinCountOfSpecialSigns` - Určuje minimálny počet výskytu špeciálnych znakov v hesle pre administrátora (0).
- `passwordAdminMinUpperCaseLetters` - Určuje minimálny počet výskytu veľkých písmen v hesle pre administrátora (1).
- `passwordAdminMinLowerCaseLetters` - Určuje minimálny počet výskytu malých písmen v hesle pre administrátora (0).
- `passwordAdminMinCountOfDigits` - Určuje minimálny počet výskytu čísel v hesle pre administrátora (1).
- `passwordAdminExpiryDays` - Určuje počet dní platnosti hesla pre administrátora. Po uplynutí času, bude užívateľ vyzvaný si zmeniť heslo. Hodnota 0 znamená, že sa nekontroluje expirácia hesla (0).

Podobne sa dajú nastaviť pravidlá hesiel aj pre prihlásenie do zabezpečenej zóny web stránky (nie administrácie), premenné sú rovnaké, ale neobsahujú výraz `Admin`. Čiže meno premennej je napr. `passwordMinUpperCaseLetters`.

Nastavením konfiguračnej premennej `isGoogleAuthRequiredForAdmin` na `true` bude pre prístup do `/admin` časti vyžadovaná dvoj faktorové overovanie. Každý používateľ ju vopred musí nastaviť v administrácii kliknutím na svoje meno vpravo hore a zvolením možnosti **Dvojstupňové overovanie**, respektíve otvorením stránky `/admin/2factorauth.jsp`.

Dvojstupňové overovanie odporúčame nastaviť minimálne na všetky kontá, cez ktoré je možné spravovať používateľské účty a práva a nastavovať konfiguráciu systému.

WebJET kontroluje pri zmene hesla históriu a nepovoľuje opakovane použiť rovnaké heslo. Ovplyvňujú to nasledovné konf. premenné:

- `passwordHistoryLength` - počet použitých hesiel používateľa, ktoré sa pamätajú v histórii (predvolene 6).
- `passwordHistoryEnabled` - ak je nastavené na `true` je kontrolovaná v databáze aj história hesiel a nie je povolené pri zmene hesla použiť také, ktoré bolo v minulosti (predvolene `true`).

Pri požiadavke na zmenu hesla sú použité nasledovné premenné:

- `passwordResetValidityInMinutes` - časová platnosť v minútach pre zaslaný odkaz na zmenu hesla (predvolene 30).
- `changePasswordPageUrl` - adresa stránky pre zmenu hesla (predvolene `/components/user/change_password.jsp`).

### 1.1.5. Blokovanie prihlásenia

Po nesprávnej kombinácii mena a hesla WebJET blokuje ďalšie prihlásenie z rovnakej IP adresy. Je možné nastaviť nasledovné konfig. premenné:

- `logonBlockedDelay` - čas v sekundách, počas ktorých nebude možné sa znova prihlásiť po zadaní zlého mena/hesla (predvolene 10).
- `logonBlockedAfterUnsuccessCount` - počet neúspešných prihlásení po ktorých sa aplikuje zdržanie definované v `logonLoginBlockedDelay` (predvolene 5).
- `logonLoginBlockedDelay` - čas v sekundách, počas ktorých nebude možné znova sa prihlásiť po zadaní zlého hesla a `logonBlockedAfterUnsuccessCount` počtu neúspešných prihlásení pre zadané prihlasovacie meno (predvolene 60).

Štandardne sa teda aplikuje hodnota 10 sekúnd ( `logonBlockedDelay` ), ak sa zadá za sebou viac ako 5 krát ( `logonBlockedAfterUnsuccessCount` ) aplikuje sa zdržanie 60 sekúnd ( `logonLoginBlockedDelay` ).

Počas času blokovania prihlásenia sa naďalej nezvyšuje počítadlo neúspešných pokusov a nepredlžuje sa čas, keďže nedochádza vôbec k volaniu kódu prihlasovania.

### 1.1.6. Algoritmus hashovania hesiel

Od verzie `2022.40` sa používa na hashovanie hesiel algoritmus BCrypt v implementácii `org.springframework.security.crypto.bcrypt.BCrypt`.

Možné nastavenia:

- `bcryptSaltRounds` (predvolene 12) - log2 počtu opakovaní saltovania
- `passwordHashAlgorithm` (predvolene `bcrypt`) - meno algoritmu pre hashovanie, možné hodnoty `bcrypt` alebo `sha-512`.

Staršie verzie používali algoritmus `SHA-512` so 100 násobným opakovaním. Staršie hash hodnoty hesla sa zmenia na `bcrypt` algoritmus pri zmene hesla používateľa. Ak chcete vynútiť zmenu algoritmu môžete nastaviť konfig. premennú `passwordAdminExpiryDays` na nenulové hodnotu, čo vyvolá požiadavku na zmenu hesla po prihlásení používateľa.

### 1.1.7. Prihlasovanie do administrácie

Prihlasovanie do administrácie ovplyvňujú už aj vyššie spomenuté konfiguračné premenné:

- `adminEnabledIPs` - obsahuje čiarkou oddelený zoznam IP adries, z ktorých je povolený prístup do `/admin` časti.
- `multidomainAdminHost` - umožňuje nastaviť samostatnú doménovú adresu pre prístup do `/admin` časti, napr. `cms.domena.sk`. Po nastavení bude volanie `/admin` adresy na ostatných doménach vracat chybu 404 - Stránka neexistuje.
- `isGoogleAuthRequiredForAdmin` - zapnutie dvoj faktorového overovania pri prihlásení do administrácie `/admin`.
- `clusterMyNodeType` - v prípade clustra nastavuje režim uzla, len uzly nastavené na hodnotu `full` obsahujú administráciu a umožňujú prihlásenie do nej.
- `auditDontLogUsrlogin` - po nastavení na `true` sa nebude auditovať bežné (nie administrátorské) prihlásenie používateľa. Vhodné na vysoko zaťažný intranet kde to zbytočne zahľucuje audit (predvolene `false`).

Používateľ, ktorý sa úspešne autorizuje musí navyše spĺňať nasledovné kritéria:

- **Schválený používateľ** - účet musí mať zvolenú uvedenú možnosť.
- **Začiatok platnosti** - ak je zadaná hodnota musí byť staršia ako aktuálny dátum.
- **Koniec platnosti** - ak je zadaná hodnota musí byť väčšia ako aktuálny dátum.
- **Povoliť vstup do admin sekcie (správa web sídla)** - účet musí mať povolenú uvedenú možnosť, inak nie je možný prístup do administrácie.

V prípade špeciálnych požiadaviek na prihlasovanie/overovanie používateľa je možné implementovať vlastnú Java triedu prihlasovania a nastaviť ju cez konfig. premennú `adminLogonMethod`. Následne sa použije zadaná Java trieda namiesto štandardného prihlásenia.

Pri prihlasovaní sa pri nesprávnych údajoch **blokuje prihlásenie**.

### 1.1.8. Overovanie voči LDAP serveru

Pri overovaní používateľa voči LDAP serveru je možné nastaviť nasledovné konf. premenné:

- `ldapProviderUrl` - URL adresa LDAP servera pre prihlasovanie cez LDAP v tvare `ldap://ldap.local:389/DC=firma,DC=com??base`.
- `ldapPassword` - prihlasovacie meno technického používateľa pre získanie údajov z LDAP.
- `ldapUsername` - prihlasovacie heslo technického používateľa pre získanie údajov z LDAP.
- `ldapUseSslProtocol` - použije SSL pri komunikácii s LDAP serverom. Je potrebné mať povolené SSL na porte 636 LDAP servera. Ak sa používa `ldapS://`, nechať hodnotu na `false`.
- `NTLMForbiddenURL` - URL adresa zamietnutého prístupu (predvolene `/500.jsp`).
- `NTLMDomainController` - meno doménového radiča.
- `ldapDomainAppend` - ak je potrebné prihlasovanie s celou doménou tu je možné zadať jej doplnenie k zadanému prihlasovaciemu menu používateľa.
- `ldapSecurityPrincipalDn` - nastaví pre LDAP špeciálny `SECURITY_PRINCIPAL` napr. `cn=!USERNAME!,dc=ad,dc=interway,dc=sk` s tým, že `!USERNAME!` zamení za prihlasovacie meno. Pokiaľ je prázdne použije sa `ldapUsername+ldapDomainAppend`.
- `ldapFilter` - prihlasovací filter pre LDAP prihlasovanie s ktorým sa vykoná vyhľadanie konta (predvolene `(&(objectClass=Person)(&(sAMAccountName=!USERNAME!)))`).
- `basicNtlmLogonAttrs` - zoznam atribútov, ktoré sa majú čítať z LDAP servera pri prihlasovaní. Ak je prázdne, overí sa len prihlásenie a používateľ sa neaktualizuje hodnotami v LDAP serveri. Predvolene `mail,title,givenName,sn,streetAddress,l,postalCode,co,company,telephoneNumber,mobile,description,memberOf,distinguishedName`.
- `ntlmDefaultUserPhoto` - ak je zadané na neprázdnu hodnotu a používateľ nemá v LDAP fotografiu nastaví fotku podľa zadanej URL adresy.

Nastavenie práv:

Po prihlásení sa automaticky kontroluje zhoda mena skupiny používateľov a skupiny práv voči skupinám v LDAP (atribút `memberOf`). Ak sa meno zhoduje skupina vo WebJETe sa používateľovi priradí. Okrem toho je možné nastaviť:

- `NTLMAdminGroupName` - meno skupiny v LDAP ktorá identifikuje, že konto má prístup do administrácie (napr. `WebJETAdmins`).
- `passwordProtectedAutoId` - čiarkou oddelený zoznam ID skupín používateľov, ktoré budú priradené automaticky používateľovi po úspešnom prihlásení.

### 1.1.9. Konfigurácia aplikačného servera Tomcat

Predpokladáme, že web stránka/aplikácia bude dostupná cez zabezpečený `https` protokol. Preto je potrebné nastaviť atribút `secure="true"`, [HTTP/AJP konektora \(https://tomcat.apache.org/tomcat-9.0-doc/config/http.html\)](https://tomcat.apache.org/tomcat-9.0-doc/config/http.html), aby session cookie bola dostupná len cez zabezpečený `https` protokol. Nastavenie vykonáte v súbore `tomcat/conf/server.xml`. Atribút `useBodyEncodingForURI="true"` nastavuje rovnaké kódovanie znakov pre URL adresu ako je použité pre telo stránky.

```
<Connector
...
secure="true"
useBodyEncodingForURI="true"
...
/>
```

xml

ak použijete nezabezpečený `HTTP` protokol nebude session cookie v prehliadači akceptovaná a session nebude držaná (prejaví sa to opakovaným zobrazením prihlasovacieho okna hneď po zadaní správnych prihlasovacích údajov).

Aby sa pri zobrazení chyby nezobrazila verzia aplikačného servera `Tomcat` a `Stack Trace` je potrebné v `server.xml` do `<Host>` elementu pridať konfiguráciu [ErrorReportValve \(https://tomcat.apache.org/tomcat-9.0-doc/config/valve.html#Error\\_Report\\_Valve\)](https://tomcat.apache.org/tomcat-9.0-doc/config/valve.html#Error_Report_Valve):



```
<Host ...>
  <Valve className="org.apache.catalina.valves.ErrorReportValve"
    showReport="false"
    showServerInfo="false" />
</Host>
```

v prípade potreby môžete vytvoriť aj statickú html stránku v kódovaní `utf-8` s chybovou správou a nakonfigurovať ju ako:

```
<Valve className="org.apache.catalina.valves.ErrorReportValve"
  errorCode.400="webapps/error400.html"
  errorCode.0="webapps/error0thers.html"
  showReport="false"
  showServerInfo="false" />
```

V konfiguračnom súbore `server.xml` odporúčame správne nastaviť možnosť `defaultHost`. Útočníci môžu modifikovať hlavičku `Host` a teda smerovať požiadavku z internetu napr. na administratívny host, ktorý nemusel byť z internetu dostupný (ak na jednom aplikačnom serveri beží administratívny aj verejný uzol clustra). Príkladom je použitie `localhost`, ktoré môže byť priradené k administratívnejmu serveru a teda upravená požiadavka môže skončiť na administratívnom node.

Hodnotu `defaultHost` odporúčame smerovať na neexistujúci `<Host>` element, v takom prípade vyhlási aplikačný server chybu, že taký `host` nepozná. Aplikačný server teda nespracuje neznáme domény. Nevýhoda takéhoto riešenia je, že po pridaní novej domény je potrebné ju pridať ako `<Alias>` aj do aplikačného servera.

Ak používate Load Balancer je potrebné zabezpečiť, aby na aplikačné servre posielal len známe (whitelist) domény. Pre neznáme domény musí odpovedať chybou.

```
<Engine name="Catalina" defaultHost="localhost">

  <Host name="localhost"...>
    <Alias>admin.domain.eu</Alias>
  </Host>
```

### 1.1.10. Notifikácie pri zmene

Odporúčame nastaviť notifikácie posielané bezpečnostnému technikovi na nasledovné typy udalostí:

- `CONF_UPDATE` a `CONF_DELETE` - zmena/zmazanie konfiguračnej premennej
- `PROP_UPDATE` a `PROP_DELETE` - zmena/zmazanie prekladového kľúča (cez prekladový kľúč je možné vkladať aj JavaScript kód)

Notifikácie nastavíte v administrácii v časti Audit->Notifikácie. Bezpečnostný technik bude mať prehľad o týchto zmenách a v prípade podozrenia na útok môže zareagovať.

### 1.1.11. Bezpečnosť servera

Dôležitá je aj bezpečnosť samotného servera a použitého softvéru. Aktualizujte softvér na aktuálne podporované verzie. Vhodné je inštalovať na server aj antivírus, ktorý bude kontrolovať nahrávané súbory a v prípade detekcie vírusu v súbore zamedzí k tomuto súboru prístup.

## 1.2. Nastavenie Load Balancera

Ak je pred aplikačnými servermi predradený Load Balancer je potrebné zabezpečiť:

- Smerovať na aplikačné servery len definované domény, aby nemohol nastať útok modifikovaním `Host` hlavičky. Load Balancer nesmie povoliť poslanie neznámej domény na aplikačný server.
- WebJET preberá nastavenie IP adresy z HTTP hlavičky `X-Forwarded-For` pri nastavení konfiguračnej premennej `serverBeyondProxy=true`. Je teda potrebné zabezpečiť, aby takáto HTTP hlavička neprechádzala z internetu ale Load Balancer ju vždy prepísal na korektnú hodnotu - IP adresu návštevníka. To isté platí pre HTTP hlavičku `x-forwarded-proto`. Nesprávne nastavenie hlavičky môže viesť k sprístupneniu častí, ktoré sú povolené len pre špecifické IP adresy, ako napríklad administrácia.

## 1.3. Nastavenie WAF

Ak je pred aplikačným serverom predradený `Web Application Firewall/WAF` je potrebné nastaviť **výnimky pre administráciu**. Niektoré HTTP požiadavky v administrácii môžu byť detegované ako útok typu XSS/SQL Injection, pretože HTTP požiadavka môže odosielať JavaScript kód, alebo SQL príkaz. Príkladom je ukladanie web stránky, kde v poli HTML kód do hlavičky môže byť vložený potrebný JavaScript kód, alebo ukladanie záznamov v aplikácii Skripty, kde sa priamo vkladá JavaScript kód.

Ideálne riešenie je použiť cluster riešenie s dedikovaným CMS uzlom v lokálnej sieti, ktorý je nedostupný z vonkajšieho prostredia. Pre tento prípad je možné WAF pre CMS nod nepoužiť.

Administrácia používa REST služby začínajúce na URL adresu `/admin/rest`, viď odporúčania pre [pravidlá URL adries](https://docs.webjetcms.sk/latest/sk/custom-apps/spring/rest-url) (<https://docs.webjetcms.sk/latest/sk/custom-apps/spring/rest-url>). Na WAF je potrebné nastaviť výnimky pre URL adresy začínajúce na:

- `/admin/rest/web-pages` - ukladanie web stránok
- `/admin/rest/components/insert-script` - aplikácia Skripty
- `/admin/v9/settings/translation-keys` - prekladové kľúče - v niektorých prípadoch môže byť potrebné vkladať HTML kód do prekladového kľúča
- `/admin/rest/settings/configuration` - konfigurácia, platí podobné ako pre prekladové kľúče
- `/admin/searchall.jsp` - vyhľadávanie v administrácii, môže byť potrebné hľadať aj HTML/JavaScript výraz
- `/admin/replaceall.jsp` - nahradenie výrazu v administrácii, platí podobné ako pre vyhľadávanie
- `/admin/updatedb.jsp` - vykonanie zadaného SQL príkazu

Ďalšie URL adresy je vhodné nastaviť na základe používaných aplikácií.

## 1.4. Riešenie bezpečnostných nálezov

- `Sensitive Data Exposure`

Prostredníctvom chybových odpovedí so servera sa podarilo odhaliť typ a verziu použitého webového servera.

Riešenie: overte nastavenie HTTP hlavičky `Server`, vo WebJETe sa dá prestaviť v konfiguračnej premennej `serverName`, viď vyššie.

- `RCE via uploaded JSP file`

WebJET CMS umožňuje nahrávanie ľubovoľných súborov vrátane súborov typu JSP, ktoré umožňujú vykonávanie ľubovoľných príkazov na bežiacom serveri.

Chybe sa dá zabrániť nastavením práv pre nahrávanie súborov, alebo úplným zamedzením zápisu programových súborov.

Riešenie: upravte nastavenie práv pre nahrávanie súborov cez konfiguračné premenné `FCKConfig.Upload*`, viď vyššie.

- `MaliciousFileUpload`

Na serveri chýba antivírusová kontrol, je teda možné na server nahrať škodlivé súbory.

Riešenie: nainštalujte na server antivírus.

- Missing Secure cookie flag

Session cookie ( JSESSIONID ) nemá nastavený bezpečnostný atribút Secure .

Riešenie: skontrolujte a nastavte secure atribút v súbore [server.xml](https://tomcat.apache.org/tomcat-9.0-doc/config/http.html) (<https://tomcat.apache.org/tomcat-9.0-doc/config/http.html>) aplikačného servera Tomcat, viď vyššie.

- Missing HTTP Strict Transport Security policy

Aplikácia nenastavuje HTTP hlavičku Strict Transport Security .

Riešenie: hodnotu hlavičky Strict Transport Security ([https://en.wikipedia.org/wiki/HTTP\\_Strict\\_Transport\\_Security](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security)) je možné nastaviť v konfiguračnej premennej strictTransportSecurity=max-age=31536000 ; includeSubDomains , viď vyššie.

- Stored XSS cez SVG obrázok

SVG súbor umožňuje vložiť do tela aj JavaScript kód, v prípade priameho zobrazenia takéhoto súboru v prehliadači sa JavaScript kód vykoná (pri štandardnom vložení cez img sa kód nevykoná a zobrazenie je bezpečné).

Riešenie: obmedziť možnosť nahrávania SVG súborov, viď nastavenie práv vyššie. Ako ochranu WebJET CMS generuje pre súbory typu SVG HTTP hlavičku Content-Security-Policy s hodnotou default-src 'self' , ktorá zamedzí vykonaniu javascript kódu ([https://github.com/digininja/svg\\_xss](https://github.com/digininja/svg_xss)) pri priamom zobrazení obrázku. Hodnota je nastaviteľná cez konfiguračnú premennú contentSecurityPolicySvg .

Pre overenie správania vytvorte SVG súbor s nasledovným obsahom, nahrajte ho do WebJET CMS a vložte do testovacej stránky a overte jeho zobrazenia a (ne)vykonanie XSS útoku:

```
<?xml version="1.0" standalone="no"?>
<!DOCTYPE svg PUBLIC "-//W3C//DTD SVG 1.1//EN" "http://www.w3.org/Graphics/SVG/1.1/DTD/svg11.dtd">
<svg version="1.1" baseProfile="full" xmlns="http://www.w3.org/2000/svg"> <polygon id="triangle" points="0,0
0,100 100,0" fill="#3e70b7"
stroke="#004400"/>
<script type="text/javascript">
alert("SVG XSS");
</script>
</svg>
```

- Stored XSS cez úpravu prekladových kľúčov

Cez prekladové texty je redaktor schopný vykonať útok typu Cross Site Scripting voči ostatným návštevníkom webu, alebo iným administrátorom.

Prekladové kľúče sa používajú aj na vkladanie HTML kódu (napr. odkazu na obchodné podmienky v kalkulačke, zvýraznenie tučným písmom, nastavenie CSS štýlov), preto táto aplikácia technicky umožňuje vkladať aj HTML/JavaScript kód (jedná sa o vlastnosť, nie chybu). Treba si uvedomiť, že redaktor môže vložiť JavaScript kód aj priamo v editore stránok, nie je zásadný dôvod mu v tom zabráňovať aj v editácii prekladových kľúčov.

Riešenie: Minimalizovať počet používateľov s prístupom k aplikácii Prekladové texty. Zároveň používatelia, ktorí nemajú právo "Editácia textov - zobrazenie všetkých textov" majú obmedzené možnosti editácie. Môžu editovať len vybrané kľúče (nastavené cez konf. premennú propertiesEnabledKeys ) a zároveň upravená hodnota je filtrovaná a povolí len definované HTML značky a atribúty. Tie sa nastavujú v konf. premennej propAllowedTags kde sú štandardne povolené značky p,div,a,sub,sup,br,strong a atribúty v konf. premennej propAllowedAttrs kde sú štandardne povolené atribúty href,src,style,class,rel . Ak chcete úplne zabrániť možnosti vkladania HTML kódu pre používateľov bez oprávnenia "Editácia textov - zobrazenie všetkých textov" môžete nastaviť konf. premennú propAllowedTags na prázdnu hodnotu (alebo znak - ). Nastavením na znak \* sa ochrana vypne.

Zároveň ako ďalšiu ochranu odporúčame nastaviť notifikácie pri zmene na bezpečnostného technika, viď vyššie.

- **Insecure Deserialization**

Import web stránok obsahuje .xml dokumenty so serializovanými java objektami. Tieto .xml dokumenty je však možné zmeniť a podstrčiť vlastné serializované java objekty typu `<object class="java.lang.Runtime" method="getRuntime">`, ktoré vykonajú zadanú operáciu priamo na serveri.

Pre úspešnú exploitáciu je potrebné upraviť konf. premennú `XMLDecoderAllowedClasses`, ktorá obsahuje zoznam povolených deserializovaných objektov a pridať tam hodnotou `java.lang.Runtime`.

Riešenie: bežný používateľ nesmie mať oprávnenia na úpravu konfiguračných premenných, tie by mala upravovať len vyhradená osoba. Ako ďalšiu ochranu sme priamo do kódu (bez možnosti upraviť tento zoznam) doplnili nepovolené typy objektov, ktoré nie je možné cez konfiguráciu pridať (povoliť).

- **Cookies: Set the 'SameSite' flag as a counter measure to cross-site request forgery**

Pre `cookies` je možné nastaviť atribút `SameSite` (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite>) pre zamedzenie posielania cookies pri CSRF útoku (zamedzenie posielania cookies iným doménam).

Aktuálne sa v `servlet-api` pripravuje podpora nastavenia tejto hodnoty vo verzii 5.x, čo môže znamenať dlhé čakanie na priamu podporu pri programovaní. Pri použití Apache Tomcat je ale možné túto hodnotu nastaviť v konfigurácii pomocou `CookieProcessor` (<https://tomcat.apache.org/tomcat-8.5-doc/config/cookie-processor.html>), ktorý v štandardnej implementácii umožňuje hodnotu nastaviť:

```
<Context>
...
<CookieProcessor sameSiteCookies="strict"/>
</Context>
```

xml

## 2. Kontrola zraniteľností knižníc

Pomocou nástroja **OWASP Dependency-Check** (<https://jeremylong.github.io/DependencyCheck/index.html>) môžete jednoducho kontrolovať zraniteľnosti v Java a JavaScript knižniciach web aplikácie. Tie odporúčame kontrolovať na pravidelnej báze.

Ak máte prístup k zdrojovému kódu/gradle projektu môžete spustiť analýzu priamo pomocou **gradlew príkazu** (<https://docs.webjetcms.sk/latest/sk/developer/backend/security>).

Nástroj je ale možné spustiť aj nad vygenerovaným `war` archívom web aplikácie. Nainštalujte si verziu nástroja pre **príkazový riadok** (<https://jeremylong.github.io/DependencyCheck/dependency-check-cli/index.html>).

Následne môžete spustiť kontrolu pomocou príkazu:

```
dependency-check --project "Meno projektu" --suppression dependency-check-suppressions.xml --suppression
dependency-check-suppressions-project.xml --scan build/libs/*.war
```

sh

parametrami sa nastavuje:

- `--project` - meno projektu, ktoré sa zobrazí v reporte.
- `--suppression` - cesta k súborom s výnimkami (<https://docs.webjetcms.sk/latest/sk/developer/backend/security>), typicky je tento súbor súčasťou git repozitára.
- `--scan` - cesta k súboru/adresáru, ktorý sa má analyzovať.

Výsledkom je súbor `dependency-check-report.html` v aktuálnom adresári.



Dependency-Check is an open source tool performing a best effort analysis of 3rd party dependencies; false positives and false negatives may exist in the analysis performed by the tool. Use of the tool and the reporting provided constitutes acceptance for use in an AS IS condition, and there are NO warranties, implied or otherwise, with regard to the analysis or its use. Any use of the tool and the reporting provided is at the user's risk. In no event shall the copyright holder or OWASP be held liable for any damages whatsoever arising out of or in connection with the use of this tool, the analysis performed, or the resulting report.

[How to read the report](#) | [Suppressing false positives](#) | [Getting Help: github issues](#)

♡ [Sponsor](#)

**Project: Meno projektu**

Scan Information ([show all](#)):

- dependency-check version: 6.5.3
- Report Generated On: Tue, 15 Feb 2022 16:51:25 +0100
- Dependencies Scanned: 3285 (3262 unique)
- Vulnerable Dependencies: 1
- Vulnerabilities Found: 7
- Vulnerabilities Suppressed: 89
- ...

## Summary

Display: [Showing Vulnerable Dependencies \(click to show all\)](#)

Dependency	Vulnerability IDs	Package	Highest Severity	CVE Count	Confidence	Evidence Count
webjet@v9.war: webjet-8.9-SNAPSHOT-admin.jar: ckeditor.js		pkg-javascript/ckeditor@4.5.0-beta	low	7		3

## 3. Aktualizácia WebJETu

Sekcia Aktualizácia WebJETu slúži k aktualizácií verzií WebJETu. Ľavá časť obrazovky zobrazuje zoznam dostupných verzií WebJETu na ktoré sa dá Váš WebJET aktualizovať. Práve aktuálna verzia Vášho WebJETu je v zozname označená ikonou

Pri kliknutí na jednotlivé verzie sa v pravej časti obrazovky zobrazí zoznam všetkých zmien, ktoré vybraná verzia prináša.

**Aktualizácia WebJETu**

[Aktualizovať](#) [Kontaktovať podporu](#) Zostávajúci počet povolených aktualizácií pre vašu licenciu: 58.

Verzia	Status
2024.0-SNAPSHOT	✓
2024.0	
2023.52	
2023.52-java17	
2023.40-SNAPSHOT	
2023.40-SNAPSHOT-java17	
<b>2023.40</b>	✓
2023.18-SNAPSHOT	
2023.18-SNAPSHOT-java17	
2023.18	
2023.0-SNAPSHOT	
2023.0	
2022.52	
2022.40	

**Verzia 2023.40**

**Stabilizovaná verzia 2023.40, nepribúdajú do nej denné zmeny.**

- Pre zjednodušenie aktualizácie môžete použiť skript `/admin/update/update-2023-18.jsp` pre kontrolu a opravu JSP súborov. Zákaznícke Java triedy je potrebné nanovo skompilovať a opraviť chyby z dôvodu zmeny API.
- Vo vašom projekte zmažte súbor `/WEB-INF/struts-config.xml` aby sa použil aktuálny súbor z WebJETu (z jar súboru).

**UPOZORNENIE:** z dôvodu veľkého počtu zmien v jar knižniciach bude počas aktualizácie potrebné vykonať reštart aplikačného servera. Presvedčte sa pred aktualizáciou, že máte dostupnú technickú pomoc pre reštart.

Verzia 2023.40 pridáva možnosť **vyhľadávania v prieskumníku/súboroch**, možnosť použiť **video banner**, zlepšuje používateľské rozhranie, zrychľuje načítanie dát vo web stránkach. **Banner** pridáva nastavenia obmedzení pre **zobrazenie len v zadaných web stránkach a priečiňkoch**. Nová aplikácia **HTTP hlavičky** umožňuje nastavovať HTTP hlavičky pre zadané URL adresy. **Médiám** sme pridali **voliteľné polia**. Zrkadlenie štruktúry podporuje **preklad aj tela web stránky** a zlepšuje detekciu zmien. Do nového dizajnu prerobené aplikácie **Monitorovanie servera**, **SEO**, **Novinky**, **Diskusia**. Verzia je zameraná aj na odstránenie starých častí kódu, z toho dôvodu je potrebné nanovo **skompilovať vaše triedy a upraviť JSP súbory**.

**Prelomové zmeny**

Táto verzia prináša viaceré zmeny, ktoré nemusia byť spätne kompatibilné:

**! Upozornenie:** aktualizáciu WebJETu vykonávajte len v prípade ak viete čo robíte. Pred aktualizáciou kontaktujte vášho poskytovateľa hostingu pre prípadnú podporu. Môže sa stať, že po aktualizácii WebJET nenašartuje správne a bude nutný reštart servera.

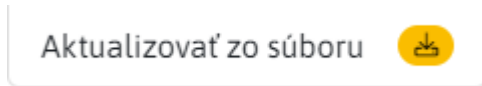
Ak váš projekt obsahuje doplnkové JAR knižnice je potrebné ich umiestniť aj do priečinka `/WEB-INF/lib-custom/`. Počas aktualizácie je plne nahradený priečinok `/WEB-INF/lib/` a teda vaše knižnice by boli zmazané. To môže mať za následok neschopnosť spustenia po reštarte. Ak taká situácia nastane skopírujte chýbajúce knižnice do `/WEB-INF/lib/` zo zálohy.

### 3.1. Aktualizácia na konkrétnu verziu

Pre aktualizovanie WebJETu na konkrétnu verziu je potrebné zvoliť želanú verziu a následne použiť tlačidlo pre spustenie aktualizácie

### 3.2. Aktualizovanie zo súboru

Podporovaná je taktiež možnosť využiť aktualizovanie zo súboru. Táto možnosť sa dá vybrať taktiež v ľavom menu ako



Následne budete vyzvaný k výberu a následnému nahraťiu súboru pomocou tlačidla **Nahrať súbor** . Ak bude súbor úspešne nahraťý, budete vyzvaný k spusteniu samotnej aktualizácie pomocou tlačidla .

Aktualizácia WebJETu

Kontaktovať podporu

Zostávajúci počet povolených aktualizácií pre vašu licenciu: 58.

2024.0-SNAPSHOT

2024.0

2023.52

2023.52-java17

2023.40-SNAPSHOT

2023.40-SNAPSHOT-java17

2023.40

2023.18-SNAPSHOT

2023.18-SNAPSHOT-java17

2023.18

2023.0-SNAPSHOT

2023.0

2022.52

2022.40

2022.18

2022.0-SNAPSHOT

Pre spustenie aktualizácie zo súboru musíte najprv nahráť aktualizčný súbor.

Aktualizačný súbor

Vybrať súbor

Nie je vybratý žiadny súbor

Nahráť súbor

## 4. Audit

Aplikácia Audit je nástroj pre sledovanie zmien v systéme. Sekcia Audit -> Vyhľadávanie umožňuje zobrazit' a filtrovať jednotlivé zaznamenané hodnoty. Filtrovanie je možné podľa typu auditných záznamov, času, používateľa atď.

**WwJET CMS**
Pomocník 🔍 Tester Playwright ↕ ➡


---

Prehľad

Úvod  
 Štatistiky  
 Monitorovanie servera  
 Audit

• Vyhľadávanie  
 • Zoznam notifikácií  
 • Zmenené stránky  
 • Čaká na publikovanie  
 • Úroveň logovania  
 • Posledné logy

Poslať správu

📁 webjet9.tau27.iwaysk

### Audit

Id	Dátum a čas	Typ	Používateľ	Opis
<input type="checkbox"/> 1553510	16.01.2024 15:23:26	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...
<input type="checkbox"/> 1553509	16.01.2024 15:20:00	CRON		Cron task executed: sk.iway.icwm.calendar.CalendarDB [] node=webjet4b S...
<input type="checkbox"/> 1553508	16.01.2024 15:20:00	CRON		Cron task executed: sk.iway.icwm.calendar.CalendarDB [] node=SWB88 Serv...
<input type="checkbox"/> 1553507	16.01.2024 15:20:00	CRON		Cron task executed: sk.iway.icwm.calendar.CalendarDB [] node=webjet4b S...
<input type="checkbox"/> 1553506	16.01.2024 15:20:00	CRON		Cron task executed: sk.iway.icwm.calendar.CalendarDB [] node=SWB88 Serv...
<input type="checkbox"/> 1553505	16.01.2024 15:07:35	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...
<input type="checkbox"/> 1553504	16.01.2024 15:07:05	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...
<input type="checkbox"/> 1553503	16.01.2024 15:06:38	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...
<input type="checkbox"/> 1553502	16.01.2024 15:04:14	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...
<input type="checkbox"/> 1553501	16.01.2024 15:02:33	USER_LOGON	Tester Playwright	LogonAction - user (ADMIN) successfully logged: name=tester node=SWB88 ...

Záznamy 1 až 10 z 160.322
 

1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
16
17
18
19
...
16033

## 5. Typy auditných záznamov

Každý auditný záznam automaticky zaznamená dátum a čas, ID prihláseného používateľa, IP adresu a ak je povolený reverzný DNS server aj meno počítača. Do textu auditného záznamu sa automaticky vkladá meno uzla clustra, URI adresa, doména a hodnota http hlavičky User-Agent.

- **ADMINLOG\_NOTIFY** - zmena v zozname notifikácií v aplikácii Audit.
- **BANNER** - operácie v aplikácii Bannerový systém
- **BASKET** - operácie v aplikácii Elektronický obchod
- **CALENDAR** - operácie v aplikácii Kalendár udalostí
- **CONF\_DELETE** - zmazanie konfiguračnej premennej, zaznamená jej meno
- **CONF\_UPDATE** - zmena alebo pridanie konfiguračnej premennej (v sekcii Nastavenia), zaznamená meno, aktuálnu hodnotu a novú hodnotu premennej
- **COOKIE\_ACCEPTED** - akceptovanie cookie na web stránke
- **COOKIE\_REJECTED** - zamietnutie použitia cookies na web stránke
- **CRON** - zaznamená beh úloh na pozadí, ak je zaškrtnutá možnosť Auditovať. Ukladá aj chyby pri vykonávaní úloh (ak nastanú), v takom prípade zaznamená **Stack Trace**.
- **DATA\_DELETING** - zaznamenáva vykonanie mazania dát v Nastavenia-Mazanie dát. Zaznamená kľúč ktorý sa v cache zmazal, alebo **ALL** pre zmazanie všetkého. Pri mazaní cache obrázkov zaznamená cestu k adresáru. Pri mazaní persistent cache zaznamená ID záznamu.
- **DMAIL** - aplikácia Hromadný email
- **DMAIL\_AUTOSENDER** - používa sa v špeciálnej situácii automatického odosielania hromadného emailu
- **DMAIL\_BLACKLIST** - zmena v Hromadný email->Odhlásené e-maily
- **DMAIL\_DOMAINLIMITS** - zmena v Hromadný email->Doménové limity
- **EXPORT\_WEBJET** - nepoužíva sa
- **EXPORT** - operácie v aplikácii Export dát (pridanie, zmena, zmazanie exportu dát)
- **FILE\_CREATE** - vytvorenie súboru alebo adresáru, zaznamená cestu
- **FILE\_DELETE** - zmazanie súboru alebo adresáru, zaznamená cestu
- **FILE\_EDIT** - premenovanie, alebo editácia súboru, zaznamená cestu
- **FILE\_SAVE** - uloženie súboru, napr. pri jeho kopírovaní / presúvaní a podobne. Zaznamená cestu k súboru
- **FILE\_UPLOAD** - nahratie súboru do WebJETu, či už cez klasické nahratie, alebo Drag & Drop. Typicky zaznamenáva cestu k nahratému súboru.
- **FORMMAIL** - odoslanie formuláru. Zaznamená úspešné odoslanie s hlásením **FormMail formName:** meno formuláru, zoznam príjemcov a **referer**. Pri neúspechu zaznamená dôvod neodoslania s hlásením **ERROR: formName:** meno formuláru, **fail:** dôvod neodoslania. Zaznamenáva aj detekciu spamu hlásením **detectSpam TRUE:** dôvod detekcie ako spam.
- **FORM\_ARCHIVE** - archivácia formuláru, zaznamená meno formuláru
- **FORM\_DELETE** - zmazanie formuláru, zaznamená meno formuláru a prípadne ID ak sa jedná o zmazanie jedného záznamu
- **FORM\_EXPORT** - export formuláru cez záložku Exportovať, aktuálne sa nezaznamenáva univerzálny export cez tlačítka pod tabuľkou. Podľa tohto záznamu sa určuje dátum posledného exportu pre možnosť exportu od posledného exportu.
- **FORM\_REGEX** - zmena v Formuláre->Regulárne výrazy
- **FORM\_VIEW** - nepoužíva sa
- **FORUM\_SAVE** - zaznamená detekciu vulgarizmu v diskusnom fóre
- **FORUM** - operácie v aplikácii Diskusia
- **GALLERY** - zmeny v aplikácii Galéria - vytvorenie adresára, pridanie/zmazanie fotky
- **GDPR\_FORMS\_DELETE** - aplikácia GDPR, mazanie starých formulárov
- **GDPR\_USERS\_DELETE** - aplikácia GDPR, mazanie starých používateľov
- **GDPR\_BASKET\_INVOICES\_DELETE** - aplikácia GDPR, mazanie starých objednávok z elektronického obchodu
- **GDPR\_EMAILS\_DELETE** - aplikácia GDPR, mazanie starých emailov
- **GDPR\_REGEX** - aplikácia GDPR, správa regulárnych výrazov
- **GDPR\_DELETE** - aplikácia GDPR, nastavenie mazania dát
- **GDPR\_COOKIES** - aplikácia GDPR, správa cookies
- **GROUP** - vytvorenie / uloženie / zmazanie adresára v sekcii Web stránky
- **HELPPESK** - nepoužíva sa

- **HELP\_LAST\_SEEN** - používa sa na evidenciu dátumu zobrazenia sekcie Čo je nové v pomocníkovi. Pri prihlasovaní sa v tejto sekcii hľadá najnovší súbor a porovnáva sa voči zaznamenanému dátumu v Audite. Ak existuje novší súbor, zobrazí sa po prihlásení vyskakovacie okno pomocníka so sekciou Čo je nové.
- **IMPORTXLS** - importu Excel súboru, používa sa v zákazníckych implementáciách. Zaznamenáva cestu k importovanému súboru a jeho veľkosť
- **IMPORT\_WEBJET** - nepoužíva sa
- **INIT** - inicializácia WebJETu (štart), zaznamenáva cestu k adresáru v ktorom bol WebJET na aplikačnom serveri spustený a číslo verzie WebJETu
- **INQUIRY** - operácie v aplikácii Anketa
- **INQUIRY** - pridanie otázky v aplikácii Anketa, zaznamenaná text otázky
- **INSERT\_SCRIPT** - zmena v aplikácii Skripty
- **INVENTORY** - operácie v aplikácii Majetok
- **JSPERROR** - chyba pri vykonávaní JSP súboru pri zobrazení web stránky, zaznamenaná **Stack Trace** chyby
- **MEDIA** - operácia s Médiami (karta Média vo web stránke).
- **MEDIA\_GROUP** - aplikácia správa skupín médií.
- **PAGE\_DELETE** - zmazanie, presun do koša, alebo požiadanie o zmazanie stránky, zaznamenaná ID stránky
- **PAGE\_UPDATE** - zaznamenáva zmeny v stránke mimo štandardného uloženia v editore - hromadné operácie v zozname stránok
- **PAYMENT\_GATEWAY** - volanie platobnej brány v aplikácii Elektronický obchod
- **PEREX\_GROUP\_CREATE** - vytvorenie perex skupiny, zaznamenaná jej meno
- **PEREX\_GROUP\_DELETE** - zmazanie perex skupiny, zaznamenaná jej meno a ID
- **PEREX\_GROUP\_UPDATE** - zmena perex skupiny, zaznamenaná jej meno
- **PERSISTENT\_CACHE** - zmena v Mazanie dát->Persistent cache objekty
- **PROP\_DELETE** - zmazanie prekladového textu, zaznamenaná jazyk a kľúč
- **PROP\_UPDATE** - editácia prekladového textu (v sekcii Nastavenia), zaznamenaná jazyk, kľúč a hodnotu
- **PROXY** - operácie v aplikácii proxy
- **QA** - operácie v aplikácii Otázky a odpovede
- **REDIRECT\_CREATE** - vytvorenie nového presmerovania (url alebo domény)
- **REDIRECT\_DELETE** - zmazanie presmerovania (url alebo domény), zaznamenaná zdroj a pre doménu aj cieľ presmerovania
- **REDIRECT\_UPDATE** - zmena presmerovania (url alebo domény), zaznamenaná zdrojovú a cieľovú adresu
- **RUNTIME\_ERROR** - zaznamenaná chýbajúcu šablónu pre zobrazenie stránky
- **SAVEDOC** - uloženie web stránky v Editore, zaznamenáva aj žiadosti o schválenie. Zaznamenáva titulok stránky, ID stránky a ID v histórii
- **SENDMAIL** - odoslanie emailu (mimo formulárov), zaznamenaná email odosielateľa, príjemcu a predmet emailu
- **SE\_SITEMAP** - generovanie súboru `/sitemap.xml`, zaznamenaná ID adresára pre ktorý sa mapa stránky generuje a obsah hlavičky User-Agent
- **SQLERROR** - databázová chyba, zaznamenaná SQL chybu, zdroj chyby a **Stack Trace**
- **TEMPLATE\_DELETE** - zmazanie šablóny, zaznamenaná meno zmazanej šablóny
- **TEMPLATE\_INSERT** - vytvorenie novej šablóny, zaznamenaná jej meno
- **TEMPLATE\_UPDATE** - zmena v šablóne, zaznamenaná zoznam zmenených polí
- **TEMPLATE\_GROUP** - zmena v skupine šablón
- **TIP** - operácie v aplikácii Tip dňa
- **TOOLTIP** - zmena v aplikácii Tooltip
- **UPDATEDB** - vykonanie zmeny v databáze cez admin konzolu
- **USER\_AUTHORIZE** - autorizácia používateľa (schválenie prístupu do zaheslovanej sekcie). Zaznamenáva ID zmazaného používateľa, ak je známe aj jeho `login` a meno.
- **USER\_CHANGE\_PASSWORD** - audituje zmenu hesla používateľa. Na základe dátumu sa počíta interval zmeny hesla (ak je nastavený)
- **USER\_DELETE** - zmazanie používateľa. Zaznamenáva ID zmazaného používateľa, ak je známe aj jeho `login` a meno.
- **USER\_EDIT** - zaznamenaná udalosť otvorenia editácie používateľa, nejedná sa ešte o jeho uloženie. Zaznamenaná ID používateľa, `login` a meno.
- **USER\_GROUP\_DELETE** - zmazanie skupiny používateľov, zaznamenaná meno skupiny a jej ID
- **USER\_GROUP\_INSERT** - vytvorenie novej skupiny používateľov, zaznamenaná meno novej skupiny a jej typ
- **USER\_GROUP\_UPDATE** - uloženie skupiny používateľov, zaznamenaná meno skupiny a zoznam zmien
- **USER\_INSERT** - vytvorenie nového používateľa (alebo nová registrácia v zaheslovanej sekcii). Zaznamenaná ID používateľa, `login` a meno.



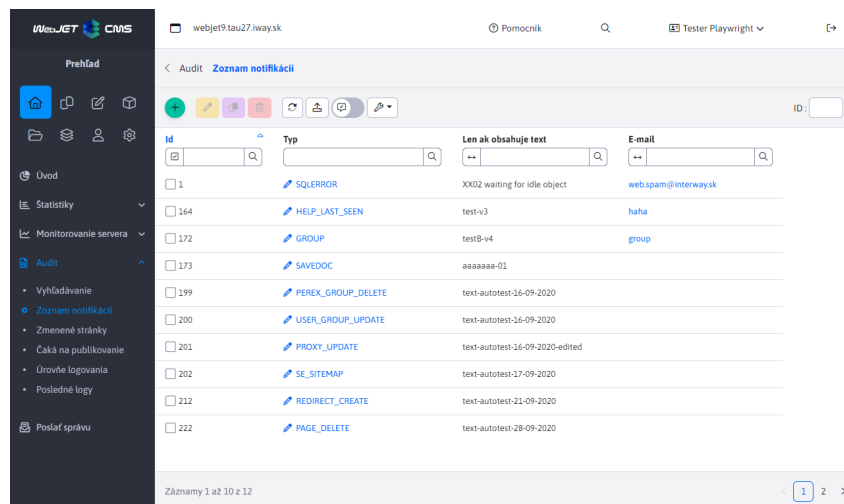
- **USER\_LOGOFF** - odhlásenie používateľa kliknutím na ikonu odhlásenia, zaznamenaná prihlasovacie meno a informáciu o tom, či sa jedná o administrátora alebo registrovaného návštevníka
- **USER\_LOGON** - prihlásenie používateľa, zaznamenaná prihlasovacie meno a informáciu o tom, či sa jedná o administrátora alebo registrovaného návštevníka. Zaznamenaná aj udalosť zadania neplatného hesla, ak používateľ nie je autorizovaný alebo prihlasovacie meno je neznáme
- **USER\_PERM\_GROUP** - operácie so skupinami práv, zaznamenaná meno skupiny a pri zmene zoznam zmien
- **USER\_SAVE** - zaznamenáva zmeny v používateľovi v zaheslovanej sekcii (ak obsahuje formulár pre zmenu údajov)
- **USER\_UPDATE** - uloženie existujúceho používateľa. Zaznamenáva aktuálne nastavenie práv a zmeny v zadaných údajoch
- **WEB\_SERVICES** - volanie zákazníckych **WebServices** (použitie záleží od implementácie pre konkrétneho zákazníka)
- **XSRF** - XSRF útok na server (nepovolený referer header), zaznamenaná hodnotu doménového mena z **referer** hlavičky
- **XSS** - XSS útok na server alebo priame (nepovolené) volanie JSP súboru. Zaznamenaná URL adresu alebo výraz kvôli ktorému sa útok vyhodnotil (napr. nepovolený token v URL, nepovolené HTTP metóda). Zaznamenáva aj ukradnutie cookie (zmena IP adresy session).

## 6. Špeciálny formát auditu

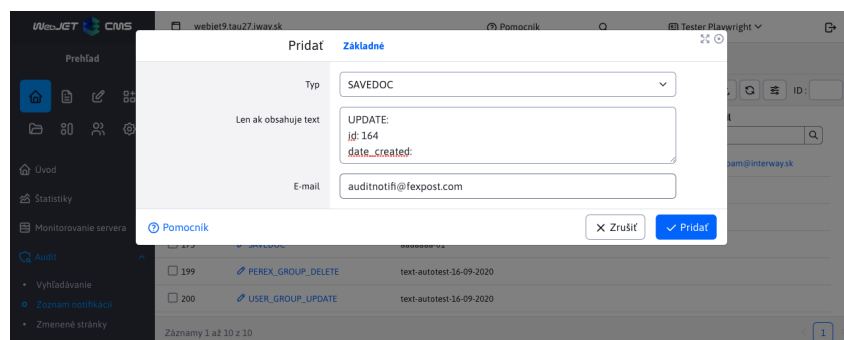
V prípade potreby je možné do WebJETu doplniť kód, ktorý audit záznamy bude ukladať do špeciálneho súboru, alebo posilať na určenú službu. Je potrebné nastaviť konf. premennú `adminLogCustomLogger` na Java triedu, ktorá implementuje triedu `sk.iway.iwcm.AdminLogCustomLogger`. Pri každom zápise sa volá metóda `addLog(logType, requestBean, descriptionParam, timestamp)`

## 7. Zoznam notifikácií

V menu položke Zoznam notifikácií je možné nastaviť email notifikácie pri určitých udalostiach / chybách systému. Odporúčame nastaviť notifikáciu pre udalosti typu **XSS** a **SQLERROR**.



V editore je možné nastaviť aj doplnkový text, ktorý chyba musí obsahovať, aby bola odoslaná na zadaný email.



## 8. Zmenené stránky

V menu položke Zmenené stránky je vidieť zoznam zmenených stránok, zoradený od poslednej zmenenej. S týmito stránkami viete pracovať rovnako ako v sekcii [Zoznam web stránok](https://docs.webjetcms.sk/latest/sk/redactor/webpages/README) (<https://docs.webjetcms.sk/latest/sk/redactor/webpages/README>).

Zobrazené sú všetky stránky bez ohľadu na práva používateľa na stromovú štruktúru stránok a zvolenú doménu.

ID	Stav	Názov web stránky	Meno autora	Posledná zmena	Cesta
80282		Marek_TEST	WebJET Administrátor	16.01.2024 14:25:10	/jet portal 4/Úvodná stránka/Test podar
80284		audit-awaiting-publish-webpage	Tester Playwright	16.01.2024 14:07:24	/test/audit-awaiting-publish-webpage
80283		audit-changed-webpage	Tester Playwright	16.01.2024 13:39:06	/test/audit-changed-webpage
80281		webPage-autotest-2024-01-15-234438-706	Tester Playwright	15.01.2024 23:45:15	/name-autotest-2024-01-15-234438-706
80280		name-autotest-2024-01-15-234438-706	Tester Playwright	15.01.2024 23:44:56	/name-autotest-2024-01-15-234438-706
259		Zobrazený v menu	Tester Playwright	15.01.2024 23:43:57	/System/Kôš/Zobrazený v menu
25100		Nesmie sa dať presunúť	Tester2 Playwright2	15.01.2024 23:39:41	/jet portal 4/Úvodná stránka/Test podar
80279		name-autotest-2024-01-15-233556-408	Tester2 Playwright2	15.01.2024 23:38:49	/System/Kôš/name-autotest-2024-01-15
24992		Nedá sa zmazať	Tester2 Playwright2	15.01.2024 23:37:57	/Test stavov/Nedá sa zmazať/Nedá sa z
80278		webPage-autotest-2024-01-15-232811-250	Tester Playwright	15.01.2024 23:29:25	/System/Kôš/name-autotest-2024-01-15

## 9. Čaká na publikovanie

V menu položke Čaká na publikovanie je zoznam stránok, ktoré majú v budúcnosti naplánované publikovanie. Obsahuje informácie o tom o akú web stránku (na akej adrese/cestě) a kedy sa bude publikovať. Bližšie informácie o web stránkach nájdete tu [Zoznam web stránok](https://docs.webjetcms.sk/latest/sk/redactor/webpages/README) (<https://docs.webjetcms.sk/latest/sk/redactor/webpages/README>).

Cieľom je prehľadne zobraziť zoznam stránok, ktoré v budúcnosti budú automaticky zmenené. Zobrazené sú všetky stránky bez ohľadu na práva používateľa na stromovú štruktúru stránok a zvolenú doménu.

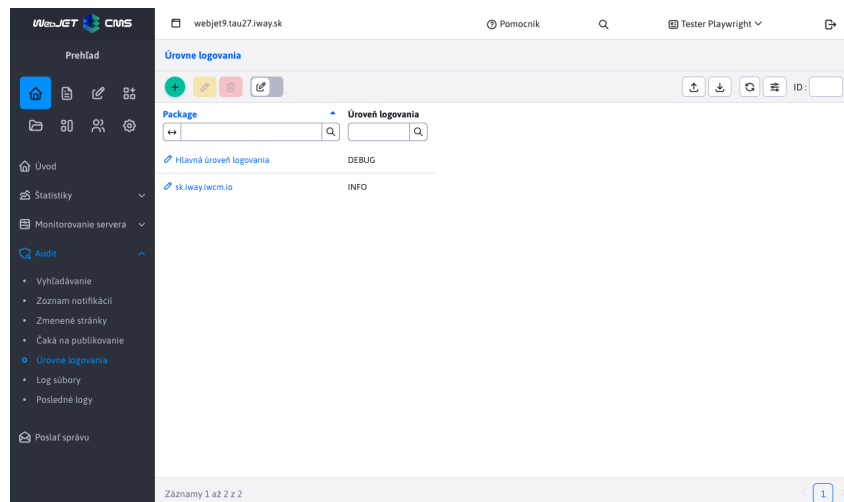
Červenou farbou sú zobrazené web stránky, ktoré čakajú na vypnutie zobrazovania - majú nastavenú možnosť Odverejniť stránku po tomto dátume. Takéto stránky po nastavenom dátume nebudú verejne zobraziteľné.

V zozname sa nezobrazujú stránky v koši, pre tie sa publikovanie nevykonáva.

ID	Doc ID	Názov	Dátum začiatku	Dátum konca	Cesta
0	105723	Test odpublikovania v budúcnosti	27.09.2024 11:34:29	01.12.2030 06:00:00	/Test stavov/Test odpublikovania v budúcnosti
174226	22955	Test publikovania v budúcnosti	01.12.2030 06:00:00		/Test stavov/Test publikovania v budúcnosti

## 10. Úrovně logovania

Aplikácia Úrovně logovania umožňuje spravovanie úrovni logovania pre jednotlivé java balíky.



Prvý záznam v tabuľke je vždy **Hlavná úrovně logovania** (základná úrovně).

Využívajú sa 2 konfiguračné premenné:

- **logLevel**, obsahuje hodnotu úrovne logovania pre **Hlavná úrovně logovania**
- **logLevels**, obsahuje zoznam java balíkov s úrovňou logovania (každý na novom riadku). Napr.:

```
sk.iway=DEBUG
sk.iway.iwcm=WARN
org.springframework=WARN
```

Zmeny nad tabuľkou sú uchovávané lokálne v konštante. Ak zmeny (nastavenia) chcete uložiť permanentne, v editore je potrebné zvoliť možnosť **Uložiť do databázy**. Pri uložení sa aktualizujú spomínané konfiguračné premenné v databáze.

## 11. Pridanie

Pri akcii pridania je potrebná hodnota java balíka (package) a úrovne logovania. Ak zadáte už pridaný package, nevytvorí sa duplicitná hodnota ale aktualizuje sa už existujúca.

Pridať

Základné

Package

Úrovně logovania

DEBUG

Uložiť do databázy

Uložiť všetky úrovne logovania do databázy

☐

Áno

Pomocník

X Zrušiť

✓ Pridať

## 12. Editácia

Akcia editácie sa správa rozdielne pre Hlavnú úroveň logovania a ostatné logovania.

## 12.1. Hlavná úroveň logovania

Pri editácii hlavnej úrovne môžeme zvoliť iba logovania typu NORMAL alebo DEBUG (pre podrobné logovanie). Ak v editore zmeníte hodnotu **Package**, žiadna zmena sa nevykoná. Nakoľko hlavná úroveň musí byť stále prítomná, zmeniť sa dá iba hodnota úrovne logovania.

## 12.2. Ostatné logovania

Zmena úrovne logovania sa uloží, ak zmeníte package, pôvodné logovanie zmizne a bude nahradené týmto novým. Povolené sú všetky úrovne logovania okrem hodnoty NORMAL.

# 13. Mazanie

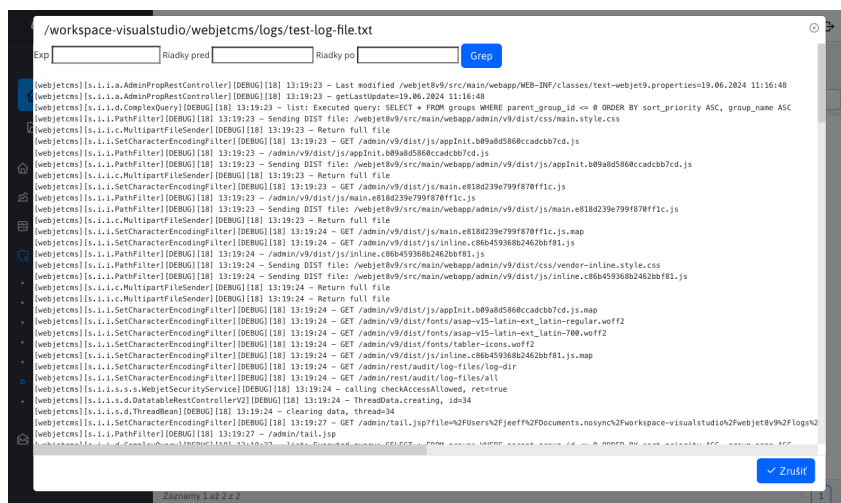
Všetky packages s úrovňou logovania sa dajú vymazať okrem **Hlavnej úrovne logovania**. Pri pokuse o vymazanie sa nič s ňou nestane (ani hodnota sa nezmení).

# 14. Log súbory

Aplikácia poskytuje prehľad všetkých log súborov. Úpravy nad tabuľkou nie sú povolené. Tabuľka slúži iba na prehľad. V ľavej hornej časti stránky, môžete vidieť cestu, kde sú tieto súbory uložené.

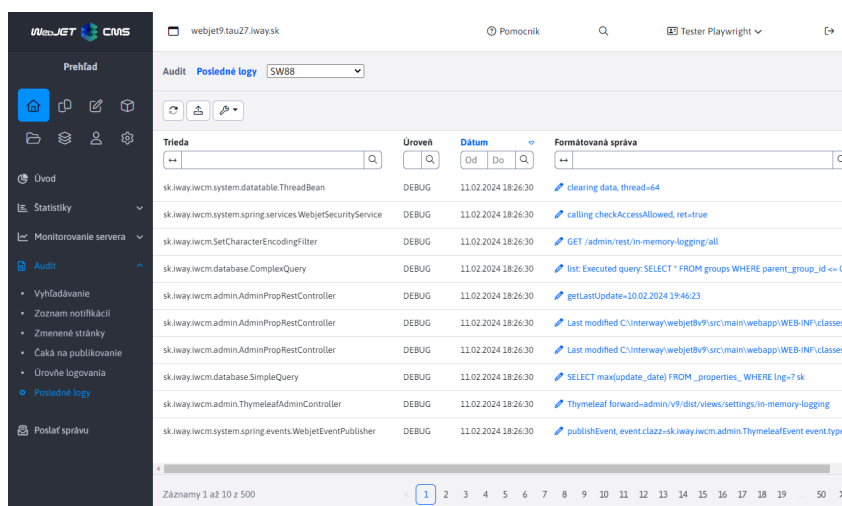
Názov	Veľkosť	Dátum
test-log-file.txt	21,28 KB	19.06.2024 15:25:41
access-log.txt	31,00 B	19.06.2024 15:25:27

Pri kliknutí na názov súboru sa zobrazí okno s obsahom súboru. Hlavička obsahuje polia pre možnosť filtrovania v súbore pomocou regulárnych výrazov (alebo priamo iba vyhľadaným výrazom).



## 15. Posledné logy

Aplikácia je určená na zobrazenie posledných logov, v prípade, že nemáte prístup k logom na súborovom systéme. Zobrazuje logy, ktoré prechádzajú cez log framework (čiže používajú triedu `Logger`), nezobrazí logy zapísané priamo cez `System.out` alebo `System.err`.



Podporuje cluster, je tak možné vyžiadať aj posledné logy z iného uzla clustra. V karte `Stack Trace` sa nachádza výpis zásobníka (obsah sa ale zobrazí len pre chybové záznamy, pre štandardné log úrovne je prázdny).

### 15.1. Konfiguračné možnosti/nastavenia:

- `loggingInMemoryEnabled` - nastavením na `true/false` povolíte alebo zakážete ukladanie logov do pamäte.
- `loggingInMemoryQueueSize` - maximálny počet logov zapísaných do pamäte (predvolene 200). Upozorňujeme, že všetky dáta sa naraz načítajú do tabuľky a z dôvodu prenosu `stack trace` môžu byť veľké. Neodporúčame túto premennú nastavovať na extrémne vysokú hodnotu.

Pre správne fungovanie musí byť `logger` nastavený aj v súbore `logback.xml`. Predvolene je takto nastavený, ak ste ale súbor menili, je potrebné doplniť `IN_MEMORY` appender a pridať jeho volanie pre `root` element.

```
...
<appender name="IN_MEMORY" class="sk.iway.iwcm.system.logging.InMemoryLoggerAppender" />

<root level="ERROR">
  <appender-ref ref="STDOUT" />

```

```
<appender-ref ref="IN_MEMORY" />
</root>
...
```

## 15.2. Implementačné detaily

- `sk.iway.iwcm.system.logging.InMemoryLoggerAppender` - appender pre `logback`, ktorý zabezpečuje odoslanie logov do `InMemoryLoggingDB`
- `sk.iway.iwcm.system.logging.InMemoryLoggingDB` - trieda zabezpečuje zápis a získanie logov z a do `queue`, načítanie logov na clustri
- `sk.iway.iwcm.system.logging.InMemoryLoggingEvent` - model pre log event
- `sk.iway.iwcm.system.logging.InMemoryLoggerRestController` - controller pre výpis logov do DataTable

## 16. Výkon servera

Pre optimálny výkon servera je potrebné splniť viacero požiadaviek a nastavení. Každá vložená aplikácia (napr. foto galéria, anketa atď.) do web stránky spôsobuje spomalenie. Aplikácie typicky vykonávajú dodatočné databázové požiadavky, alebo potrebujú čítať údaje zo súborového systému.

Výrazný vplyv na výkon môžu mať aj vyhľadávače, ktoré neustále prechádzajú a indexujú web stránky na vašom serveri. Ich návštevnosť nemusí byť vidieť napr. v Google Analytics, ale je vidieť v [štatistike](https://docs.webjetcms.sk/latest/sk/redactor/apps/stat/README) (<https://docs.webjetcms.sk/latest/sk/redactor/apps/stat/README>), ktorú poskytuje WebJET CMS.

### 16.1. Identifikácia problémov

Ako prvé je potrebné identifikovať miesta, kde dochádza k spomaleniu. Ak viete na prvý pohľad identifikovať web stránku, ktorá sa vám zdá pomalá, môžete použiť URL parameter `?_writePerfStat=true`. Inak zapnite monitorovanie servera, v ktorom viete identifikovať web stránky, ktoré sú vykonávané najdlhšie.

#### 16.1.1. URL parametrom

Pomocou URL parametra `?_writePerfStat=true` je možné získať výpis aplikácií vložených vo web stránke s časom ich vykonania. Napríklad stránku `/sk/` zobrazíte ako `/sk/?_writePerfStat=true`.

Pri takomto zobrazení web stránky sa do HTML kódu vloží po každej aplikácii výraz typu `PerfStat: 3 ms (+3) !INCLUDE(...)`. V štandardne zobrazenej web stránke nemusí byť dobre vyhľadateľný, preto odporúčame zobraziť zdrojový kód stránky - v Chrome menu Zobraziť-Vývojár-Zobraziť zdrojový kód. Následne použite vyhľadávanie v prehliadači výrazu `PerfStat:`.

Tento výraz je vo formáte `PerfStat: 3 ms (+3)` kde prvé číslo znamená celkový čas vykonania jedného `iwcm:write` výrazu a číslo v zátvorke je čas vykonania tejto aplikácie. Následne nasleduje cesta k aplikácii a jej parametre. Vás teda zaujíma primárne číslo v zátvorke.

Pomocou URL parametra `_disableCache=true` je možné vypnúť vyrovnávaciu pamäť aplikácií.

## 16.1.2. Monitorovanie servera

Pre komplexný pohľad môžete zapnúť funkciu **monitorovanie servera** nastavením nasledovných konfiguračných premenných:

- `serverMonitoringEnable` - zapne funkciu monitorovania servera a zaznamenávania hodnôt
- `serverMonitoringEnablePerformance` - zapne funkciu monitorovania výkonu aplikácií a web stránok
- `serverMonitoringEnableJPA` - zapne funkciu monitorovania SQL požiadaviek

**! Upozornenie:** monitorovanie výkonu aplikácií a SQL požiadaviek zaťažuje server, neodporúčame mať túto funkciu permanentne zapnutú.

Po nastavení konfiguračných premenných je potrebné vykonať **reštart aplikačného servera**, aby sa pri inicializácii aktivovalo sledovanie výkonu.

Následne v sekcii Monitorovanie servera - Aplikácie/WEB stránky/SQL dotazy viete identifikovať časti, ktoré sa dlho vykonávajú. Zamerajte sa na najčastejšie vykonávané aplikácie/SQL dotazy a ich optimalizáciu.

## 16.1.3. Celkový čas generovania web stránky

Existuje aplikácia `/components/_common/generation_time.jsp` ktorú ak vložíte do pätičky šablóny web stránky vygeneruje do HTML kódu celkový čas generovania web stránky.

Je možné nastaviť nasledovné parametre aplikácie:

- `hide` - predvolene `true` - čas generovania sa zobrazí ako komentár v HTML kóde
- `onlyForAdmin` - predvolene `false` - čas generovania sa zobrazí len ak je prihlásený administrátor

Do pätičky (alebo vhodného voľného poľa) šablóny web stránky vložte nasledovný kód:

```
!INCLUDE(/components/_common/generation_time.jsp, hide=true, onlyForAdmin=false)!
```

html

Na mieste vlozenej aplikácie sa zobrazí informácia o čase vykonania celej web stránky v ms:

```
<!-- generation time: 4511 ms -->
```

html

## 16.2. Meranie výkonu databázového servera a súborového systému

Pre porovnanie výkonu prostredí - napr. testovacie VS produkčné prostredie je možné použiť nižšie uvedené skripty. Ich spustenie vyžaduje právo na aktualizáciu WebJET. Merať a porovnávať prostredia môžete bez záťaže, ale aj počas prevádzky, alebo výkonnostných testov.

- `/admin/update/dbspeedtest.jsp` - meria výkon čítania údajov z databázového servera.

Dobré hodnoty sú napríklad:

```
Image read, count=445
...
Total time: 649 ms, per item: 1.4584269662921348 ms
Total bytes: 4.8050469E7, per second: 7.403770261941448E7 B/s

Random web page read, count=3716
...
Total time: 3608 ms, per item: 0.9709364908503767 ms
```

html

```
Total bytes: 1371566.0, per second: 380145.78713968955 B/s
```

```
Only documents.data web page read, count=3716
```

```
...
```

```
Total time: 2205 ms, per item: 0.5933799784714747 ms
```

```
Total bytes: 685783.0, per second: 311012.6984126984 B/s
```

```
Documents read using web page API, count=3716
```

```
...
```

```
Total time: 1869 ms, per item: 0.5029601722282023 ms
```

```
Total bytes: 685783.0, per second: 366925.09363295883 B/s
```

Z dôvodu rozdielneho počtu záznamov v databáze je potrebné porovnávať `per item` hodnoty.

- `/admin/update/fsspeedtest.jsp` - kontroluje rýchlosť čítania zoznamu súborov zo súborového systému, je potrebné overiť hlavne ak používate sieťový súborový systém.

Dobré hodnoty sú napríklad:

```
Testing mime speed, start=0 ms
has base file object, fullPath=/Users/jeeff/Documents.nosync/workspace-visualstudio/webjet/webjet8v9-
hotfix/src/main/webapp/components/_common/mime diff=1 ms
listFiles, size=678, diff=284 ms
listing done, diff=16 ms

Testing modinfo speed, start=0 ms
modinfo list, size=102, diff=1 ms
modinfo listing done, diff=220 ms
Total time=522ms
```

html

## 16.3. Optimalizácia databázových požiadaviek

Optimalizovať počet databázových požiadaviek je možné zapnutím vyrovnávacej pamäte - `cache`.

### 16.3.1. Web stránky

Každá web stránka má v karte Základné možnosť **Povoliť uloženie stránky do vyrovnávacej pamäte**. Zapnutím tejto možnosti sa obsah web stránky z tabuľky `documents` uloží do vyrovnávacej pamäte. Pri zobrazení web stránky nebude potrebné vykonať databázové volanie pre získanie obsahu web stránky.

Túto možnosť odporúčame zapnúť na najviac navštevovaných web stránkach, ktorých zoznam získate v aplikácii [Štatistika](https://docs.webjetcms.sk/latest/sk/redactor/apps/stat/README) (<https://docs.webjetcms.sk/latest/sk/redactor/apps/stat/README>).



### 16.3.2. Aplikácie

Podobne ako pre web stránky je možné zapnúť vyrovnávaciu pamäť aj pre aplikácie. Niektoré aplikácie majú túto možnosť dostupnú priamo v **nastavení aplikácie** (<https://docs.webjetcms.sk/latest/sk/custom-apps/appstore/README>) vlozenej vo web stránke v karte Zobrazenie ako pole **Čas vyrovnávacej pamäte**.

Ak aplikácia toto nastavenie nemá dostupné stále môžete parameter nastaviť v HTML kóde textu web stránky pridaním parametra `cacheMinutes=xxx` k parametrom vlozenej aplikácie, napríklad:

```
!INCLUDE(sk.iway.iwcm.components.reservation.TimeBookApp, reservationObjectIds=2560+2561, device=, cacheMinutes=10)!
```

html

**! Upozornenie:** je potrebné si uvedomiť, že vyrovnávacia pamäť je globálna pre celý aplikačný server. Ako kľúč sa použije cesta k súboru aplikácie, jednotlivé parametre zadané v HTML kóde web stránky a jazyk aktuálne zobrazenej web stránky. Neberú sa do úvahy URL parametre web stránky.

Vyrovnávaciu pamäť nie je teda možné použiť napríklad ak sa zobrazí napríklad stránkovanie zoznamu kde číslo strany sa prenáša pomocou URL parametra. Aby ale bolo možné uložiť zoznam noviniek existuje výnimka - pre aplikácie obsahujúce v názve súboru `/news/news` sa použije vyrovnávacia pamäť iba ak v URL adrese nie je zadaný parameter `page`, respektíve hodnota tohto parametra je iná ako `1`. Takto sa vyrovnávacia pamäť použije aj pre zoznam noviniek, ale uloží sa do nej len prvá strana výsledkov. Ďalšie strany nie sú ukladané.

## 16.4. Optimalizácia súborového systému

Web stránky typicky obsahujú veľa doplnkových súborov - obrázky, CSS štýly, JavaScript súbory a podobne, ktoré je potrebné spolu s web stránkou načítať. Rýchlosť zobrazenia teda závisí aj od počtu a veľkosti týchto súborov.

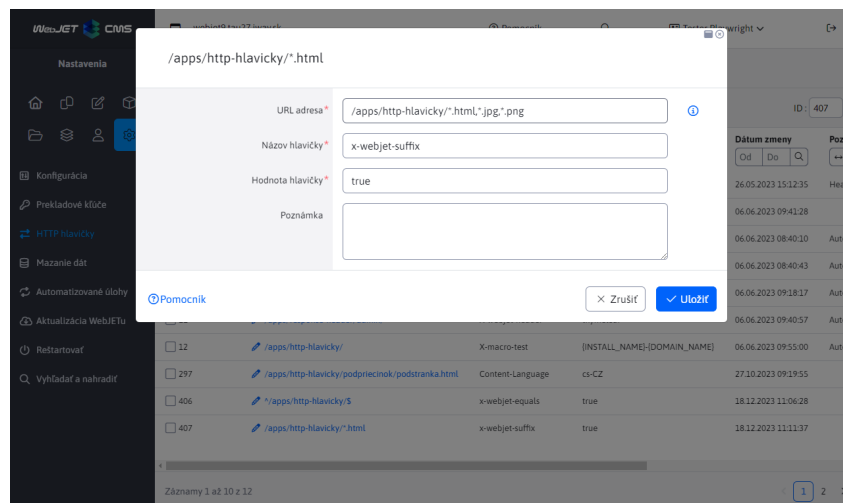
### 16.4.1. Nastavenie vyrovnávacej pamäte

Pre súbory web stránky je možné nastaviť použitie vyrovnávacej pamäte v prehliadači - súbor sa tak nebude opakovane čítať pri každom zobrazení web stránky, ale ak ho už má prehliadač vo vyrovnávacej pamäti, tak sa použije. Zrýchli sa tak zobrazenie web stránky a zníži záťaž na server. Príkladom je obrázok loga, ktorý je typický na každej stránke, ale jeho zmena je vysoko nepravdepodobná - respektíve mení sa rádomo raz za niekoľko mesiacov.

Je možné nastaviť nasledovné konfiguračné premenné, ktoré ovplyvňujú HTTP hlavičku `Cache-Control` :

- `cacheStaticContentSeconds` - nastavený počet sekúnd, predvolene `300` .
- `cacheStaticContentSuffixes` - zoznam prípon, pre ktoré sa HTTP hlavička `Cache-Control` vygeneruje, predvolene `.gif,.jpg,.png,.swf,.css,.js,.woff,.svg,.woff2` .

Pre presnejšie nastavenie je možné použiť aplikáciu [HTTP hlavičky \(https://docs.webjetcms.sk/latest/sk/admin/settings/response-header/README\)](https://docs.webjetcms.sk/latest/sk/admin/settings/response-header/README), kde môžete nastaviť rozdielne hodnoty pre rozdielne URL adresy.



## 16.5. Správanie pre administrátora

Ak je prihlásený administrátor vyrovnávacia pamäť pre aplikácie sa nepoužije (predpokladá sa, že administrátor vždy chce vidieť aktuálny stav).

Toto správanie je možné zmeniť nastavením konfiguračnej premennej `cacheStaticContentForAdmin` na hodnotu `true` . Vhodné je túto hodnotu nastaviť hlavne pre intranet inštalácie, kde sa používatelia overujú voči `SSO/ActiveDirectory` serveru a aj pri bežnej práci v intranet prostredí majú práva administrátora.

## 16.6. Vyhľadávače

Vyhľadávače a rôzne iné roboty môžu výrazne zaťažiť server. Zvlášť s nástupom učenia umelej inteligencie dochádza k výraznému prehľadávaniu internetu a plneniu databáz pre učenie umelej inteligencie. Roboty často skúšajú rôzne URL parametre pre získanie dodatočných dát.

### 16.6.1. Nastavenie robots.txt

Správanie robotov je možné ovplyvniť nastavením v súbore `/robots.txt`. Tento ak neexistuje je generovaný v predvolenom stave. Vami upravenú verziu umiestnite do `/files/robots.txt`, z tejto lokality ho WebJET zobrazí pri volaní `/robots.txt`.

Pomocou súboru `robots.txt` (<https://en.wikipedia.org/wiki/Robots.txt>) môžete ovplyvniť správanie robotov a vyhľadávačov - obmedziť URL adresy, ktoré môžu použiť, nastaviť odstup medzi požiadavkami atď.

## 16.7. Ostatné nastavenia

### 16.7.1. Reverzný DNS server

Štatistika, audit a ďalšie aplikácie môžu získavať reverzný DNS záznam z IP adresy. Používa sa API volanie

`InetAddress.getByName(ip).getHostName()`. Na serveroch/v DMZ nemusí ale byť DNS server dostupný a toto volanie môže trvať niekoľko sekúnd kým nastane chyba. Všeobecne takéto volanie spomaľuje vykonanie HTTP požiadavky.

Nastavením konfiguračnej premennej `disableReverseDns` na hodnotu `true` je možné vypnúť získavanie DNS názvu z IP adresy návštevníka a zrýchliť vykonávanie požiadaviek. Do poľa pre hodnotu `hostname` sa vtedy zapíše hodnota IP adresy.

### 16.7.2. Vypnutie štatistiky

Zapisovanie údajov štatistiky je asynchrónne, vykonáva sa v dávkach tak, aby zobrazenie web stránky nečakalo na zápis údajov štatistiky do databázy.

Pri vysokej návštevnosti, alebo hľadaní problémov s výkonom môžete dočasne vypnúť zapisovanie štatistík návštevnosti nastavením konfiguračnej premennej `statMode` na hodnotu `none`. Štandardná hodnota je `new`.

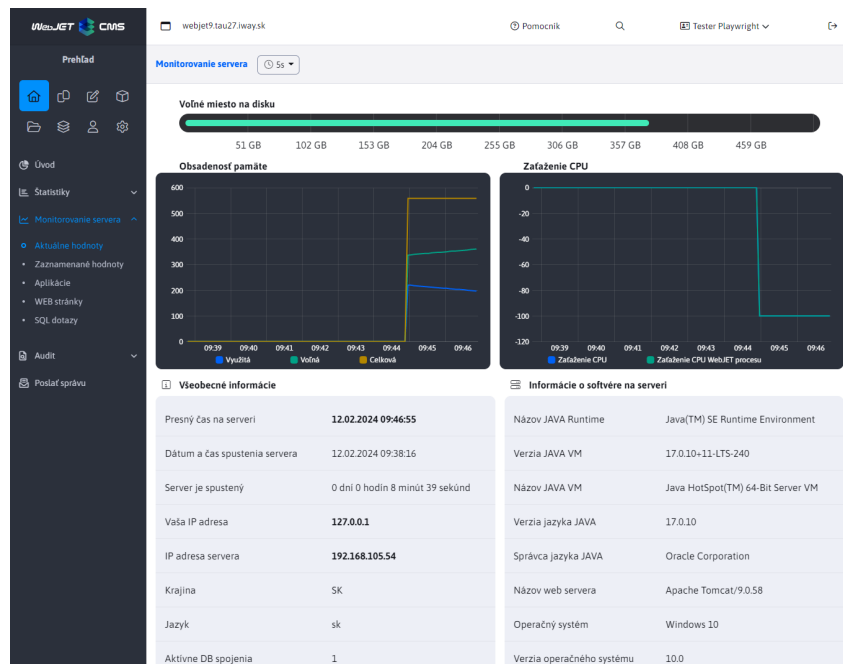
## 17. Monitorovanie servera

### 17.1. Vnútorne monitorovanie

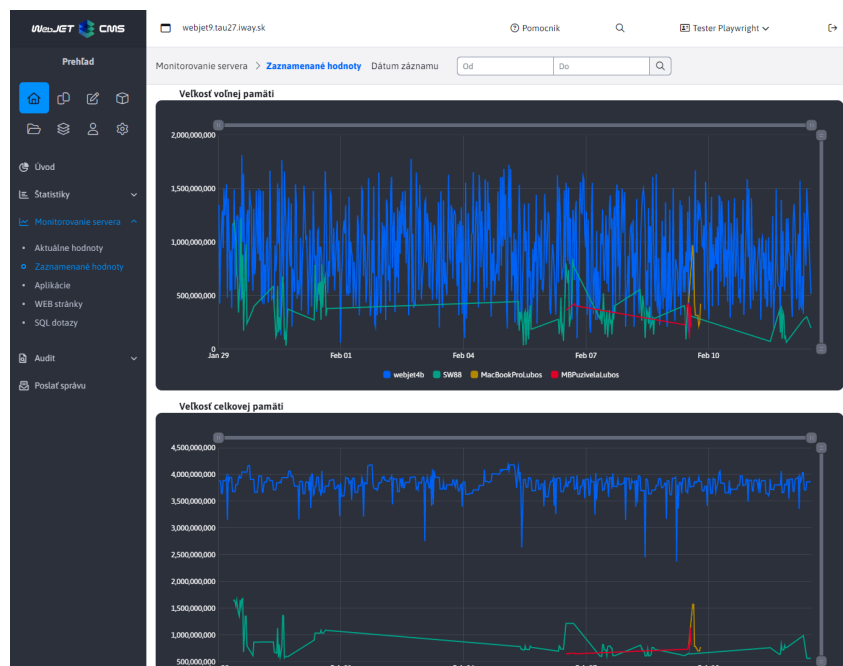
Analýza výkonu a záťaže servera, jednotlivých aplikácií, databázových dotazov a samotných stránok je možné sledovať priamo v aplikácii Monitorovanie servera (v administrácii WebJETu v sekcii Prehľad).

Modul poskytuje nasledovné možnosti:

- **Aktuálne hodnoty** - aktuálne hodnoty zaťaženia servera, pamäte a počet databázových spojení.



- **Zaznamenané hodnoty** - výpis historických zaznamenaných hodnôt využitia pamäte, `sessions`, `cache` a spojení s databázou. Pre ukladanie historických hodnôt je potrebné nastaviť konf. premennú `serverMonitoringEnable` na hodnotu `true`.



Po nastavení konfiguračnej premennej `serverMonitoringEnablePerformance` na `true` sú dostupné aj:

- **Aplikácie** - štatistika vykonaní jednotlivých aplikácií. Zobrazuje počet vykonaní, priemerný čas vykonania, počet vykonaní z cache pamäte a najpomalšie vykonanie.
- **WEB stránky** - štatistika zobrazení jednotlivých web stránok. Zobrazuje počet zobrazení, priemerný čas zobrazenia, najpomalšie a najrýchlejšie zobrazenie.

Po nastavení konfiguračnej premennej `serverMonitoringEnableJPA` na `true` je dostupné aj:

- **SQL dotazy** - štatistika rýchlosti vykonávania SQL dotazov. Zobrazuje počet vykonaní, priemerný čas vykonania, najpomalšie a najrýchlejšie vykonanie a samotný SQL dotaz.

**! Upozornenie:** aktivácia monitorovania má vplyv na výkon servera a jeho pamäťové zaťaženie. Okrem možnosti zaznamenané hodnoty má zapnutie monitoringu dopad na výkon servera. Všetky údaje okrem časti zaznamenané hodnoty sú držané len v pamäti servera, takže po jeho reštarte sa začnú evidovať nanovo.

**! Upozornenie:** modulové možnosti **Aplikácie, WEB stránky a SQL dotazy** využívajú jedinečnú spoločnú logiku, ktorá je bližšie opísaná v [Monitorovanie servera podľa vybraného uzla](#)

## 17.2. Vzdialené monitorovanie behu servera

Ak potrebujete monitorovať stav WebJETu cez [Nagios](http://www.nagios.org/) (<http://www.nagios.org/>)/[Zabbix](https://www.zabbix.com) (<https://www.zabbix.com>) alebo inú službu, WebJET poskytuje na URL adrese `/components/server_monitoring/monitor.jsp` svoj stav. Odpovedá HTTP **stavom 200 ak je všetko v poriadku**, alebo **stavom 500** (Internal Server Error) ak **nie sú splnené všetky kontroly**.

Uvedenú URL adresu je možné volať aj v sekundových intervaloch, odporúčame ju používať aj v rámci clustra pre monitorovanie dostupnosti jednotlivých nodov.

**Povolené IP adresy**, pre ktoré monitor.jsp korektne odpovedá sa nastavujú v konfiguračnej premennej `serverMonitoringEnableIPs`.

Komponenta monitoruje nasledovné časti:

- **Inicializácia WebJETu**, vrátane jeho `preheating` (čakanie na inicializáciu cache objektov, alebo úloh na pozadí). Čas `preheating` sa nastavuje v konf. premennej `monitoringPreheatTime` (predvolene 0). WebJET odpovedá textom `NOT INITIALISED` ak nie je korektne inicializovaný (napr. nie je vôbec konektivita do databázy pri jeho štarte, alebo má neplatnú licenciu). Textom `T00 SHORT AFTER START` odpovedá počas `preheating` času (zaradenie do clustra by malo čakať na dokončenie načítania cache objektov/úloh na pozadí).
- Monitorovanie **dostupnosti databázového spojenia** - vykonáva sa SQL select z tabuľky `documents` (konkrétne `SELECT title FROM documents WHERE doc_id=?`), pričom v konfiguračnej premennej `monitorTestDocId` je docid testovanej stránky. Ak sa SQL dotaz nepodarí odpovedá textom `DEFAULT DOC NOT FOUND`.
- **Dostupnosť šablón** - ak je zoznam inicializovaných šablón menší ako 3 odpovedá textom `NOT ENOUGH TEMPLATES`.
- **Zápis údajov štatistiky** - overuje, že v zásobníku zápisu štatistík nie je podozrivo veľa záznamov (ich počet sa nastavuje v konfiguračnej premennej `statBufferSuspicionThreshold`, predvolene 1000). Ak zásobník zápisu štatistík obsahuje väčšie množstvo údajov na zápis indikuje to buď problém s výkonom SQL servera, alebo problém s úlohami na pozadí. V prípade prekročenia počtu záznamov odpovedá textom `STAT BUFFER SUSPICION`.
- Ak nastane **iná chyba** odpovedá textom `EXCEPTION: xxxx`.

WebJET je možné aj manuálne **prepnúť do servisného režimu** nastavením konfiguračnej premennej `monitorMaintenanceMode` na `true`. Vtedy monitor.jsp odpovedá textom `UNAVAILABLE`.

Ak je všetko v poriadku odpovedá textom `OK`. Pre monitorovanie **postačuje sledovať HTTP stav** odpovede, text je len informačný pre presnejšie určenie problému.

## 17.3. Konfiguračné premenné

- `serverMonitoringEnable` - ak je nastavené na `true`, spúšťa monitorovanie servera každých 30 sekúnd a zapisuje tieto hodnoty do tabuľky `monitoring`
- `appendQueryStringWhenMonitoringDocuments` - zachytávať pri monitorovaní aj SQL parametre `?`
- `monitorTestDocId` - ID stránky, ktorej databázové spojenie (získanie názvu) sa testuje v komponente `/components/server_monitoring/monitor.jsp` ktorú môže testovať dohľadový SW (predvolená hodnota: 1)
- `serverMonitoringEnablePerformance` - ak je nastavené na `true`, spúšťa monitorovanie rýchlosti SQL dotazov, web stránok a aplikácií (predvolená hodnota: false)
- `serverMonitoringEnableJPA` - ak je nastavené na `true`, spúšťa monitorovanie rýchlosti vykonávania SQL dotazov pre JPA, má ale za následok zvýšenie záťaže na pamäť servera (predvolená hodnota: false)

- `serverMonitoringEnableIPs` - Zoznam IP adries z ktorých je dostupná komponenta `monitor.jsp` pre monitorovanie servera (predvolená hodnota: 127.0.0.1,192.168.,10.,62.65.161.,85.248.107.,195.168.35.)
- `monitoringPreheatTime` - Počet sekúnd potrebných pre zahriatie web sídla (načítanie cache) po reštarte, počas ktorého bude `monitor.jsp` komponenta vracat' nedostupnosť uzla clustra (predvolená hodnota: 0)
- `monitoringEnableCountUsersOnAllNodes` - Ak verejné uzle clustra nemajú možnosť zapisovať do tabuľky `_conf_/webjet_conf` nastavte na hodnotu `false`. Celkový počet `sessions` bude potom dostupný len súčtom z jednotlivých záznamov v monitorovaní servera.

## 18. Reštartovať

Kliknutím na možnosť **Reštartovať** v sekcii Nastavenia sa vám zobrazí potvrdenie reštartu WebJETu. Reštart sa systémovo vykoná na serveri, avšak záleží od nastavenia servera, či je reštart z web aplikácie povolený. Ak nie, reštart sa nevykoná.

V konfigurácii `server.xml` aplikačného servera [Tomcat](https://tomcat.apache.org/tomcat-9.0-doc/config/context.html) (<https://tomcat.apache.org/tomcat-9.0-doc/config/context.html>) je potrebné mať povolený reštart pomocou atribútu `reloadable="true"` v elemente `Context` :

```
<Host name="...">
  <Context reloadable="true" />
</Host>
```

xml

**!** **Upozornenie:** Pred reštartom si overte dostupnosť technickej podpory vášho hostingu, pretože môže byť potrebné reštartovať aj aplikačný server. To však nie je možné vykonať priamo z prostredia WebJETu.

Opakovaným reštartom sa môže tiež zaplniť pamäť aplikačného servera, čo môže vyžadovať reštart aplikačného servera priamo na serveri.

## 19. Výmena údajov uzlov clustra

Stránky **Aplikácie**, **WEB stránky** a **SQL dotazy** zdieľajú rovnakú logiku ohľadne monitorovania servera podľa aktuálne zvoleného uzla. Na výber uzla slúži pole, ktorý sa nachádza v hlavičke stránky vedľa názvu stránky.

SQL dotazy		SW88 (Aktuálny uzol)	
SQL		# vykonaní	Čas vyko
		Oc Dc Q	Od
SELECT insert_script_gr_id, domain_id, group_id, insert_script FROM insert_script_gr WHERE (insert_script = ?)		254	
SELECT insert_script_doc_id, doc_id, insert_script FROM insert_script_doc WHERE (insert_script = ?)		254	
SELECT templates_group_id, directory, inline_editing_mode, key_prefix, name FROM templates_group WHERE (templates_group_id = ?)		104	
SELECT perm_id, permission, perm_group_id FROM user_perm_groups_perms WHERE (perm_group_id = ?)		29	
SELECT group_id, editable_groups, editable_pages, group_title, writable_folders FROM user_perm_groups WHERE (group_id = ?)		27	
SELECT id, group_id, banner_id FROM banner_group WHERE (banner_id = ?)		14	
Záznamy 1 až 10 z 18		1 2	

Po otvorení klikom, môžeme vidieť všetky dostupné možnosti. Prednastavená hodnota je vždy aktuálny uzol (uzol clustra na ktorý ste práve prihlásený), ktorý je označený textom **(Aktuálny uzol)**.

SW88 (Aktuálny uzol)

MBPuzivelaLubos

MacBookProLubos

node3

webjet4b

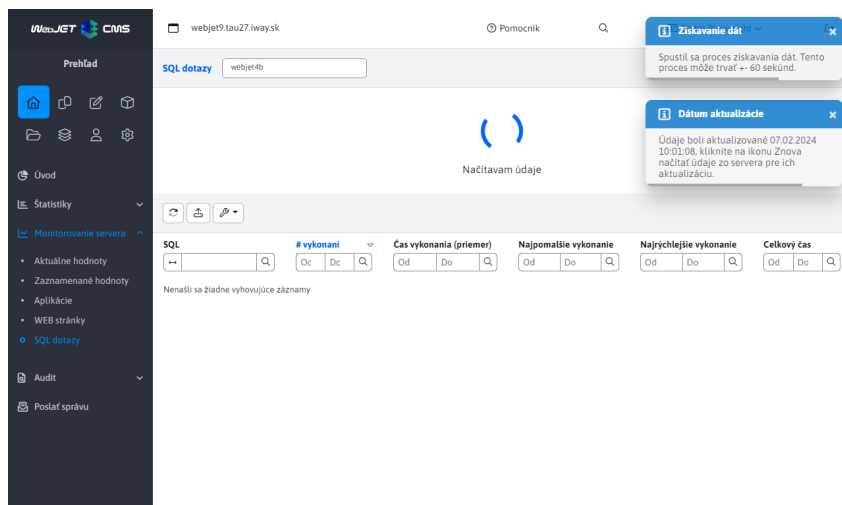
Ak je zvolený uzol aktuálny, zobrazujú sa lokálne uložené dáta. V tomto prípade je taktiež k dispozícii aj tlačidlo vymazania, ktoré odstráni tieto lokálne uložené dáta (tlačidlo vymazania je dostupné iba v prípade aktuálneho uzla). V prípade iného ako aktuálneho uzla sa dáta získavajú z databázovej tabuľky.

## 19.1. Obnovenie dát - aktuálny uzol

Ak je zvolený aktuálny uzol, tak po stlačení tlačidla obnovenia údajov sa iba získajú aktuálne uložené dáta (nepracuje sa tu s databázovými tabuľkami). Ak boli dáta predtým vymazané, môže chvíľu trvať kým sa tam objavia nové záznamy.

## 19.2. Obnovenie dát - vzdialený uzol

V prípade iných uzlov, ako aktuálnych, je obnovenie dát zložitejšie. Dáta iných uzlov sú uložené v tabuľku `cluster_monitoring`. Proces obnovenia dát začína vymazaním týchto dát z tabuľky, nakoľko už nemusia byť aktuálne.



Ako je vidieť na obrázku vyššie, dáta boli odstránené a zobrazí sa animácia čakajúca na dáta. Taktiež vidíme informačnú notifikáciu, ktorá nás upozorňuje, že tento proces môže trvať +- niekoľko sekúnd. Tento interval sa môže líšiť v závislosti od nastavenej konfiguračnej premennej `clusterRefreshTimeout`.

Proces získania aktuálnych dát spočíva vo vytvorení požiadavky o aktuálne dáta pre nejaký uzol vytvorením záznamu v databázovej tabuľke `cluster_refresher`. Samotný cluster v intervaloch zadaných konf. premennou `clusterRefreshTimeout` aktualizuje dáta v tabuľke `cluster_monitoring` pre konkrétny uzol, ak existuje pre tento uzol žiadosť v tabuľke `cluster_refresher`. Preto proces získavania dát môže trvať aj niekoľko minút a môže sa líšiť v závislosti od nastaveného intervalu obnovovania cluster-a (môže nastať aj situácia, kde cluster interval bol tesne pred obnovením a aktuálne dáta získame za 10 sekúnd, aj keď interval bol nastavený na 5 minút).

Síce to nie je zobrazené, ale stránka sa bude každých 10 sekúnd dopytovať, či do tabuľky `cluster_monitoring` neboli pridané nové dáta, ktoré by mohli byť zobrazené. V prípade, že požadovaný uzol neobsahoval žiadne dáta (ale tabuľka už bola aktualizovaná), vytvorí sa nová cluster požiadavka o dáta, a opäť budeme každých 10 sekúnd kontrolovať, či sa tieto dáta už aktualizovali. Celý proces sa bude opakovať dovtedy, kým aktualizovaná tabuľka `cluster_monitoring` nebude obsahovať aspoň jeden záznam k zobrazeniu. V tej chvíli sa skryje animácia a aktuálne získane dáta iného uzla sú zobrazené.

## 20. Mazanie dát

Aplikácia **Mazanie dát** vám umožňuje odstrániť nepotrebné dáta z databázy, čím môžete zvýšiť výkon servera a uvoľniť miesto na disku. Tento nástroj nájdete v sekcii **Nastavenia** pod položkou **Mazanie dát**.



## 20.1. Databázové záznamy

Mazanie dát z vybraných databázových tabuliek, mazanie je možné z nasledovných skupín:

- **Štatistika:** Odstraňuje štatistické dáta. Zmazanie starších dát môže významne zlepšiť výkon servera, stratíte ale informácie o návštevnosti webu za zvolené obdobie.
- **E-maily:** Umožňuje odstrániť odoslané e-maily z aplikácie Hromadný e-mail a emaily odoslané s časovým oneskorením (prípadne emaily odoslané v rámci viac uzlového clustra).
- **História stránok:** Maže zaznamenané historické verzie webových stránok, tie sa ukladajú pri každom publikovaní web stránky. Sú zobrazené v karte História pri editácii web stránky. Zmazanie neovplyvní aktuálne zobrazené stránky, zmažú sa historické verzie.
- **Monitorovanie servera:** Odstraňuje zaznamenané údaje z monitorovania servera, ako sú výkonnostné metriky a logy.
- **Audit:** Maže záznamy auditu, ktoré monitorujú aktivity používateľov a systémové udalosti, zmazať je možné len vybrané typy záznamov.

Pri každom zmazení sa vykonáva aj optimalizácia danej databázovej tabuľky, aby sa fyzicky uvoľnilo miesto na disku a optimalizovalo sa poradie záznamov v databázovej tabuľke.

## 20.2. Cache objekty

Zobrazuje zoznam objektov uložených v aplikačnej cache pamäti a umožňuje ich jednotlivé vymazanie, čím môžete znížiť spotrebu pamäte, alebo vyvolať obnovenie dát v cache pamäti servera. Kliknutím na názov je možné pre vybrané dátové typy zobraziť obsah záznamu. Pre prácu sa používa objekt [Cache](https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/Cache.java) (<https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/Cache.java>)

## 20.3. Persistent cache objekty

Správa a mazanie objektov uložených v trvalej cache pamäti, ktorá uchováva dáta aj po reštarte servera (údaje sú uložené v databáze). Pre prácu sa používa objekt `PersistentCacheDB` (<https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/system/cache/PersistentCacheDB.java>). Do tejto cache je možné ukladať len textové dáta, typicky sa využíva metóda `downloadUrl(String url, int cacheInMinutes)` ktorá na pozadí sťahuje dáta zo zadanej URL adresy a aktualizuje ich v nastavenom čase. Aplikácia používa túto metódu a ihneď získava dáta z cache.

ID	Kľúč (názov)	Veľkosť	Každých minút	Ďalšia aktualizácia
2	<a href="http://www.interway.sk/admin/mem.jsp">http://www.interway.sk/admin/mem.jsp</a>	230	100	28.08.2024 12:55:20
3	<a href="http://www.interway.sk/test.jsp">http://www.interway.sk/test.jsp</a>	211	236	29.10.2020 15:26:30

## 21. Zálohovanie systému

Aplikácia slúži na vytvorenie ZIP archívu jednotlivých priečinkov súborového systému WebJET. Môžete si zvoliť, ktoré priečinky sa do ZIP archívu majú zahrnúť a do ktorého priečinku sa má vytvoriť výsledný ZIP archív. Nevytvára sa záloha databázy, tú je potrebné vytvoriť nástrojmi na zálohovanie databáz.

**! Upozornenie:** Objem dát v zvolených priečinkoch môže byť veľký a ZIP súbor sa nemusí vygenerovať správne (obmedzenie je na 2GB súbor). V prípade potreby môžete vytvárať zálohy po častiach (jednotlivých priečinkoch).

**Vytvoriť ZIP archív**  
Zo zoznamu vyberte priečinky, ktoré chcete archivovať.

Cesta k archívu:

Archivovať priečinky:

- ☒ images
- ☒ admin
- ☒ wjerrorpages
- ☒ components
- ☒ WEB-INF
- ☒ files
- ☒ templates
- ☒ static-files
- ☒ apps

Tento proces môže trvať niekoľko desiatok minút podľa objemu dát v zvolených priečiinkoch. Čakajte, kým celý proces skončí. Počas toho by sa vám v okne mala zobrazovať informácia o počte už vygenerovaných stránok a o celkovom počte stránok.

Výsledkom je zip archív vytvorený v zadanom priečinku.