

Manuál pro provoz

Verze: 2024.0-SNAPSHOT.33 20.01.2025 9:39:09

Obsah

- Zabezpečení
 - [Bezpečnostní testy](#)
 - [Kontrola zranitelnosti knihoven](#)
 - [Aktualizace WebJET](#)
- Audit
 - [Audit](#)
 - [Seznam oznámení](#)
 - [Změněné stránky](#)
 - [Čeká se na zveřejnění](#)
 - [Úrovně logování](#)
 - [Soubory protokolu](#)
 - [Nejnovější protokoly](#)
- Operace
 - [Výkonnost serveru](#)
 - [Monitorování serveru](#)
 - [Restartování](#)
 - [Výměna dat uzlu clusteru](#)
 - [Vymazání dat](#)
- Soubory
 - [Zálohování systému](#)

1. Bezpečnostní testy

Zabezpečení systému WebJET CMS závisí na jeho správné konfiguraci a správném nastavení přístupových práv. Informace na této stránce je třeba nastavit před uvedením do produkčního provozu a následně kontrolovat alespoň jednou za čtvrt roku a vždy před provedením bezpečnostních testů.

1.1. Nastavení systému

1.1.1. Skupiny práv

Prostřednictvím WebJET CMS je také možné modifikovat programové soubory, proto je nutné před penetračním testováním nastavit omezení oprávnění. Doporučujeme vytvořit následující [skupiny práv \(https://docs.webjetcms.sk/latest/cs/admin/users/perm-groups\)](https://docs.webjetcms.sk/latest/cs/admin/users/perm-groups). **Jiné skupiny uživatelů nebo přímo uživatelé by neměli mít níže uvedená jednotková práva.**

Správa uživatelů

Skupina obsahuje oprávnění, která umožňují měnit oprávnění. Uživatel s takovou skupinou práv musí být dostatečně obezřetný, aby věděl, že má nejvyšší možnosti oprávnění (protože může nastavit práva pro sebe nebo pro ostatní uživatele).

Uživatel s tímto oprávněním může ohrozit celý systém (např. může nastavit oprávnění tak, aby mohl odstranit všechny webové stránky nebo všechny soubory).

Nastavte následující práva pro skupinu práv:

- správa administrátorů - právo umožňuje nastavit oprávnění uživatelů v administraci.
- Skupiny práv - právo umožňuje nastavit oprávnění pro skupiny.

Programátor

Výchozí nastavení by mělo být takové, že uživatelé (editoři) nemohou nahrávat a upravovat soubory programu. Programátor však často potřebuje provést rychlou změnu (`hotfix`) programového kódu, a proto musí upravit i programové soubory. Současně má přidána práva upravovat všechny konfigurační proměnné a editovat všechny texty překladu.

Uživatel s tímto oprávněním může ohrozit celý systém (např. nahrát škodlivý kód, který může na serveru provést jakoukoli operaci, včetně odstranění souborů na serveru nebo úplného vymazání databáze).

- Neomezené nahrávání souborů (přípony a velikosti)
- Konfigurace - zobrazení všech proměnných
- Úprava textu - zobrazení všech textů

Poznámka: seznam konfiguračních proměnných bez oprávnění "Konfigurace - zobrazit všechny proměnné" je nastaven v proměnné `conf.configEnabledKeys`, seznam překladových klíčů bez oprávnění "Úprava textu - zobrazení všech textů" v konf. proměnné `propertiesEnabledKeys`. HTML kód je také filtrován v překladových klíčích, pravidla jsou popsána níže v části `Stored XSS cez úpravu překladových klíčův`.

Kromě oprávnění je třeba povolit přístup k adresářům souborového systému pro zápis:

- `/apps` - obsahuje kód aplikace
- `/components` - obsahuje kód aplikace
- `/templates` - obsahuje šablony designu

Pokud je prostředí nasazeno přímo z úložiště GIT a nepředpokládáte, že bude spuštěno. `hot-fixov` přímo přes WebJET CMS, nemusíte nastavovat výše uvedená práva pro zápis do souborového systému. Navíc pro tento případ doporučujeme nastavit práva pro zápis do souborového systému pouze pro adresáře (ostatní adresáře a soubory mají práva pouze pro čtení):

- `/images` - obsahuje obrázky nahrané editory CMS

- `/files` - obsahuje soubory nahrané editory CMS
- `/shared` - obsahuje obrázky a soubory nahrané editory CMS a sdílené mezi doménami.
- `/WEB-INF/tmp` - obsahuje dočasné soubory CMS
- `/WEB-INF/imgcache` - obsahuje vygenerované náhledy obrázků a výřezy pro použití prostřednictvím `/thumb` předpona
- `/WEB-INF/formfiles` - obsahuje soubory nahrané prostřednictvím formulářů na webových stránkách vytvořených pomocí aplikace Formuláře.

1.1.2. Konfigurace

Nastavte a zkontrolujte následující konfigurační proměnné (v nabídce Nastavení->Správa konfigurace):

- `defaultDisableUpload=true` - aktivuje režim, ve kterém má uživatel práva souborového systému pouze pro nakonfigurované adresáře. Pokud nejsou nastaveny žádné adresáře, nemá práva zápisu do žádného adresáře.
- `emailProtectionSenderEmail` - nastavit vhodný typ e-mailové adresy `noreply@domena.sk`, která se používá jako e-mailová adresa odesílaných e-mailů (původní hodnota je nastavena na `Reply-To` e-mailové hlavičky).
- `adminEnabledIPs` - obsahuje čárkou oddělený seznam IP adres, ze kterých je přístup k serveru `/admin` díly.
- `multidomainAdminHost` - umožňuje nastavit samostatnou doménovou adresu pro přístup k `/admin` díly, např. `cms.domena.sk`. Po nastavení bude hovor `/admin` adresy na jiných doménách vrátit chybu 404 - Stránka neexistuje.
- `serverBeyondProxy` - pokud je aplikační server za Load Balancerem / proxy serverem, je třeba nastavit hodnotu na `true` (jinak nastavte hodnotu `false`). Load Balancer pak musí v hlavičce HTTP odeslat následující údaje `x-forwarded-for` IP adresa návštěvníka webové stránky a v záhlaví. `x-forwarded-proto` protokol (`http` nebo `https`). Při auditu (např. po vyplnění formuláře na webových stránkách) ověřte, zda je IP adresa návštěvníka webových stránek správně zaznamenána.
- `serverName` - výchozí nastavení `unknown` - nastaví hodnotu hlavičky HTTP `Server` pro odpověď HTTP. Pokud máte za Load Balancerem/proxy serverem aplikační server, ověřte hodnotu této hlavičky v odpovědi HTTP a případně ji nastavte na vhodnou neznámou hodnotu na Load Balanceru/proxy serveru.

Omezení pro nahrané soubory ze strany editorů v administraci:

- `FCKConfig.UploadMaxSize[Default][image]` - výchozí 0 - limit velikosti v kB pro nahrávání **Obrázky**, doporučujeme nastavit hodnotu 10000 pro nahrávání max. 10 MB obrázku.
- `FCKConfig.UploadMaxSize[Basic][image]` - výchozí 2048 - limit velikosti v kB pro nahrávání **Obrázky** pro uživatele, kteří **nemají v editoru správnou nabídku Kompletní**
- `FCKConfig.UploadMaxSize[Default][file]` - výchozí 0 - limit velikosti v kB pro nahrávání **soubory**, doporučujeme nastavit hodnotu 50000 pro nahrávání max. 50 MB souboru.
- `FCKConfig.UploadMaxSize[Basic][file]` - výchozí 2048 - limit velikosti v kB pro nahrávání **soubory** pro uživatele, kteří **nemají v editoru správnou nabídku Kompletní**
- `FCKConfig.UploadFileTypes[Default][image]` - výchozí prázdný = bez omezení - typ omezení **Obrázky**, doporučujeme nastavit na `jpg, jpeg, png, gif, svg, mp3, mp4`. Je třeba zvážit možnost povolení přípony SVG, viz potenciální riziko níže v bloku. **Stored XSS** cez SVG obrázok.
- `FCKConfig.UploadFileTypes[Basic][image]` - výchozí nastavení `jpg, jpeg, png, gif, mp4` - typové limity **Obrázky** pro uživatele, kteří **nemají v editoru správnou nabídku Kompletní**
- `FCKConfig.UploadFileTypes[Default][file]` - výchozí prázdný = bez omezení - typ omezení **soubory**, doporučujeme nastavit na `pdf, docx, xlsx, pptx, ppsx, zip, rtf`
- `FCKConfig.UploadFileTypes[Basic][file]` - výchozí nastavení `doc, docx, xls, xlsx, pdf, zip, rtf` - typové limity **soubory** pro uživatele, kteří **nemají v editoru správnou nabídku Kompletní**

Můžete také zkontrolovat následující konfigurační proměnné:

- `overviewJsonUrl` - definuje adresu URL, ze které se načítá seznam novinek v systému WebJET. Pokud uživatelé nemají přístup k internetu z prohlížeče, můžete tuto hodnotu nastavit na hodnotu `/admin/v9/json/` pro čtení z místní instance. V nových verzích systému WebJET CMS se však uživatelům novinky nezobrazí.
- `springSecurityAllowedAuths` - seznam povolených autorizačních metod pro služby REST, ve výchozím nastavení `basic, api-token`. Nastavte na prázdnou hodnotu, pokud projekt nepotřebuje jiné než standardní přihlášení do formuláře. Po změně hodnoty je nutné restartovat aplikační server.

1.1.3. Hlavičky HTTP

V aplikaci Konfigurace můžete nastavit hodnoty záhlaví zabezpečení:

- `contentSecurityPolicy` - nastavení záhlaví `Content-Security-Policy` . Omezení, jak má stránka načítat různé zdroje. Pokud máte certifikát https, můžete jej nastavit na:
`default-src 'none'; script-src https: blob: data: 'unsafe-inline' 'unsafe-eval'; worker-src https: blob:; child-src https:`
Ve výchozím nastavení prázdné (záhlaví není nastaveno).
- `contentSecurityPolicySvg` - specifické omezení pro obrázky SVG kvůli jejich odlišnému zpracování v prohlížeči Internet Explorer.
- `featurePolicyHeader` - Hodnota hlavičky HTTP `Feature-Policy/Permissions-Policy` (např: `microphone 'none'; geolocation 'none'`), více na: https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy (https://developer.mozilla.org/en-US/docs/Web/HTTP/Feature_Policy). Ve výchozím nastavení prázdné.
- `referrerPolicy` - Nastavení hlavičky HTTP `Referrer-Policy` , doporučujeme nastavit na `same-origin` . Výchozí `same-origin` .
- `serverName` - hodnota záhlaví `Server` v odpovědích HTTP. Výchozí `unknown` . Nelze ji nastavit na prázdnou hodnotu, protože pak aplikační server vloží tuto hlavičku.
- `strictTransportSecurity` - ve výchozím nastavení prázdný - nastaví hlavičku HTTP [Přísný transport a zabezpečení](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) (https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) v odpovědích HTTP, který zajišťuje přesměrování požadavků HTTP na zabezpečený https, doporučujeme nastavit na: `max-age=31536000 ; includeSubDomains` . Vyžaduje, aby byl aplikační server přístupný prostřednictvím zabezpečeného protokolu https.
- `xContentTypeOptions` - hodnota záhlaví `X-Content-Type-Options` nastavit určování typů souborů podle obsahu (bez ohledu na přípony). Výchozí `nosniff` .
- `xFrameOptions` - hodnota záhlaví `X-Frame-Options` pro ochranu před útokem CSRF. Výchozí `SAMEORIGIN` .
- `xRobotsTagValue` - hodnota záhlaví `X-Robots-Tag` pro adresy URL nastavené v proměnné `xRobotsTagUrls` . Výchozí `noindex, nofollow` .
- `xRobotsTagUrls` - seznam začátků adres URL oddělených čárkami pro nastavení hlavičky `X-Robots-Tag` . Pokud seznam obsahuje hodnotu `NOT_SEARCHABLE_PAGE` záhlaví je nastaveno i pro stránky s vypnutým vyhledáváním. Výchozí `/components/,NOT_SEARCHABLE_PAGE` .
- `xXssProtection` - hodnota záhlaví `X-XSS-Protection` pro ochranu před útokem XSS. Výchozí `1; mode=block` .

Nastavení záhlaví `Access-Control` pro přístup ke službám REST z jiných serverů:

- `accessControlAllowOriginValue` - hodnota záhlaví `Access-Control-Allow-Origin` pro URL set v proměnné `accessControlAllowOriginUrls` . V hodnotě můžete použít makro (viz níže). Ve výchozím nastavení nastaveno na `{HTTP_PROTOCOL}://{SERVER_NAME}:{HTTP_PORT}` .
- `accessControlAllowOriginUrls` - seznam začátků adres URL oddělených čárkami pro nastavení hlavičky `Access-Control-Allow-Origin` . Výchozí nastavení je `/rest/,/private/rest/,/admin/rest/` .
- `accessControlAllowHeaders` - hodnota nastavení záhlaví `Access-Control-Allow-Headers` , se nastavuje pouze při generování záhlaví. `Access-Control-Allow-Origin` . Výchozí `Origin, Accept, X-Requested-With, Content-Type, Access-Control-Request-Method, Access-Control-Request-Headers, x-csrf-token` .
- `accessControlAllowMethods` - hodnota nastavení záhlaví `Access-Control-Allow-Methods` , se nastavuje pouze při generování záhlaví. `Access-Control-Allow-Origin` . Výchozí `HEAD,POST,GET,OPTIONS,PUT` .
- `accessControlMaxAge` - hodnota nastavení záhlaví `Access-Control-Max-Age` , se nastavuje pouze při generování záhlaví. `Access-Control-Allow-Origin` . Výchozí `1800` .
- `accessControlAllowedOrigins` - pokud není prázdný, vyžaduje v požadavku hlavičku `origin` jehož hodnota musí být v tomto seznamu (seznam oddělený čárkou nebo novým řádkem). Nastavuje se pouze při generování záhlaví `Access-Control-Allow-Origin` .
Ve výchozím nastavení prázdné.

Pokud potřebujete nastavit jinou hlavičku HTTP, můžete použít aplikaci [Hlavičky HTTP](https://docs.webjetcms.sk/latest/cs/admin/settings/response-header/README) (<https://docs.webjetcms.sk/latest/cs/admin/settings/response-header/README>) v části Nastavení.

V hodnotě můžete použít makro `{HTTP_PROTOCOL}`, `{SERVER_NAME}/{DOMAIN_NAME}/{DOMAIN_ALIAS}`, `{HTTP_PORT}` , která bude nahrazena hodnotou získanou na serveru. `SERVER_NAME` je název domény z `request.getServerName()` , `DOMAIN_NAME` a `DOMAIN_ALIAS` jsou hodnoty domény nebo aliasu nastavené na webové stránce. Hodnota `{INSTALL_NAME}` představuje název instalace. Hodnota `{HEADER_ORIGIN}` obsahuje hodnotu hlavičky HTTP `origin` .

Ve starších instalacích bylo také možné nastavit hlavičky HTTP pomocí proměnné `conf.responseHeaders` ve kterém můžete nastavit hlavičku pro prefix adresy URL (začátek adresy URL). Na každém řádku zadáte hodnotu ve formátu: `url-prefix:hlavička:hodnota`, například:

```
/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 prostřednictvím konfigurační proměnné `responseHeaders` jsou globální bez ohledu na aktuální doménu.

1.1.4. Pravidla pro zadávání hesel

Pravidla hesla lze nastavit pomocí následujících konfiguračních proměnných (výchozí hodnota je uvedena v závorce vedle proměnné):

- `passwordAdminMinLength` - Určuje minimální délku hesla pro správce (5).
- `passwordAdminMinCountOfSpecialSigns` - Určuje minimální počet výskytů speciálních znaků v hesle správce (0).
- `passwordAdminMinUpperCaseLetters` - Určuje minimální počet výskytů velkých písmen v hesle správce (1).
- `passwordAdminMinLowerCaseLetters` - Určuje minimální počet výskytů malých písmen v hesle správce (0).
- `passwordAdminMinCountOfDigits` - Určuje minimální počet výskytů čísel v hesle pro správce (1).
- `passwordAdminExpiryDays` - Určuje počet dní platnosti hesla pro správce. Po uplynutí této doby bude uživatel vyzván ke změně hesla.

Hodnota 0 znamená, že platnost hesla (0) se nekontroluje.

Podobně lze nastavit pravidla hesla pro přihlášení do zabezpečené oblasti webu (nikoliv do administrace), proměnné jsou stejné, ale neobsahují výraz `Admin`. Název proměnné je tedy např. `passwordMinUpperCaseLetters`.

Nastavením konfigurační proměnné `isGoogleAuthRequiredForAdmin` na adrese `true` bude pro přístup k `/admin` části vyžadovány dvoufaktorové ověření. Každý uživatel si ho musí předem nastavit v administraci kliknutím na své jméno vpravo nahoře a výběrem možnosti

Dvoufaktorové ověření nebo otevřením stránky `/admin/2factorauth.jsp`.

Doporučujeme nastavit dvoufaktorové ověřování alespoň pro všechny účty, které lze použít ke správě uživatelských účtů a oprávnění a k nastavení konfigurace systému.

WebJET při změně hesla kontroluje historii a nedovolí opakované použití stejného hesla. To je ovlivněno následujícími konfiguračními proměnnými:

- `passwordHistoryLength` - počet použitých uživatelských hesel, která jsou pamatována v historii (ve výchozím nastavení 6).
- `passwordHistoryEnabled` - pokud je nastavena na `true` historie hesel je kontrolována v databázi a není povoleno měnit heslo, které bylo použito v minulosti (ve výchozím nastavení `true`).

Při žádosti o změnu hesla se používají následující proměnné:

- `passwordResetValidityInMinutes` - časová platnost v minutách pro odeslaný odkaz na změnu hesla (výchozí 30).
- `changePasswordPageUrl` - adresa stránky pro změnu hesla (výchozí `/components/user/change_password.jsp`).

1.1.5. Blokování přihlášení

Po nesprávné kombinaci uživatelského jména a hesla WebJET zablokuje další přihlášení ze stejné IP adresy. Je možné nastavit následující konfigurační proměnné:

- `loginBlockedDelay` - Doba v sekundách, po kterou se nebude možné znovu přihlásit po zadání nesprávného jména/hesla (výchozí 10).
- `loginBlockedAfterUnsuccessCount` - počet neúspěšných přihlášení, po kterých se prodleva definovaná v položce `loginLoginBlockedDelay` (výchozí hodnota 5).
- `loginLoginBlockedDelay` - dobu v sekundách, po kterou se nebude možné po zadání špatného hesla znovu přihlásit, a `loginBlockedAfterUnsuccessCount` počet neúspěšných přihlášení pro zadané přihlašovací jméno (výchozí 60).

Ve výchozím nastavení je tedy použita hodnota 10 sekund (`loginBlockedDelay`), pokud je zadán více než pětkrát za sebou (`loginBlockedAfterUnsuccessCount`) se použije zpoždění 60 sekund (`loginLoginBlockedDelay`).

Během doby uzamčení přihlášení se počítadlo neúspěšných pokusů stále nezvyšuje a čas se neprodlužuje, protože se vůbec nevolá přihlašovací kód.

1.1.6. Algoritmus hashování hesel

Z verze `2022.40` algoritmus BCrypt se v implementaci používá k hašování hesel.

`org.springframework.security.crypto.bcrypt.BCrypt` .

Možné nastavení:

- `bcryptSaltRounds` (výchozí 12) - log2 počtu opakování převrácení
- `passwordHashAlgorithm` (výchozí nastavení `bcrypt`) - název hashovacího algoritmu, možné hodnoty `bcrypt` nebo `sha-512` .

Dřívější verze používaly algoritmus `SHA-512` se 100 opakováními. Starší hodnoty hash hesel se při změně hesla uživatele změní na algoritmus `bcrypt`. Chcete-li změnu algoritmu vynutit, můžete nastavit proměnnou `conf. passwordAdminExpiryDays` na nenulovou hodnotu, což uživatele po přihlášení vyzve ke změně hesla.

1.1.7. Přihlášení do správy

Přihlašování do administrace je rovněž ovlivněno výše uvedenými konfiguračními proměnnými:

- `adminEnabledIPs` - obsahuje čárkou oddělený seznam IP adres, ze kterých je přístup k serveru `/admin` díly.
- `multidomainAdminHost` - umožňuje nastavit samostatnou doménovou adresu pro přístup k `/admin` díly, např. `cms.domena.sk` . Po nastavení bude hovor `/admin` adresy na jiných doménách vrátit chybu 404 - Stránka neexistuje.
- `isGoogleAuthRequiredForAdmin` - zapnutí dvoufaktorového ověřování při přihlašování do správy. `/admin` .
- `clusterMyNodeType` - v případě clusteru nastaví režim uzlu pouze uzly nastavené na hodnotu `full` obsahují administraci a umožňují přihlášení.
- `auditDontLogUsrlogin` - po nastavení na `true` přihlášení běžných uživatelů (neadministrátorů) nebudou kontrolována. Vhodné pro velmi zatížený intranet, kde zbytečně zahrnuje audit (ve výchozím nastavení `false`).

Uživatel, který se úspěšně autorizuje, musí navíc splňovat následující kritéria:

- `Schválený používateľ` - na účtu musí být tato možnost vybrána.
- `Začiatok platnosti` - pokud zadaná hodnota musí být starší než aktuální datum.
- `Koniec platnosti` - pokud zadaná hodnota musí být větší než aktuální datum.
- `Povoľiť vstup do admin sekcie (správa web sídla)` - Účet musí mít tuto možnost povolenou, jinak není přístup do administrace možný.

V případě speciálních požadavků na přihlašování a ověřování uživatelů je možné implementovat vlastní přihlašovací třídu v jazyce Java a nastavit ji pomocí proměnné `conf. adminLogonMethod` . Zadaná třída Java se pak použije místo standardního přihlášení.

Při přihlášení s nesprávnými údaji [blokuje přihlášení](#).

1.1.8. Ověřování proti serveru LDAP

Při ověřování uživatele proti serveru LDAP lze nastavit následující konfigurační proměnné:

- `ldapProviderUrl` - Adresa URL serveru LDAP pro přihlášení do LDAP ve tvaru `ldap://ldap.local:389/DC=firma,DC=com??base`.
- `ldapPassword` - přihlašovací jméno technického uživatele pro načítání dat LDAP.
- `ldapUsername` - přihlašovací heslo technického uživatele pro načtení dat LDAP.
- `ldapUseSslProtocol` - používá při komunikaci se serverem LDAP protokol SSL. Na portu 636 serveru LDAP musí být povolen protokol SSL. Pokud se používá `ldapS://`, ponechte hodnotu `false`.
- `NTLMForbiddenURL` - URL adresy odepřeného přístupu (ve výchozím nastavení `/500.jsp`).
- `NTLMDomainController` - název řadiče domény.
- `ldapDomainAppend` - pokud je nutné přihlásit se celou doménou, je možné zadat její doplnění k zadanému přihlašovacímu jménu uživatele.
- `ldapSecurityPrincipalDn` - nastaví speciální `SECURITY_PRINCIPAL`. Např. `cn=!USERNAME!,dc=ad,dc=interway,dc=sk` s tím, že `!USERNAME!` je nahrazen přihlašovacím jménem. Pokud je prázdné, použije se `ldapUsername+ldapDomainAppend`.
- `ldapFilter` - přihlašovací filtr pro přihlášení LDAP, pomocí kterého se vyhledává účet (výchozí hodnota `(&(objectClass=Person)(&(sAMAccountName=!USERNAME!)))`).
- `basicNtlmLogonAttrs` - Seznam atributů, které se mají načíst ze serveru LDAP při přihlašování. Pokud je prázdný, ověří se pouze přihlášení a uživatel se neaktualizuje podle hodnot na serveru LDAP. Výchozí `mail,title,givenName,sn,streetAddress,l,postalCode,co,company,telephoneNumber,mobile,description,memberOf,distinguishedName`.
- `ntlmDefaultUserPhoto` - pokud je nastavena na neprázdnou hodnotu a uživatel nemá fotografii v LDAP, nastaví fotografii na zadanou adresu URL.

Nastavení práv:

Po přihlášení se název uživatelské skupiny a práva skupiny automaticky porovnají se skupinami v LDAP (atribut `memberOf`). Pokud jméno odpovídá skupině ve WebJET, je uživatel přiřazen. Kromě toho je možné nastavit:

- `NTLMAdminGroupName` - Název skupiny LDAP, která identifikuje, že účet má administrátorský přístup (např. `WebJETAdmins`).
- `passwordProtectedAutoId` - Čárkou oddělený seznam ID uživatelských skupin, které budou uživateli automaticky přiřazeny po úspěšném přihlášení.

1.1.9. Konfigurace aplikačního serveru Tomcat

Předpokládáme, že webové stránky/aplikace budou přístupné prostřednictvím zabezpečeného protokolu `httpS`. Proto je nutné nastavit atribut `secure="true"`, [Konektor HTTP/AJP \(https://tomcat.apache.org/tomcat-9.0-doc/config/http.html\)](https://tomcat.apache.org/tomcat-9.0-doc/config/http.html) aby byl soubor cookie relace přístupný pouze prostřednictvím zabezpečeného protokolu `httpS`. Nastavení provedete v souboru `tomcat/conf/server.xml`. Atribut `useBodyEncodingForURI="true"` nastaví pro adresu URL stejné kódování znaků, jaké se používá pro tělo stránky.

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

xml

pokud použijete nezabezpečený protokol `HTTP`, prohlížeč soubor cookie relace nepřijme a relace se neudrží (to se projeví opakovaným zobrazením přihlašovacího okna, jakmile zadáte správné přihlašovací údaje).

Vyhnutí se zobrazení verze aplikačního serveru při zobrazení chyby `Tomcat` a `Stack Trace` je třeba v souboru `server.xml` `<Host` prvek přidat konfiguraci [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"
```

xml


```

        showReport="false"
        showServerInfo="false" />
</Host>

```

v případě potřeby můžete také vytvořit statickou html stránku v kódování `utf-8` s chybovou zprávou a nakonfigurujte ji jako:

```

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

```

V konfiguračním souboru `server.xml` doporučujeme tuto možnost správně nastavit `defaultHost`. Útočníci mohou hlavičku upravit `Host` a tím přesměrovat požadavek z internetu, např. na hostitele pro správu, který nemusí být z internetu přístupný (pokud jsou uzly pro správu i veřejné uzly clusteru spuštěny na stejném aplikačním serveru). Příkladem je použití `localhost` které lze přiřadit serveru pro správu, a upravený požadavek tak může skončit v uzlu pro správu.

Hodnota `defaultHost` doporučujeme směřovat na neexistující `<Host>` v takovém případě aplikační server ohlásí chybu, že takový prvek je chybný. `host` neví. Aplikační server tedy neznámé domény nezpracovává. Nevýhodou tohoto řešení je, že po přidání nové domény je nutné ji přidat jako `<Alias>` také na aplikační server.

Pokud používáte nástroj Load Balancer, musíte zajistit, aby na aplikační servery odesílal pouze známé domény (whitelist). Na neznámé domény musí odpovědět chybou.

```

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

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

```

1.1.10. Oznámení o změnách

Doporučujeme nastavit zaslání oznámení bezpečnostnímu technikovi pro následující typy událostí:

- `CONF_UPDATE` a `CONF_DELETE` - změna/odstranění konfigurační proměnné
- `PROP_UPDATE` a `PROP_DELETE` - změna/odstranění překladového klíče (kód JavaScriptu lze vložit také prostřednictvím překladového klíče).

Oznámení můžete nastavit v administraci v části Audit->Oznámení. Bezpečnostní technik bude o těchto změnách informován a v případě podezření na útok může reagovat.

1.1.11. Zabezpečení serveru

Důležité je také zabezpečení samotného serveru a použitého softwaru. Aktualizujte software na nejnovější podporované verze. Na serveru je také vhodné nainstalovat antivirový program, který bude kontrolovat nahrávané soubory a v případě, že v některém souboru zjistí virus, zabrání přístupu k tomuto souboru.

1.2. Nastavení služby Vyrovnávání zatížení

Pokud je před aplikačními servery předinstalován Load Balancer, je nutné zajistit:

- Směřovat pouze definované domény na aplikační servery, aby nemohlo dojít k útoku změnou. `Host` záhlaví. Load Balancer nesmí povolit odeslání neznámé domény na aplikační server.
- WebJET přebírá nastavení IP adresy z hlavičky HTTP. `X-Forwarded-For` při nastavování konfigurační proměnné `serverBeyondProxy=true`. Je tedy nutné zajistit, aby taková hlavička HTTP nepocházela z internetu, ale Load Balancer ji vždy přepíše na správnou hodnotu - IP adresu návštěvníka. Totéž platí pro hlavičku HTTP `x-forwarded-proto`. Nesprávné nastavení hlavičky může vést k přístupu k částem, které jsou povoleny pouze pro určité IP adresy, jako je například správa.

1.3. Nastavení WAF

Pokud je aplikační server předdefinován `Web Application Firewall/WAF` je třeba nastavit **výjimky pro správu**. Některé požadavky HTTP v administraci mohou být detekovány jako útok XSS/SQL Injection, protože požadavek HTTP může odesílat kód JavaScript nebo příkaz SQL. Příkladem je ukládání webové stránky, kdy může být potřebný kód JavaScriptu vložen do pole kódu HTML v záhlaví, nebo ukládání záznamů v aplikaci Skripty, kde je kód JavaScriptu vložen přímo.

Ideálním řešením je použití clusterového řešení s vyhrazeným uzlem CMS v místní síti, který není přístupný z vnějšího prostředí. V takovém případě lze WAF pro uzel CMS vynechat.

Správa používá služby REST začínající na adrese URL `/admin/rest`, viz doporučení pro [Pravidla URL](https://docs.webjetcms.sk/latest/cs/custom-apps/spring/rest-url) (<https://docs.webjetcms.sk/latest/cs/custom-apps/spring/rest-url>). V systému WAF je třeba nastavit výjimky pro adresy URL začínající na:

- `/admin/rest/web-pages` - ukládání webových stránek
- `/admin/rest/components/insert-script` - Skripty aplikací
- `/admin/v9/settings/translation-keys` - překladové klíče - v některých případech může být nutné vložit do překladového klíče kód HTML.
- `/admin/rest/settings/configuration` - konfigurace, platí podobně jako u překladových klíčů
- `/admin/searchall.jsp` - vyhledávání v administraci, může být nutné vyhledat výraz HTML/JavaScript.
- `/admin/replaceall.jsp` - nahrazení výrazu v administraci, podobně jako při hledání
- `/admin/updatedb.jsp` - provedení zadaného příkazu SQL

Ostatní adresy URL by měly být nastaveny na základě používaných aplikací.

1.4. Řešení zjištění zabezpečení

- `Sensitive Data Exposure`

Prostřednictvím chybových odpovědí serveru bylo možné zjistit typ a verzi použitého webového serveru.

Řešení: Ověřte nastavení hlavičky HTTP `Server`, ve WebJETu lze přebudovat v konfigurační proměnné `serverName`, viz výše.

- `RCE via uploaded JSP file`

WebJET CMS umožňuje nahrávání libovolných souborů, včetně souborů JSP, které umožňují spuštění libovolných příkazů na běžícím serveru.

Chybě lze zabránit nastavením práv pro nahrávání souborů nebo úplným zamezením zápisu souborů programu.

Řešení: upravte nastavení práv pro nahrávání souborů pomocí konfiguračních proměnných `FCKConfig.Upload*`, viz výše.

- `MaliciousFileUpload`

Server nemá antivirovou kontrolu, takže je možné na něj nahrát škodlivé soubory.

Řešení: Nainstalujte na server antivirový program.

- Missing Secure cookie flag

Soubor cookie relace (`JSESSIONID`) nemá nastaven atribut zabezpečení `Secure` .

Řešení: kontrola a nastavení `secure` atribut v souboru `server.xml` (<https://tomcat.apache.org/tomcat-9.0-doc/config/http.html>) Aplikační server Tomcat, viz výše.

- Missing HTTP Strict Transport Security policy

Aplikace nenastavuje hlavičku HTTP `Strict Transport Security` .

Řešení: hodnota [Záhlaví Strict Transport Security](https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) (https://en.wikipedia.org/wiki/HTTP_Strict_Transport_Security) lze nastavit v konfigurační proměnné `strictTransportSecurity=max-age=31536000 ; includeSubDomains` , viz. výše.

- Stored XSS cez SVG obrázok

Soubor SVG umožňuje vložit do těla JavaScript kód, v případě přímého zobrazení takového souboru v prohlížeči se kód JavaScript spustí (v případě standardního vložení přes aplikaci `img` kód se neprovede a zobrazení je bezpečné).

Řešení: Omezte možnost nahrávat soubory SVG, viz nastavení práv výše. Jako ochranu WebJET CMS generuje hlavičku HTTP pro soubory SVG `Content-Security-Policy` s hodnotou `default-src 'self'` který [zabraňuje spuštění kódu javascript](https://github.com/digininja/svg_xss) (https://github.com/digininja/svg_xss) při přímém zobrazení obrázku. Hodnotu lze nastavit pomocí konfigurační proměnné `contentSecurityPolicySvg` .

Pro ověření chování vytvořte soubor SVG s následujícím obsahem, nahrajte jej do systému WebJET CMS, vložte jej do testovací stránky a ověřte její zobrazení a (ne)provedení útoku XSS:

```
<?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 úpravou překladových klíčů

Prostřednictvím překladových textů je editor schopen provést útok typu `Cross Site Scripting` proti ostatním návštěvníkům stránek nebo jiným správcům.

Překladové klávesy se používají také k vkládání kódu HTML (např. odkaz na podmínky v kalkulačce, tučné písmo, nastavení stylů CSS), takže tato aplikace technicky umožňuje vkládat také kód HTML/JavaScript (to je vlastnost, nikoli chyba). Všimněte si, že editor může vkládat kód JavaScriptu i přímo v editoru stránky, není žádný zásadní důvod mu bránit i v úpravě překladových klíčů.

Řešení: Minimalizujte počet uživatelů s přístupem k aplikaci Překlad textu. Uživatelé, kteří nemají oprávnění "Upravovat texty - zobrazit všechny texty", mají zároveň omezené možnosti úprav. Mohou upravovat pouze vybrané klíče (nastavené prostřednictvím konf. proměnné `propertiesEnabledKeys`) a zároveň je upravená hodnota filtrována a umožňuje pouze definované značky a atributy HTML. Ty se nastavují v proměnné konf. `propAllowedTags` kde jsou ve výchozím nastavení povoleny značky `p,div,a,sub,sup,br,strong` a atributy v proměnné konf. `propAllowedAttrs` kde jsou ve výchozím nastavení povoleny atributy `href,src,style,class,rel` . Pokud chcete uživatelům bez oprávnění "Upravovat texty - zobrazovat všechny texty" zcela zamezit vkládání kódu HTML, můžete nastavit proměnnou konf. `propAllowedTags` na prázdnou hodnotu (nebo znak `-`). Nastavením na znak `*` ochrana je vypnutá.

Jako další ochranu doporučujeme nastavit oznámení při změně na bezpečnostního inženýra, viz výše.

- `Insecure Deserialization`

Import webové stránky obsahuje dokumenty .xml se serializovanými objekty java. Tyto dokumenty .xml však mohou být upraveny a obsluhovány vlastními serializovanými objekty java typu `<object class="java.lang.Runtime" method="getRuntime">` které provedou zadanou operaci přímo na serveru.

Pro úspěšné zneužití je nutné upravit proměnnou `conf.xmlDecoderAllowedClasses` který obsahuje seznam povolených deserializovaných objektů, a přidejte tam hodnotu `java.lang.Runtime`.

Řešení: Běžný uživatel nesmí mít oprávnění k úpravě konfiguračních proměnných, ty by měla upravovat pouze k tomu určená osoba. Jako dodatečnou ochranu jsme přímo do kódu (bez možnosti editace tohoto seznamu) přidali nepovolené typy objektů, které nelze přidat (povolit) prostřednictvím konfigurace.

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

Pro `cookies` lze nastavit atribut `SameSite` (<https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers/Set-Cookie/SameSite>) zabránit odesílání souborů cookie při útoku CSRF (zabránit odesílání souborů cookie do jiných domén).

V současné době v `servlet-api` podpora pro nastavení této hodnoty ve verzi 5.x se chystá, což může znamenat dlouhé čekání na přímou programátorskou podporu. Při použití Apache Tomcat je však možné tuto hodnotu nastavit v konfiguraci pomocí příkazu `CookieProcessor` (<https://tomcat.apache.org/tomcat-8.5-doc/config/cookie-processor.html>), což ve standardní implementaci umožňuje nastavit hodnotu:

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

xml

2. Kontrola zranitelnosti knihoven

Použití nástroje **Kontrola závislostí OWASP** (<https://jeremylong.github.io/DependencyCheck/index.html>) můžete snadno zkontrolovat zranitelnosti v knihovnách Java a JavaScript webové aplikace. Doporučujeme je pravidelně kontrolovat.

Pokud máte přístup ke zdrojovému kódu/gradu projektu, můžete analýzu spustit přímo pomocí příkazu `příkaz gradlew` (<https://docs.webjetcms.sk/latest/cs/developer/backend/security>).

Nástroj však lze spustit i nad vygenerovanými `war` archiv webových aplikací. Nainstalujte verzi nástroje pro `příkazový řádek` (<https://jeremylong.github.io/DependencyCheck/dependency-check-cli/index.html>).

Kontrolu pak můžete spustit pomocí příkazu:

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

sh

jsou nastaveny parametry:

- `--project` - název projektu, který se zobrazí v sestavě.
- `--suppression` - způsob, jak `soubor s výjimkami` (<https://docs.webjetcms.sk/latest/cs/developer/backend/security>), obvykle je tento soubor součástí repozitáře git.
- `--scan` - cesta k analyzovanému souboru/adresáři.

Výsledkem je sada `dependency-check-report.html` v aktuálním adresáři.



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@9.0-war: webjet-8.9-SNAPSHOT-admin-jar: ckeditor.js		pkg-javascript:ckeditor@4.5.0-beta	low	7		3

3. Aktualizace WebJET

Sekce Aktualizace WebJET slouží k aktualizaci verzí WebJET. V levé části obrazovky je zobrazen seznam dostupných verzí WebJET, na které lze váš WebJET aktualizovat. Aktuální verze vašeho WebJETu je v seznamu označena ikonou

Po kliknutí na jednotlivé verze se v pravé části obrazovky zobrazí seznam všech změn, které vybraná verze přináší.



Varování: aktualizujte WebJET pouze v případě, že víte, co děláte. Před aktualizací se obraťte na poskytovatele hostingu a požádejte ho o podporu. Může se stát, že WebJET po aktualizaci nenaběhne správně a bude nutné restartovat server.

Pokud váš projekt obsahuje další knihovny JAR, musíte je umístit do složky `/WEB-INF/lib-custom/`. Složka je během aktualizace plně nahrazena `/WEB-INF/lib/` a vaše knihovny by tak byly odstraněny. To může mít za následek nemožnost spuštění systému po restartu. Pokud taková situace nastane, zkopírujte chybějící knihovny do adresáře `/WEB-INF/lib/` od zálohy.

5. Typy auditních záznamů

Každý auditní záznam automaticky zaznamenává datum a čas, ID přihlášeného uživatele, IP adresu, a pokud je povolen reverzní server DNS, i název počítače. Do textu auditního záznamu se automaticky vloží název uzlu clusteru, adresa URI, doména a hodnota http hlavičky User-Agent.

- **ADMINLOG_NOTIFY** - změna v seznamu oznámení v aplikaci Audit.
- **BANNER** - operace v aplikaci Banner System
- **BASKET** - operace v aplikaci E-Commerce
- **CALENDAR** - operace v aplikaci Kalendář událostí
- **CONF_DELETE** - při mazání konfigurační proměnné zaznamená její název.
- **CONF_UPDATE** - změna nebo přidání konfigurační proměnné (v sekci Nastavení), zaznamená název, aktuální hodnotu a novou hodnotu proměnné.
- **COOKIE_ACCEPTED** - přijímání souborů cookie na webových stránkách
- **COOKIE_REJECTED** - odmítnutí používání souborů cookie na webových stránkách
- **CRON** - zaznamenává úlohy spuštěné na pozadí, pokud je zaškrtnuta možnost Audit. Ukládá také chyby během provádění úlohy (pokud se vyskytnou), v takovém případě se protokoluje **Stack Trace**.
- **DATA_DELETING** - zaznamená provedení vymazání dat v části Nastavení-Vymazání dat. Zaznamená klíč, který byl odstraněn v mezipaměti, nebo **ALL** odstranit vše. Při mazání mezipaměti obrázků zaznamená cestu k adresáři. Při mazání trvalé mezipaměti zaznamená ID záznamu.
- **DMAIL** - Aplikace pro hromadné zasílání e-mailů
- **DMAIL_AUTOSENDER** - používá se ve zvláštní situaci automatického odesílání hromadných e-mailů.
- **DMAIL_BLACKLIST** - změna v sekci Hromadné e-maily->Odebrané e-maily
- **DMAIL_DOMAINLIMITS** - změna v sekci Hromadný e-mail->Omezení domény
- **EXPORT_WEBJET** - nepoužívá se
- **EXPORT** - operace exportu dat (přidání, změna, odstranění exportu dat).
- **FILE_CREATE** - vytvořit soubor nebo adresář, zaznamenat cestu
- **FILE_DELETE** - při mazání souboru nebo adresáře zaznamená cestu.
- **FILE_EDIT** - přejmenování nebo úpravě souboru zaznamená cestu.
- **FILE_SAVE** - uložení souboru, např. při kopírování/přesouvání atd. Zaznamenat cestu k souboru
- **FILE_UPLOAD** - Nahrání souboru do WebJETu, a to buď klasickým odesláním, nebo metodou Drag & Drop. Obvykle se zaznamená cesta k nahranému souboru.
- **FORMMAIL** - odeslání formuláře. Úspěšné odeslání zaznamená pomocí zprávy **FormMail formName:** název formuláře, seznam příjemců a **referer**. V případě neúspěchu zaznamená důvod neodeslání spolu s hlášením. **ERROR: formName:** název formuláře, **fail:** důvod neposílání. Zaznamenává také detekci spamu hlášením **detectSpam TRUE:** důvod pro detekci jako spamu.
- **FORM_ARCHIVE** - archivace formuláře, zaznamená název formuláře.
- **FORM_DELETE** - smazání formuláře, zaznamená název formuláře a případně ID, pokud se jedná o smazání jednoho záznamu.
- **FORM_EXPORT** - export formuláře přes záložku Export, v současné době není zaznamenán univerzální export přes tlačítka pod tabulkou. Datum posledního exportu je určeno tímto záznamem pro možnost exportu od posledního exportu.
- **FORM_REGEXP** - změna v sekci Formuláře->Pravidelné výrazy
- **FORM_VIEW** - nepoužívá se
- **FORUM_SAVE** - detekuje vulgaritu v diskusním fóru.
- **FORUM** - operace v aplikaci Diskuze
- **GALLERY** - změny v aplikaci Galerie - vytvoření adresáře, přidání/odstranění fotografie.
- **GDPR_FORMS_DELETE** - Aplikace GDPR, vymazání starých formulářů
- **GDPR_USERS_DELETE** - Aplikace GDPR, mazání starých uživatelů
- **GDPR_BASKET_INVOICES_DELETE** - Aplikace GDPR, mazání starých objednávek z elektronického obchodu
- **GDPR_EMAILS_DELETE** - Aplikace GDPR, mazání starých e-mailů
- **GDPR_REGEXP** - Aplikace GDPR, správa regulárních výrazů
- **GDPR_DELETE** - Aplikace GDPR, nastavení mazání dat
- **GDPR_COOKIES** - Aplikace GDPR, správa souborů cookie
- **GROUP** - vytvořit/uložit/odstranit adresář v sekci Webové stránky.
- **HELPPDESK** - nepoužívá se

- **HELP_LAST_SEEN** - se používá k zaznamenání data zobrazení sekce Co je nového v nápovědě. Při přihlášení tato sekce vyhledá nejnovější soubor a porovná jej se zaznamenaným datem v sekci Audit. Pokud existuje novější soubor, zobrazí se po přihlášení vyskakovací okno nápovědy s oddílem Co je nového.
- **IMPORTXLS** - Import souboru aplikace Excel, který se používá při implementacích u zákazníků. Zaznamenává cestu k importovanému souboru a jeho velikost.
- **IMPORT_WEBJET** - nepoužívá se
- **INIT** - Inicializace WebJET (start), zaznamená cestu k adresáři, ve kterém byl WebJET na aplikačním serveru spuštěn, a číslo verze WebJET.
- **INQUIRY** - operace v aplikaci Anketa
- **INQUIRY** - přidání otázky v aplikaci Anketa, zaznamená text otázky.
- **INSERT_SCRIPT** - změna v aplikaci Skripty
- **INVENTORY** - operace v aplikaci Property
- **JSPERROR** - chyba při spuštění souboru JSP při zobrazení webové stránky, zaznamenaná v protokolu **Stack Trace** chyby
- **MEDIA** - Operace s médii (karta Média na webové stránce).
- **MEDIA_GROUP** - Aplikace pro správu skupin médií.
- **PAGE_DELETE** - smazat, přesunout do koše nebo požádat o smazání stránky, zaznamenaná ID stránky.
- **PAGE_UPDATE** - záznamy změn na stránce mimo standardní ukládání v editoru - hromadné operace v seznamu stránek.
- **PAYMENT_GATEWAY** - volání platební brány v aplikaci E-Commerce.
- **PEREX_GROUP_CREATE** - vytvořit skupinu perex, zapsat její název
- **PEREX_GROUP_DELETE** - smazání perexu skupiny, zaznamenaná její název a ID.
- **PEREX_GROUP_UPDATE** - změnit perex skupiny, zapsat její název.
- **PERSISTENT_CACHE** - změna v sekci Odstranění dat->Persistentní objekty cache
- **PROP_DELETE** - vymazání textu překladu, zaznamenaná jazyk a klíč.
- **PROP_UPDATE** - editace textu překladu (v sekci Nastavení), záznam jazyka, klíče a hodnoty.
- **PROXY** - operace proxy aplikace
- **QA** - operace v aplikaci Otázky a odpovědi
- **REDIRECT_CREATE** - vytvořit nové přesměrování (url nebo doména).
- **REDIRECT_DELETE** - odstranění přesměrování (url nebo doména), zaznamenaná zdroj a v případě domény cíl přesměrování.
- **REDIRECT_UPDATE** - změna přesměrování (url nebo doména), záznam zdrojové a cílové adresy.
- **RUNTIME_ERROR** - zaznamenaná chybějící šablonu pro zobrazení stránky
- **SAVEDOC** - uložení webové stránky v Editoru, zaznamenává také žádosti o schválení. Zaznamenává název stránky, ID stránky a ID v historii
- **SENDMAIL** - odeslání e-mailu (mimo formuláře), zaznamenaná e-mail odesílatele, e-mail příjemce a předmět e-mailu.
- **SE_SITEMAP** - generování souborů `/sitemap.xml`, zaznamenaná ID adresáře, pro který je mapa stránek generována, a obsah hlavičky User-Agent.
- **SQLERROR** - databázi, zaznamenaná chybu SQL, zdroj chyby a **Stack Trace**
- **TEMPLATE_DELETE** - při odstraňování šablony zaznamenaná název odstraněné šablony.
- **TEMPLATE_INSERT** - vytvořit novou šablonu, zapsat její název
- **TEMPLATE_UPDATE** - změna v šabloně, záznam seznamu změněných polí
- **TEMPLATE_GROUP** - změna ve skupině šablon
- **TIP** - operace v aplikaci Tip dne
- **TOOLTIP** - změna v aplikaci Tooltip
- **UPDATEDB** - provádění změn v databázi prostřednictvím konzoly správce.
- **USER_AUTHORIZE** - autorizace uživatele (schválení přístupu do sekce chráněné heslem). Zaznamená ID smazaného uživatele, pokud je ID uživatele také známo. **login** a jméno.
- **USER_CHANGE_PASSWORD** - kontroluje změnu hesla uživatele. Na základě data se vypočítá interval změny hesla (je-li nastaven).
- **USER_DELETE** - odstranění uživatele. Zaznamená ID smazaného uživatele, pokud je známo, a jméno uživatele. **login** a jméno.
- **USER_EDIT** - zaznamenaná událost otevření editace uživatele, nejedná se ještě o uložení. Zaznamená ID uživatele, **login** a jméno.
- **USER_GROUP_DELETE** - odstranit skupinu uživatelů, zaznamenat název skupiny a její ID.
- **USER_GROUP_INSERT** - vytvořit novou skupinu uživatelů, zapsat název nové skupiny a její typ.
- **USER_GROUP_UPDATE** - uložit skupinu uživatelů, zaznamenat název skupiny a seznam změn.
- **USER_INSERT** - vytvoření nového uživatele (nebo nové registrace v sekci chráněné heslem). Zaznamenejte ID uživatele, **login** a jméno.

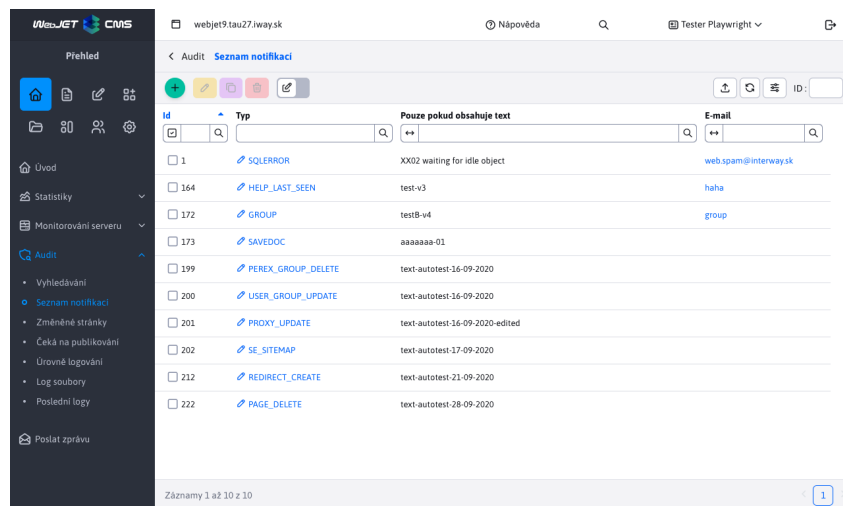
- **USER_LOGOFF** - odhlášení uživatele kliknutím na ikonu odhlášení, zaznamenaná přihlašovací jméno a informaci o tom, zda je uživatel správce nebo registrovaný návštěvník.
- **USER_LOGON** - přihlášení uživatele, zaznamenaná přihlašovací jméno a informaci o tom, zda je uživatel správcem nebo registrovaným návštěvníkem. Zaznamenaná také událost neplatného hesla, pokud uživatel není autorizován nebo přihlašovací jméno není známo.
- **USER_PERM_GROUP** - operace se skupinami práv, zaznamenává název skupiny a při změně seznam změn.
- **USER_SAVE** - zaznamenává změny uživatele v sekci chráněné heslem (pokud obsahuje formulář pro změnu údajů).
- **USER_UPDATE** - uložení existujícího uživatele. Zaznamená aktuální nastavení práv a změny zadaných údajů.
- **WEB_SERVICES** - volání zákazníků **WebServices** (použití závisí na implementaci pro konkrétního zákazníka)
- **XSRF** - XSRF útok na server (neautorizovaná hlavička referer), zaznamenaná hodnotu názvu domény z **referer** Záhloví
- **XSS** - Útok XSS na server nebo přímé (neautorizované) volání souboru JSP. Zaznamená adresu URL nebo výraz, který způsobil vyhodnocení útoku (např. neoprávněný token v adrese URL, neoprávněná metoda HTTP). Zaznamenává také krádež souborů cookie (změna IP adresy relace).

6. Zvláštní formát auditu

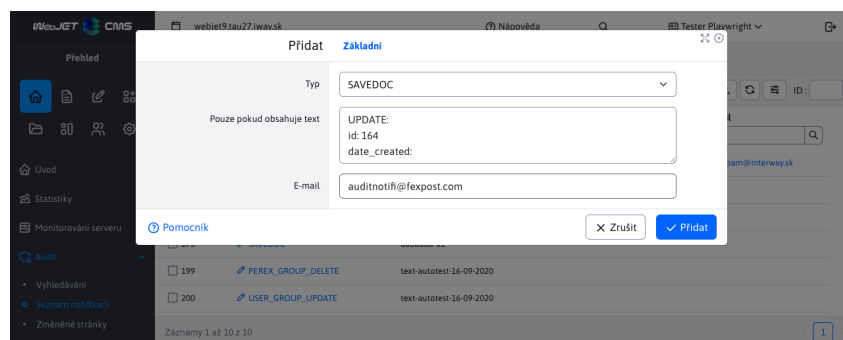
V případě potřeby lze do systému WebJET přidat kód, který uloží auditní záznamy do zvláštního souboru nebo je odešle určené službě. Je nutné nastavit konfigurační proměnnou `adminlogCustomLogger` do třídy jazyka Java, která implementuje třídu `sk.iway.iwcm.AdminlogCustomLogger`. Pro každou položku se volá metoda `addLog(logType, requestBean, descriptionParam, timestamp)`

7. Seznam oznámení

V položce nabídky Seznam oznámení můžete nastavit e-mailová oznámení pro určité systémové události/chyby. Doporučujeme nastavit upozornění na události typu **XSS** a **SQLERROR**.



V editoru můžete také nastavit další text, který musí chyba obsahovat, aby mohla být odeslána na zadaný e-mail.



8. Změněné stránky

V položce nabídky Změněné stránky se zobrazí seznam změněných stánek, seřazený od poslední změny. S těmito stránkami můžete pracovat stejným způsobem jako v nabídce [Seznam webových stránek](https://docs.webjetcms.sk/latest/cs/redactor/webpages/README) (<https://docs.webjetcms.sk/latest/cs/redactor/webpages/README>).

Všechny stránky se zobrazí bez ohledu na práva uživatele ke stromové struktuře stránek a vybrané doméně.

WebJET CMS

Přehled

Úvod

Statistiky

Monitorování serveru

Audit

- Vyhledávání
- Seznam notifikací
- Změněné stránky
- Čeká na publikování
- Úrovně logování
- Log soubory
- Poslední logy

Poslat zprávu

webjet9.tau27.iway.sk

Nápověda

Tester Playwright

Změněné stránky

ID

Stav

Název web stránky

Jméno autora

Poslední změna

Cesta

<input type="checkbox"/>	110308		Aktualita_B	Tester Playwright	12.11.2024 12:13:28	/System/K64/Aktuality/Aktualita_B/Aktualita_B
<input type="checkbox"/>	110307		Aktualita_A	Tester Playwright	12.11.2024 12:13:28	/System/K64/Aktuality/Aktualita_A/Aktualita_A
<input type="checkbox"/>	110306		Aktuality	Tester Playwright	12.11.2024 12:13:28	/System/K64/Aktuality/Aktuality
<input type="checkbox"/>	97032		lotr-meme.jpg	Tester Playwright	12.11.2024 12:04:48	/Jet portal 4/files/test-sivan/lotr-meme.jpg
<input type="checkbox"/>	97033		o_lotr-meme.jpg	Tester Playwright	12.11.2024 12:04:48	/Jet portal 4/files/test-sivan/o_lotr-meme.jpg
<input type="checkbox"/>	97034		s_lotr-meme.jpg	Tester Playwright	12.11.2024 12:04:48	/Jet portal 4/files/test-sivan/s_lotr-meme.jpg
<input type="checkbox"/>	110305		NewSubFolder	Blogger Permission	12.11.2024 09:58:47	/System/K64/NewSubFolder/NewSubFolder
<input type="checkbox"/>	110304		Subfolder-autotest	Tester Playwright	12.11.2024 09:54:18	/clone-dest-autotest11129/Subfolder-autotest/Subfolder-autotest
<input type="checkbox"/>	110303		New page-autotest	Tester Playwright	12.11.2024 09:54:17	/clone-dest-autotest11129/New page-autotest
<input type="checkbox"/>	110302		clone-dest-autotest11129	Tester Playwright	12.11.2024 09:54:13	/clone-dest-autotest11129/clone-dest-autotest11129
<input type="checkbox"/>	110301		Subfolder-autotest	Tester Playwright	12.11.2024 09:54:03	/clone-src-autotest11129/Subfolder-autotest/Subfolder-autotest

Záznamy 1 až 11 z 5,889

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 536

9. Čeká se na zveřejnění

Položka nabídky Čekající obsahuje seznam stránek, jejichž zveřejnění je naplánováno v budoucnu. Obsahuje informace o tom, jaká webová stránka (na jaké adrese/cestě) a kdy bude zveřejněna. Další informace o webových stránkách naleznete zde [Seznam webových stránek](https://docs.webjetcms.sk/latest/cs/redactor/webpages/README) (<https://docs.webjetcms.sk/latest/cs/redactor/webpages/README>).

Cílem je přehledně zobrazit seznam stránek, které budou v budoucnu automaticky změněny. Zobrazí se všechny stránky bez ohledu na práva uživatele ke stromové struktuře stránek a vybrané doméně.

Webové stránky, které čekají na vypnutí zobrazení, jsou zobrazeny červeně - po tomto datu jsou nastaveny na stránku Publikovat. Takové stránky nebudou po nastaveném datu veřejně zobrazitelné.

V seznamu se nezobrazují stránky v koši, ty se nezveřejňují.

WebJET CMS

Přehled

Úvod

Statistiky

Monitorování serveru

Audit

- Vyhledávání
- Seznam notifikací
- Změněné stránky
- Čeká na publikování
- Úrovně logování
- Log soubory
- Poslední logy

Poslat zprávu

webjet9.tau27.iway.sk

Nápověda

Tester Playwright

Čeká na publikování

ID

Dec ID

Název

Začátek

Konec

Cesta

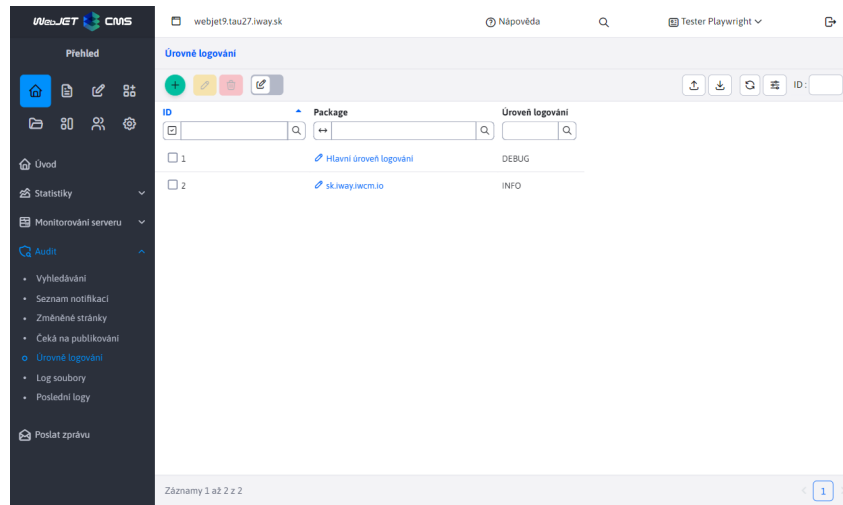
<input type="checkbox"/>	0	105723	Test odpublikování v budoucnosti	27.09.2024 11:34:29	01.12.2030 06:00:00	/Test stavov/Test odpublikování v budoucnosti
<input type="checkbox"/>	180519	108610	Publish notification screenshot			/Test stavov/Publish notification screenshot
<input type="checkbox"/>	180520	108610	Publish notification screenshot			/Test stavov/Publish notification screenshot
<input type="checkbox"/>	180522	108611	Publish notification screens			/Test stavov/Publish notification screens
<input type="checkbox"/>	183343	22955	Test publikování v budoucnosti	01.12.2030 06:00:00		/Test stavov/Test publikování v budoucnosti

Záznamy 1 až 5 z 5

1

10. Úrovně logování

Aplikace Úrovně protokolování umožňuje spravovat úrovně protokolování pro jednotlivé balíčky java.



První záznam v tabulce je vždy **Hlavní úroveň logování** (základní úroveň).

Používají se 2 konfigurační proměnné:

- **logLevel**, obsahuje hodnotu úrovně protokolování pro **Hlavní úroveň logování**
- **logLevels**, obsahuje seznam balíčků java s úrovněmi protokolování (každý na novém řádku). Např:

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

Změny nad tabulkou se ukládají lokálně do konstanty. Pokud chcete změny (nastavení) uložit trvale, musíte v editoru vybrat možnost **Uložit do databáze**. Po uložení se aktualizují konfigurační proměnné v databázi.

11. Přidat

Pro přidání akcí je vyžadována hodnota balíčku java a úroveň protokolování. Pokud zadáte již přidáný balíček, nevytvoří se duplicitní hodnota, ale stávající se aktualizuje.

Přidat

Základní

Package

Úroveň logování

DEBUG

Uložit do databáze

Uložit všechny úrovně logování do databáze

Ano

Pomocník

X Zrušit

✓ Přidat

12. Upravit podle

Akce úprav se chová odlišně pro hlavní úroveň protokolování a pro ostatní úrovně protokolování.

12.1. Hlavní úroveň logování

Při úpravách hlavní úrovně můžeme vybrat pouze protokolování NORMAL nebo DEBUG (pro podrobné protokolování). Pokud v editoru změníte hodnotu `Package` , nebude provedena žádná změna. Protože hlavní úroveň musí být stále přítomna, lze měnit pouze hodnotu úrovně protokolování.

12.2. Ostatní těžba dřeva

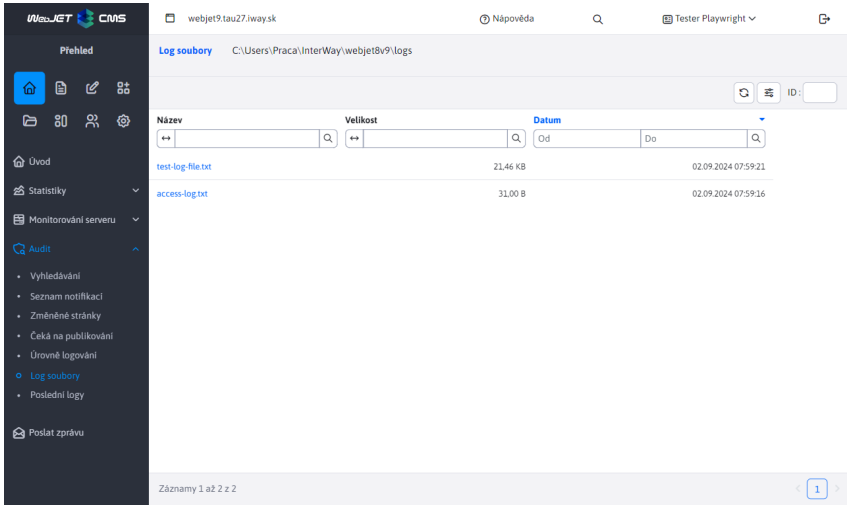
Změna úrovně protokolování se uloží, pokud změníte balíček, původní protokolování zmizí a bude nahrazeno tímto novým. Povoleny jsou všechny úrovně protokolování kromě hodnoty NORMAL.

13. Mazání

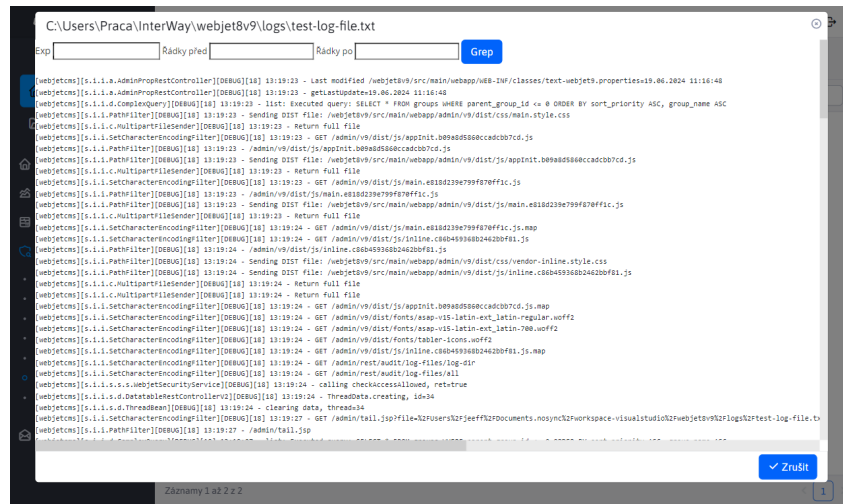
Všechny balíčky úrovně protokolování lze odstranit s výjimkou **Hlavní úroveň protokolování**. Když se jej pokusíte odstranit, nic se s ním nestane (nezmění se ani hodnota).

14. Soubory protokolu

Aplikace poskytuje přehled všech souborů protokolu. Úpravy nad tabulkou nejsou povoleny. Tabulka slouží pouze pro přehled. V levé horní části stránky je zobrazena cesta, kde jsou tyto soubory uloženy.

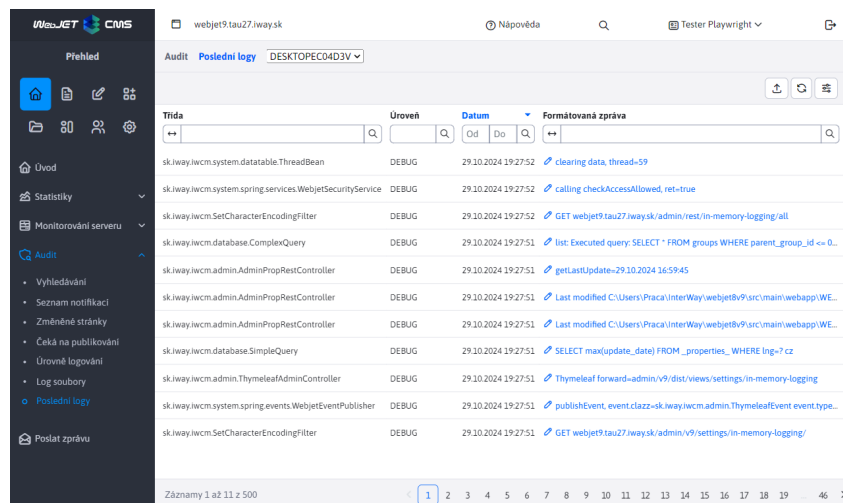


Po kliknutí na název souboru se zobrazí okno s obsahem souboru. Záhlaví obsahuje pole pro možnost filtrování souboru pomocí regulárních výrazů (nebo přímo pouze podle hledaného výrazu).



15. Nejnovější protokoly

Aplikace je navržena tak, aby zobrazovala nejnovější protokoly pro případ, že nemáte přístup k protokolům v souborovém systému. Zobrazuje protokoly, které procházejí logovacím rámcem (tj. používají třídu `Logger`), nezobrazuje protokoly zapsané přímo prostřednictvím `System.out` nebo `System.err`.



Podporuje clustering, takže je možné vyžádat si poslední protokoly z jiného uzlu clusteru. Na kartě `Stack Trace` výpis zásobníku (obsah se však zobrazuje pouze u chybových protokolů, u standardních úrovní protokolů je prázdný).

15.1. Možnosti/nastavení konfigurace:

- `loggingInMemoryEnabled` - nastavením na hodnotu `true/false` Povolení nebo zakázání ukládání protokolů.
- `loggingInMemoryQueueSize` - maximální počet protokolů zapsaných do paměti (výchozí 200). Vezměte prosím na vědomí, že všechna data jsou do tabulky načtena najednou a vzhledem k přenosu `stack trace` mohou být velké. Nedoporučujeme nastavovat tuto proměnnou na extrémně vysokou hodnotu.

Aby správně fungoval, musí být `logger` nastavené také v souboru `logback.xml`. Ve výchozím nastavení je to tak nastaveno, ale pokud jste soubor změnili, musíte přidat `IN_MEMORY` appender a přidat jeho výzvu k `root` prvek.

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

xml

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

15.2. Implementační detaily

- `sk.iway.iwcm.system.logging.InMemoryLoggerAppender` - `appender` Pro `logback`, který zajišťuje, že protokoly jsou odesílány na adresu `InMemoryLoggingDB`
- `sk.iway.iwcm.system.logging.InMemoryLoggingDB` - třída zajišťuje zápis a načítání protokolů z a na `queue`, načítání protokolů v clusteru
- `sk.iway.iwcm.system.logging.InMemoryLoggingEvent` - model pro událost protokolu
- `sk.iway.iwcm.system.logging.InMemoryLoggerRestController` - řadič pro výpis protokolu do DataTable

16. Výkonnost serveru

Pro optimální výkon serveru je třeba splnit několik požadavků a nastavení. Každá aplikace (např. fotogalerie, anketa atd.) vložená do webové stránky způsobuje zpomalení. Aplikace obvykle provádějí další požadavky na databázi nebo potřebují číst data ze souborového systému.

Vyhledávače, které neustále procházejí a indexují webové stránky na vašem serveru, mohou mít také významný vliv na výkon. Jejich návštěvnost nemusí být viditelná např. v nástroji Google Analytics, ale je viditelná v nástroji [Statistiky](https://docs.webjetcms.sk/latest/cs/redactor/apps/stat/README) (<https://docs.webjetcms.sk/latest/cs/redactor/apps/stat/README>) poskytované systémem WebJET CMS.

16.1. Identifikace problémů

Nejprve je třeba zjistit, kde dochází ke zpomalení. Pokud dokážete na první pohled identifikovat webovou stránku, která se vám zdá pomalá, můžete použít parametr URL. `?_writePerfStat=true`. V opačném případě zapněte monitorování serveru, při kterém můžete identifikovat webové stránky, jejichž spuštění trvá nejdéle.

16.1.1. Parametr URL

Použití parametru URL `?_writePerfStat=true` je možné získat seznam aplikací vložených do webové stránky s časem jejich spuštění. Například stránka `/sk/` zobrazit jako `/sk/?_writePerfStat=true`.

Při tomto způsobu zobrazení webové stránky se výraz typu `PerfStat: 3 ms (+3) !INCLUDE(...)`. Na standardní webové stránce nemusí být snadno vyhledatelný, proto doporučujeme zobrazit zdrojový kód stránky - v nabídce Chrome Zobrazit-Vývojář-Zobrazit zdrojový kód. Poté použijte vyhledávací výraz prohlížeče `PerfStat:`.

Tento výraz je ve formátu `PerfStat: 3 ms (+3)` kde první číslo je celková doba provedení jednoho úkonu. `iwcm:write` a číslo v závorce je doba provádění této aplikace. Následuje cesta k aplikaci a její parametry. Zajímá vás tedy primární číslo v závorce.

Použití parametru URL `_disableCache=true` můžete vypnout ukládání aplikací do mezipaměti.

16.1.2. Monitorování serveru

Chcete-li získat komplexní zobrazení, můžete zapnout funkci [monitorování serveru](#) nastavením následujících konfiguračních proměnných:

- `serverMonitoringEnable` - umožňuje funkci monitorování a protokolování serveru
- `serverMonitoringEnablePerformance` - zapíná monitorování výkonu aplikací a webových stránek
- `serverMonitoringEnableJPA` - umožňuje funkci sledování dotazů SQL

Varování: monitorování výkonu aplikací a dotazů SQL zatěžuje server, nedoporučujeme mít tuto funkci trvale zapnutou.

Po nastavení konfiguračních proměnných je třeba provést následující úkony. **restartovat aplikační server** aktivovat sledování výkonu při inicializaci.

V části Sledování serveru - Aplikace/WEB stránky/Dotazy SQL pak můžete identifikovat části, jejichž spuštění trvá dlouho. Zaměřte se na nejčastěji spouštěné aplikace/dotazy SQL a optimalizujte je.

16.1.3. Celková doba generování webové stránky

K dispozici je aplikace `/components/_common/generation_time.jsp` který po vložení do zápatí šablony webové stránky vygeneruje do kódu HTML celkový čas generování webové stránky.

Lze nastavit následující parametry aplikace:

- `hide` - výchozí nastavení `true` - čas generování se zobrazí jako komentář v kódu HTML.
- `onlyForAdmin` - výchozí nastavení `false` - čas generování se zobrazí pouze v případě, že je přihlášen správce.

Do zápatí (nebo do vhodného volného pole) šablony webové stránky vložte následující kód:

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

html

V místě vložené aplikace se zobrazí informace o době provádění celé webové stránky v ms:

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

html

16.2. Měření výkonu databázového serveru a souborového systému

Pro porovnání výkonu prostředí - např. testovacího a produkčního prostředí - lze použít níže uvedené skripty. Jejich spuštění vyžaduje právo aktualizovat WebJET. Prostorů můžete měřit a porovnávat bez zátěže, ale také za provozu nebo při testech výkonu.

- `/admin/update/dbspeedtest.jsp` - měří výkon při čtení dat z databázového serveru.

Dobré hodnoty jsou například:

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

html

```
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
```

Vzhledem k rozdílnému počtu záznamů v databázi je nutné porovnat. `per item` Hodnoty.

- `/admin/update/fsspeedtest.jsp` - kontroluje rychlost čtení seznamu souborů ze souborového systému, měla by být kontrolována zejména v případě, že používáte síťový souborový systém.

Dobré hodnoty jsou například:

```
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. Optimalizace databázových dotazů

Chcete-li optimalizovat počet požadavků na databázi, můžete povolit ukládání do mezipaměti - `cache` .

16.3.1. Webové stránky

Každá webová stránka má na kartě Základní možnost **Povolení ukládání stránek do mezipaměti**. Zapnutím této možnosti se obsah webové stránky přenese z tabulky. `documents` je uložen v mezipaměti. Při zobrazení webové stránky není nutné volat databázi pro načtení obsahu webové stránky.

Tuto možnost doporučujeme povolit na nejnavštěvovanějších webových stránkách, jejichž seznam můžete získat v aplikaci. [Statistiky](https://docs.webjetcms.sk/latest/cs/redactor/apps/stat/README) (<https://docs.webjetcms.sk/latest/cs/redactor/apps/stat/README>).

16.3.2. Aplikace

Podobně jako u webových stránek můžete mezipaměť povolit také u aplikací. Některé aplikace mají tuto možnost k dispozici přímo v [nastavení aplikace](https://docs.webjetcms.sk/latest/cs/custom-apps/appstore/README) (<https://docs.webjetcms.sk/latest/cs/custom-apps/appstore/README>) vložené na webové stránce na kartě Zobrazit jako pole. **Doba vyrovnávací paměti.**

Pokud aplikace nemá toto nastavení k dispozici, můžete parametr nastavit v kódu HTML textu webové stránky přidáním parametru `, cacheMinutes=xxx` například na parametry vestavěné aplikace:

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

html

Varování: je důležité si uvědomit, že mezipaměť je globální pro celý aplikační server. Jako klíč se používá cesta k souboru aplikace, jednotlivé parametry uvedené v kódu HTML webové stránky a jazyk aktuálně zobrazené webové stránky. Parametry URL webové stránky nejsou brány v úvahu.

Mezipaměť tedy nelze použít, pokud se například zobrazuje stránkový seznam, kde se číslo stránky předává pomocí parametru URL. Existuje však výjimka pro aplikace, které obsahují seznam novinek v názvu souboru `/news/news` vyrovnávací paměť se použije pouze v případě, že v adrese URL není zadán žádný parametr. `page` nebo je hodnota tohoto parametru jiná než `1`. Tímto způsobem se vyrovnávací paměť používá i pro seznam novinek, ale ukládá se pouze první stránka výsledků. Další stránky se neukládají.

16.4. Optimalizace souborového systému

Webové stránky obvykle obsahují mnoho dalších souborů - obrázky, soubory stylů CSS, soubory JavaScriptu atd. - které je třeba načíst společně s webovou stránkou. Rychlost zobrazení proto závisí také na počtu a velikosti těchto souborů.

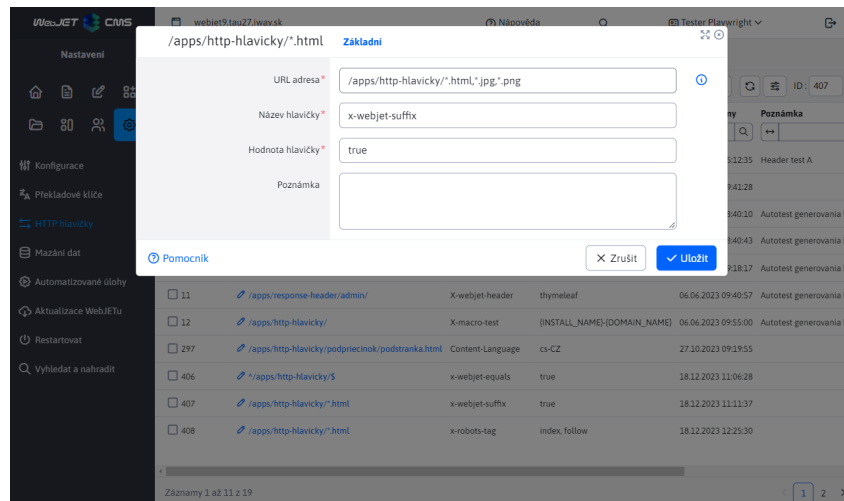
16.4.1. Nastavení vyrovnávací paměti

Je možné nastavit prohlížeč tak, aby používal mezipaměť pro soubory webových stránek - soubor se tak nebude načítat opakovaně při každém zobrazení webové stránky, ale pokud jej prohlížeč již má uložený v mezipaměti, použije jej. Tím se zrychlí zobrazení webové stránky a sníží se zatížení serveru. Příkladem může být obrázek loga, který je obvykle na každé stránce, ale je velmi nepravděpodobné, že by se měnil - nebo se měnil řádově jednou za několik měsíců.

Je možné nastavit následující konfigurační proměnné, které ovlivňují hlavičku HTTP. `Cache-Control` :

- `cacheStaticContentSeconds` - nastavit počet sekund, výchozí `300` .
- `cacheStaticContentSuffixes` - seznam rozšíření, pro která je hlavička HTTP `Cache-Control` ve výchozím nastavení vygenerována `.gif, .jpg, .png, .swf, .css, .js, .woff, .svg, .woff2` .

Pro přesnější nastavení můžete použít aplikaci [Hlavičky HTTP](https://docs.webjetcms.sk/latest/cs/admin/settings/response-header/README) (<https://docs.webjetcms.sk/latest/cs/admin/settings/response-header/README>) kde můžete nastavit různé hodnoty pro různé adresy URL.



16.5. Chování správce

Pokud je přihlášen správce, vyrovnávací paměť aplikace se nepoužívá (předpokládá se, že správce chce vždy vidět aktuální stav).

Toto chování lze změnit nastavením konfigurační proměnné `cacheStaticContentForAdmin` na hodnotu `true` . Tuto hodnotu je vhodné nastavit zejména u intranetových instalací, kde se uživatelé ověřují proti `SSO/ActiveDirectory` serveru a i při práci v intranetovém prostředí mají práva správce.

16.6. Vyhledávače

Vyhledávače a různí další roboti mohou server značně zatížit. Zejména s nástupem učení umělé inteligence dochází k významnému procházení internetu a naplňování databází pro učení umělé inteligence. Boti často zkoušejí různé parametry URL, aby získali další data.

16.6.1. Nastavení souboru robots.txt

Chování robotů lze ovlivnit nastavením v souboru `/robots.txt`. Pokud neexistuje, je vygenerován jako výchozí. Umístěte svou upravenou verzi do `/files/robots.txt`, z tohoto umístění jej WebJET zobrazí při volání `/robots.txt`.

Použití souboru `robots.txt` (<https://en.wikipedia.org/wiki/Robots.txt>) můžete ovlivnit chování robotů a vyhledávačů - omezit adresy URL, které mohou používat, nastavit rozestupy mezi požadavky atd.

16.7. Další nastavení

16.7.1. Reverzní server DNS

Statistiky, audit a další aplikace mohou z IP adresy načíst reverzní záznam DNS. Používají se volání API

`InetAddress.getByName(ip).getHostName()`. Server DNS však nemusí být na serverech/DMZ k dispozici a toto volání může trvat několik sekund, než dojde k chybě. Obecně takové volání zpomaluje provádění požadavku HTTP.

Nastavením konfigurační proměnné `disableReverseDns` na hodnotu `true` je možné zakázat načítání názvu DNS z IP adresy návštěvníka a urychlit provádění dotazů. V poli pro hodnotu `hostname` pak se zapíše hodnota IP adresy.

16.7.2. Vypnutí statistik

Zápis statistických dat je asynchronní, provádí se dávkově, takže zobrazení webové stránky nečeká na zápis statistických dat do databáze.

Pokud je provoz vysoký nebo hledáte problémy s výkonem, můžete dočasně zakázat zaznamenávání statistik provozu nastavením konfigurační proměnné `statMode` na hodnotu `none`. Standardní hodnota je `new`.

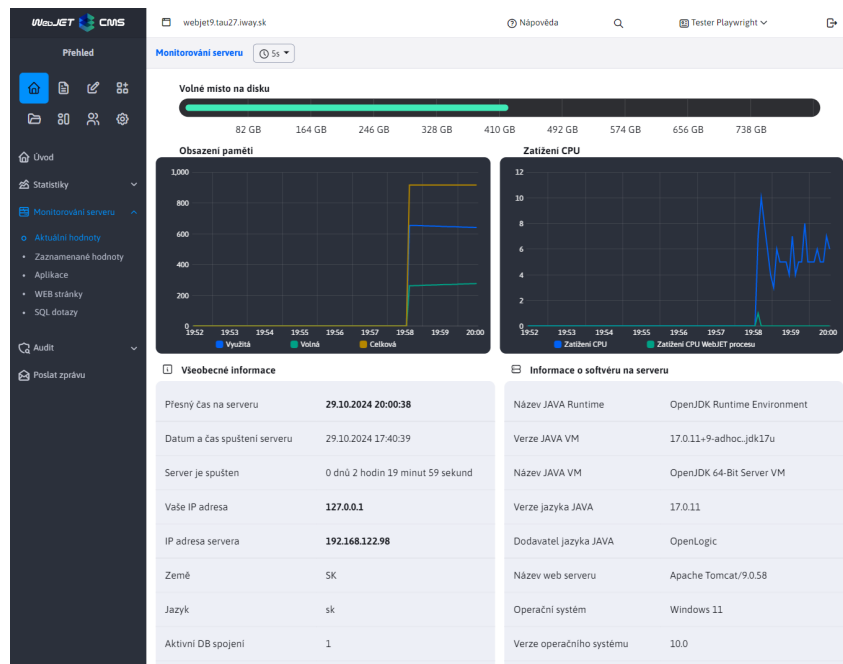
17. Monitorování serveru

17.1. Interní monitorování

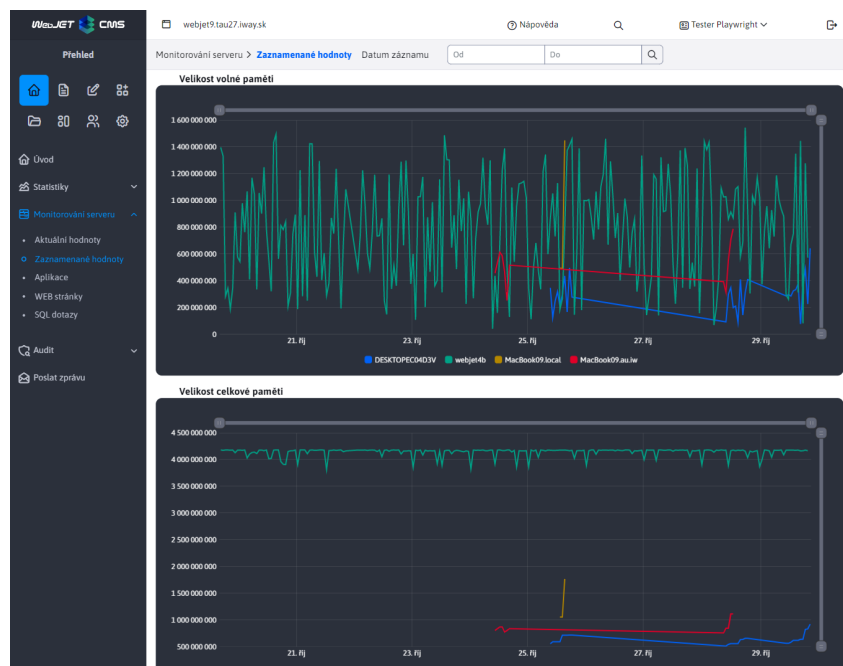
Analýzu výkonu a zatížení serveru, jednotlivých aplikací, databázových dotazů i samotných stránek lze sledovat přímo v aplikaci Server Monitoring (v administraci WebJET v sekci Přehled).

Modul nabízí následující možnosti:

- **Aktuální hodnoty** - aktuální zatížení serveru, paměť a počet databázových připojení.



- **Zaznamenané hodnoty** - výpis historických zaznamenaných hodnot využití paměti, `sessions`, mezipaměti a připojení k databázi. Pro ukládání historických hodnot je nutné nastavit konf. proměnnou `serverMonitoringEnable` na hodnotu `true`.



Po nastavení konfigurační proměnné `serverMonitoringEnablePerformance` na adrese `true` jsou také k dispozici:

- **Aplikace** - statistiky o provádění jednotlivých aplikací. Zobrazuje počet spuštění, průměrnou dobu spuštění, počet spuštění z paměti cache a nejpomalejší spuštění.
- **WEBové stránky** - statistiky zobrazení jednotlivých webových stránek. Zobrazuje počet zobrazení, průměrnou dobu zobrazení, nejpomalejší a nejrychlejší zobrazení.

Po nastavení konfigurační proměnné `serverMonitoringEnableJPA` na adrese `true` je také k dispozici:

- **Dotazy SQL** - Statistika rychlosti provádění dotazů SQL. Zobrazuje počet provedení, průměrnou dobu provedení, nejpomalejší a nejrychlejší provedení a samotný dotaz SQL.

! Varování: Aktivace monitorování ovlivňuje výkon serveru a zatížení paměti. Kromě možnosti zaznamenávat hodnoty má zapnutí monitorování vliv na výkon serveru. Všechna data s výjimkou sekce zaznamenaných hodnot jsou uchovávána pouze v paměti serveru, takže se po restartování serveru opět začnou zaznamenávat.

! Varování: modulární možnosti **Aplikace**, **WEBové stránky** a **Dotazy SQL** používají jedinečnou společnou logiku, která je podrobněji popsána v části [Sledování serveru podle vybraného uzlu](#)

17.2. Vzdálené monitorování běhu serveru

Pokud potřebujete sledovat stav WebJETu prostřednictvím [Nagios](http://www.nagios.org) (<http://www.nagios.org>) / [Zabbix](https://www.zabbix.com) (<https://www.zabbix.com>) nebo jinou službu, kterou WebJET poskytuje na adrese URL. `/components/server_monitoring/monitor.jsp` váš stav. Odpovědi HTTP **stav 200**, **pokud je vše v pořádku**, nebo **se stavem 500** (Chyba vnitřního serveru), pokud **nejsou splněny všechny kontroly**.

Tuto adresu URL lze volat také v jednosekundových intervalech a doporučujeme ji používat v rámci clusteru ke sledování dostupnosti jednotlivých uzlů.

Povolné IP adresy pro které `monitor.jsp` správně reaguje, jsou nastaveny v konfigurační proměnné `serverMonitoringEnableIPs`.

Komponenta monitoruje následující části:

- **Inicializace WebJET**, včetně jeho `preheating` (čekání na inicializaci objektů mezipaměti nebo úloh na pozadí). Doba předehřívání se nastavuje v konfigurační proměnné `monitoringPreheatTime` (výchozí hodnota 0). WebJET odpovídá textem `NOT INITIALISED` pokud není správně inicializován (např. při spuštění není vůbec žádné připojení k databázi nebo má neplatnou licenci). Text `T00 SHORT AFTER START` reaguje v době předehřívání (začlenění do clusteru by mělo počkat na dokončení načítání mezipaměti objektů/úloh na pozadí).
- Monitorování **dostupnost připojení k databázi** - SQL select se provádí z tabulky `documents` (konkrétně `SELECT title FROM documents WHERE doc_id=?`), zatímco v konfigurační proměnné `monitorTestDocId` je docid testované stránky. Pokud dotaz SQL selže, odpoví textem `DEFAULT DOC NOT FOUND`.
- **Dostupnost šablon** - pokud je seznam inicializovaných šablon menší než 3, odpoví textem `NOT ENOUGH TEMPLATES`.
- **Zaznamenávání statistických údajů** - ověří, zda v zásobníku pro zápis statistik není podezřele mnoho záznamů (počet záznamů je nastaven v konfigurační proměnné `statBufferSuspicionThreshold`, výchozí 1000). Pokud zásobník pro zápis statistik obsahuje větší množství dat k zápisu, znamená to buď problém s výkonem SQL Serveru, nebo problém s úlohami na pozadí. Pokud je počet záznamů překročen, reaguje textem `STAT BUFFER SUSPICION`.
- Pokud se vyskytne **jiná chyba** odpoví s textem `EXCEPTION: xxxx`.

WebJET je možné používat i ručně **přepnutí do servisního režimu** nastavením konfigurační proměnné `monitorMaintenanceMode` skutečně. Pak `monitor.jsp` odpoví textem `UNAVAILABLE`.

Pokud je vše v pořádku, odpoví textem `OK`. Pro sledování **stačí sledovat stav HTTP** odpovědi, text má pouze informativní charakter pro přesnější určení problému.

17.3. Konfigurační proměnné

- `serverMonitoringEnable` - pokud je nastavena na `true`, začne monitorovat server každých 30 sekund a zapíše tyto hodnoty do tabulky `monitoring`
- `appendQueryStringWhenMonitoringDocuments` - zachycení parametrů SQL během monitorování ?
- `monitorTestDocId` - ID stránky, jejíž připojení k databázi (načítání názvu) se v komponentě testuje. `/components/server_monitoring/monitor.jsp` které může dohledový SW testovat (výchozí hodnota: 1)
- `serverMonitoringEnablePerformance` - pokud je nastavena na `true`, spouštěče urychlují monitorování dotazů SQL, webových stránek a aplikací (výchozí: false).
- `serverMonitoringEnableJPA` - pokud je nastavena na `true`, spustí sledování rychlosti provádění dotazů SQL pro JPA, ale vede ke zvýšení zatížení paměti serveru (výchozí: false).


- `serverMonitoringEnableIPs` - Seznam IP adres, ze kterých je součást dostupná `monitor.jsp` pro sledování serveru (výchozí: 127.0.0.1,192.168.,10.,62.65.161.,85.248.107.,195.168.35.)
- `monitoringPreheatTime` - Počet sekund potřebných k zahřátí webu (načtení mezipaměti) po restartu, během kterých se web zahřeje. `monitor.jsp` komponenta vracející nedostupnost uzlu clusteru (výchozí: 0)
- `monitoringEnableCountUsersOnAllNodes` - Pokud veřejné uzly clusteru nemají možnost zapisovat do tabulky. `_conf_/webjet_conf` nastavit na `false`. Celkový počet `sessions` pak bude k dispozici pouze po sečtení jednotlivých záznamů v monitorování serveru.

18. Restartování

Klikněte na možnost **Restartování** v sekci Nastavení se zobrazí potvrzení o restartování WebJETu. Ve výchozím nastavení se restart provede na serveru, ale záleží na nastavení serveru, zda je restart z webové aplikace povolen. Pokud ne, restart se neprovede.

V konfiguraci `server.xml` aplikační server [Tomcat](https://tomcat.apache.org/tomcat-9.0-doc/config/context.html) (<https://tomcat.apache.org/tomcat-9.0-doc/config/context.html>) je nutné povolit restartování pomocí atributu `reloadable="true"` v prvcích `Context` :

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

**Varování:** Před restartem si ověřte dostupnost technické podpory hostingu, protože může být nutné restartovat i aplikační server. To však nelze provést přímo z prostředí WebJET.

Opakované restarty mohou také zaplnit paměť aplikačního serveru, což může vyžadovat restartování aplikačního serveru přímo na serveru.

19. Výměna dat uzlu clusteru

Webové stránky **Aplikace**, **WEBové stránky** a **Dotazy SQL** sdílejí stejnou logiku monitorování serveru podle aktuálně vybraného uzlu. Pro výběr uzlu použijte pole, které se zobrazuje v záhlaví stránky vedle jejího názvu.

SQL dotazy

DESKTOPEC04D3V (Aktuální uzel)

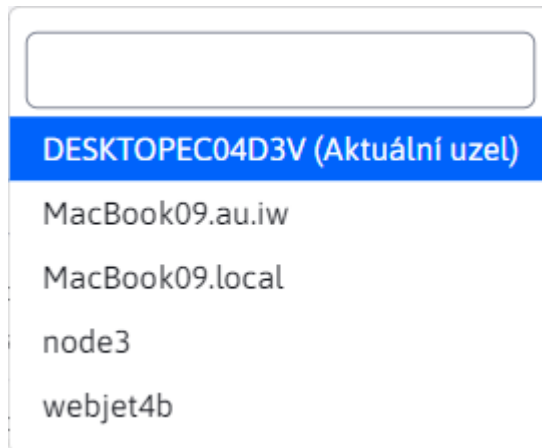
SQL	# vykonání	Čas vykonání (p			
	Oc	Dc	Q	Od	Do
SELECT insert_script_doc_id, doc_id, insert_script FROM insert_script_doc WHERE (insert_script = ?)			956		
SELECT insert_script_gr_id, domain_id, group_id, insert_script FROM insert_script_gr WHERE (insert_script = ?)			956		
SELECT templates_group_id, directory, inline_editing_mode, key_prefix, name FROM templates_group WHERE (templates_group_id = ?)			614		
SELECT group_id, editable_groups, editable_pages, group_title, writable_folders FROM user_perm_groups WHERE (group_id = ?)			86		
SELECT perm_id, permission, perm_group_id FROM user_perm_groups_perms WHERE (perm_group_id = ?)			77		
SELECT id, doc_id, banner_id FROM banner_doc WHERE (banner_id = ?)			56		

Záznamy 1 až 11 z 21

1

2

Po otevření kliknutím se zobrazí všechny dostupné možnosti. Výchozí hodnotou je vždy aktuální uzel (uzel clusteru, ke kterému jste právě přihlášení), který je označen textem (Aktuální uzel) .



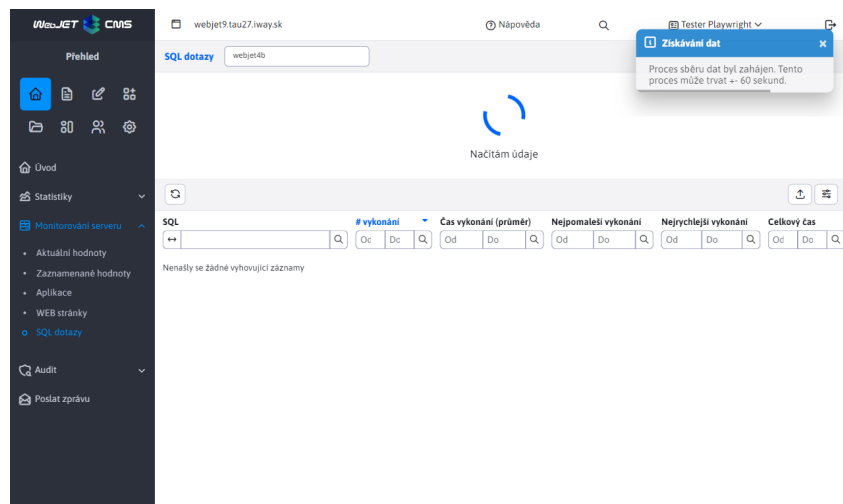
Pokud je vybraný uzel aktuální, zobrazí se lokálně uložená data. V tomto případě je k dispozici také tlačítko pro odstranění, které tato lokálně uložená data odstraní (tlačítko pro odstranění je k dispozici pouze pro aktuální uzel). V případě jiného než aktuálního uzlu se data načítají z databázové tabulky.

19.1. Obnovení dat - aktuální uzel

Pokud je vybrán aktuální uzel, stisknutím tlačítka pro obnovení dat se načtou pouze aktuálně uložená data (s databázovými tabulkami se zde nepracuje). Pokud byla data dříve smazána, může chvíli trvat, než se objeví nové záznamy.

19.2. Obnova dat - vzdálený uzel

U jiných uzlů než aktuálního je obnova dat obtížnější. Data ostatních uzlů jsou uložena v tabulce `cluster_monitoring` . Proces obnovy dat začíná odstraněním dat z tabulky, protože již nemusí být aktuální.



Jak vidíte na obrázku výše, data byla odstraněna a zobrazí se animace čekající na data. Zobrazí se také informační oznámení, které nás upozorňuje, že tento proces může trvat +- několik sekund. Tento interval se může lišit v závislosti na nastavené konfigurační proměnné `clusterRefreshTimeout` .

Proces získávání aktuálních dat spočívá ve vytvoření požadavku na aktuální data pro uzel vytvořením záznamu v databázové tabulce `cluster_refresher` . Samotný shluk v intervalech zadaných proměnnou `conf.clusterRefreshTimeout` aktualizuje údaje v tabulce `cluster_monitoring` pro určitý uzel, pokud je v tabulce požadavek na tento uzel. `cluster_refresher` . Proces načítání dat proto může trvat několik minut a může se lišit v závislosti na nastaveném intervalu obnovy clusteru (může nastat situace, kdy byl interval clusteru těsně před obnovou a skutečná data jsou načtena za 10 sekund, i když byl interval nastaven na 5 minut).

Ačkoli se nezobrazuje, stránka se každých 10 sekund zeptá, zda je tabulka `cluster_monitoring` nebyla přidána žádná nová data, která by bylo možné zobrazit. Pokud požadovaný uzel neobsahoval žádná data (ale tabulka již byla aktualizována), bude vytvořen nový požadavek na data v clusteru a opět budeme každých 10 sekund kontrolovat, zda data již nebyla aktualizována. Celý proces se bude opakovat, dokud nebude aktualizovaná tabulka `cluster_monitoring` nebude obsahovat alespoň jeden záznam, který se má zobrazit. V tomto okamžiku se animace skryje a zobrazí se aktuálně načtená data druhého uzlu.

20. Vymazání dat

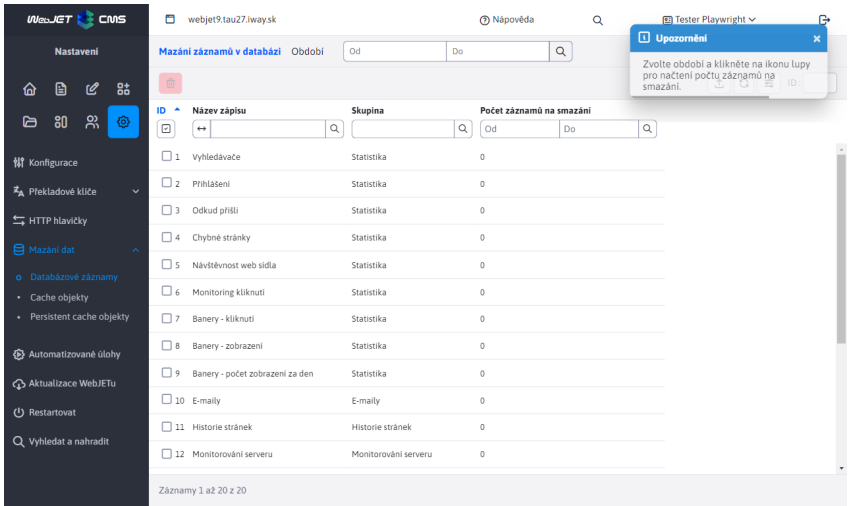
Aplikace **Vymazání dat** umožňuje odstranit nepotřebná data z databáze, což může zvýšit výkon serveru a uvolnit místo na disku. Tento nástroj naleznete v **Nastavení** pod nadpisem **Vymazání dat**.

20.1. Záznamy v databázi

Odstranění dat z vybraných databázových tabulek, odstranění je možné z následujících skupin:

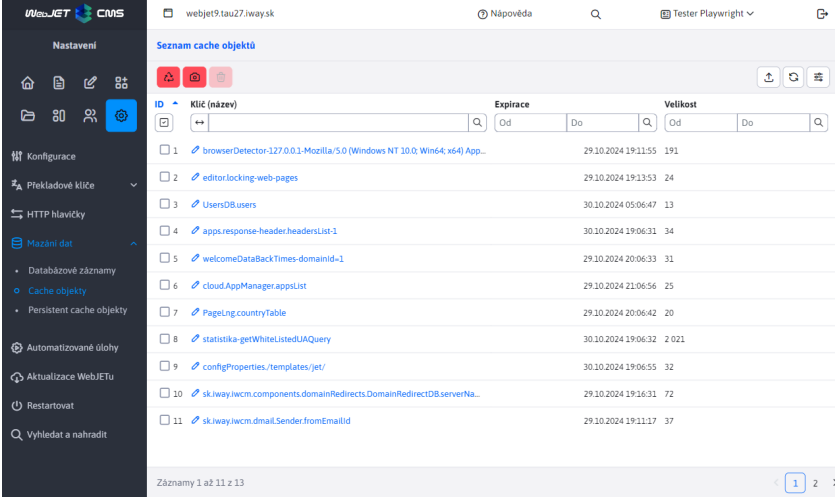
- **Statistiky:** Odstraní statistické údaje. Odstranění starších dat může výrazně zlepšit výkon serveru, ale ztratíte informace o návštěvnosti webu za zvolené období.
- **E-mailly:** Umožňuje odstranit odeslané e-maily z aplikace Hromadná pošta a e-maily odeslané s časovým zpožděním (nebo e-maily odeslané v rámci clusteru s více uzly).
- **Historie webu:** Odstraní zaznamenané historické verze webových stránek, které se ukládají při každém zveřejnění webové stránky. Zobrazují se na kartě Historie při úpravách webové stránky. Odstranění nemá vliv na aktuálně zobrazené stránky, odstraňují se historické verze.
- **Monitorování serveru:** Odstraní zaznamenaná data monitorování serveru, jako jsou metriky výkonu a protokoly.
- **Audit:** Odstraní auditní záznamy, které sledují aktivitu uživatelů a systémové události, odstranit lze pouze vybrané typy záznamů.

S každým odstraněním se také provede optimalizace databázové tabulky, aby se fyzicky uvolnilo místo na disku a optimalizovalo pořadí záznamů v databázové tabulce.



20.2. Objekty mezipaměti

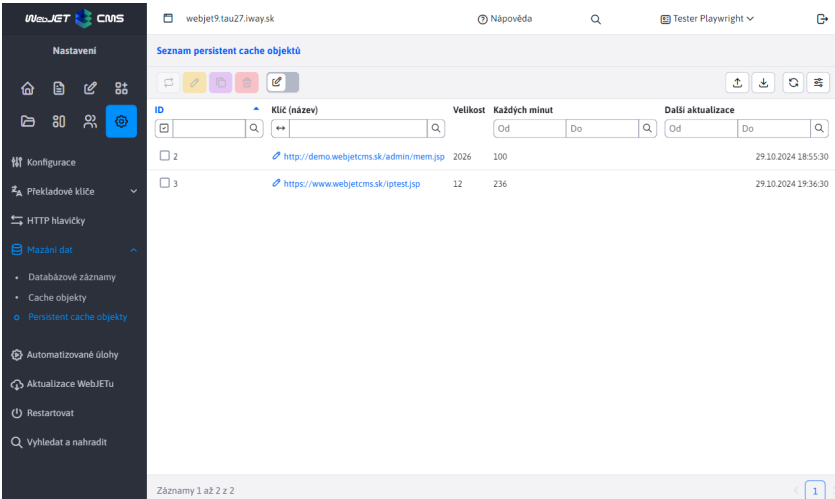
Zobrazí seznam objektů uložených v mezipaměti aplikace a umožní je jednotlivě odstranit, což může snížit spotřebu paměti nebo vyvolat obnovení dat v mezipaměti serveru. Klepnutím na název můžete zobrazit obsah záznamu pro vybrané typy dat. Objekt se používá pro práci [Cache](https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/Cache.java) (<https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/Cache.java>)



ID	Key (Name)	Expiry	Size
1	browserDetector-327.0.0.1-Mozilla/5.0 (Windows NT 10.0; Win64; x64) App...	29.10.2024 19:11:55	191
2	editorlocking-web-pages	29.10.2024 19:13:53	24
3	UsersDB.users	30.10.2024 05:06:47	13
4	apps.response-header.headersList-1	30.10.2024 19:06:31	34
5	welcomeDataBackTimes-domainid-1	29.10.2024 20:06:33	31
6	cloudAppManager.appsList	29.10.2024 21:06:56	25
7	PageLng.countryTable	29.10.2024 20:06:42	20
8	statistika-getWhiteListedUAQuery	30.10.2024 19:06:32	2 021
9	configProperties./templates/jet/	30.10.2024 19:06:55	32
10	sk.iway.iwcm.components.domainRedirects.DomainRedirectDB.serverNa...	29.10.2024 19:16:31	72
11	sk.iway.iwcm.dmail.Sender.fromEmailid	29.10.2024 19:11:17	37

20.3. Trvalé objekty mezipaměti

Správa a mazání objektů uložených v trvalé mezipaměti, která uchovává data i po restartu serveru (data jsou uložena v databázi). Objekt se používá pro práci [PersistentCacheDB](https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/system/cache/PersistentCacheDB.java) (<https://github.com/webjetcms/webjetcms/tree/main/src/webjet8/java/sk/iway/iwcm/system/cache/PersistentCacheDB.java>). Do této mezipaměti lze ukládat pouze textová data, typicky metodou `downloadUrl(String url, int cacheInMinutes)` který na pozadí stahuje data ze zadané adresy URL a v nastaveném čase je aktualizuje. Aplikace použije tuto metodu a okamžitě načte data z mezipaměti.



ID	Key (Name)	Size	Každých minut	Další aktualizace
2	http://demo.webjetcms.sk/admin/mem.jsp	2026	100	29.10.2024 18:55:30
3	https://www.webjetcms.sk/iptest.jsp	12	236	29.10.2024 19:36:30

21. Zálohování systému

Aplikace slouží k vytvoření archivu ZIP jednotlivých složek souborového systému WebJET. Můžete si zvolit, které složky mají být do archivu ZIP zahrnuty a ve které složce má být výsledný archiv ZIP vytvořen. Nevytváří se záloha databáze, tu je třeba vytvořit pomocí nástrojů pro zálohování databáze.

Varování: Množství dat ve vybraných složkách může být velké a soubor ZIP nemusí být vygenerován správně (omezení je na soubor o velikosti 2 GB). V případě potřeby můžete vytvářet zálohy po částech (jednotlivých složkách).

Vytvořit ZIP archiv

Ze seznamu vyberte adresáře, které chcete archivovat.

Cesta k archivu:

Archivovat adresáře:

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

[Nápověda](#)[Zrušit](#)[OK](#)

Tento proces může trvat několik desítek minut v závislosti na množství dat ve vybraných složkách. Počkejte na dokončení celého procesu. Během této doby byste měli v okně vidět informace o počtu již vygenerovaných stránek a celkovém počtu stránek.

Výsledkem je archiv zip vytvořený v zadané složce.