

# Serilog

The screenshot shows the 'Serilog' configuration page in the 'Configuration Manager'. At the top, there is a blue header with 'Configuration Manager' and a link to the 'Configuration Manual'. Below the header, there is a navigation bar with tabs: 'Urls', 'Licence', 'Database', 'Active Directory/OpenId', 'App Logs', 'Background Jobs', 'XFrame Settings', and 'Encryption Key'. The 'App Logs' tab is selected. The main content area is titled 'Serilog' with a link to the 'Serilog Section'. There is a checkbox for 'Insights' which is checked. Below this, there are four input fields: 'LogPath' (text input with 'logs'), 'Log Type' (dropdown menu with 'Information'), 'Service Log Write To' (dropdown menu with 'Both'), and 'RollingInterval' (dropdown menu with 'Day'). At the bottom, there are four checkboxes for auditing: 'Audit for login/logout', 'Audit for Enterprise Architect Database modifications', 'Audit for HTTP status codes', and 'Audit for Infoport permissions'. All these checkboxes are checked. There is also a checkbox for 'Audit for Access Keys' which is checked. At the bottom left, there is a green button labeled 'CHECK'.

Další sekce nám umožní nastavit logování Infoportu.

První položka je zaškrťovací políčko, které říká, jestli mají být logovány aktivity uživatelů. (Přehled navštívených URL).

Insights

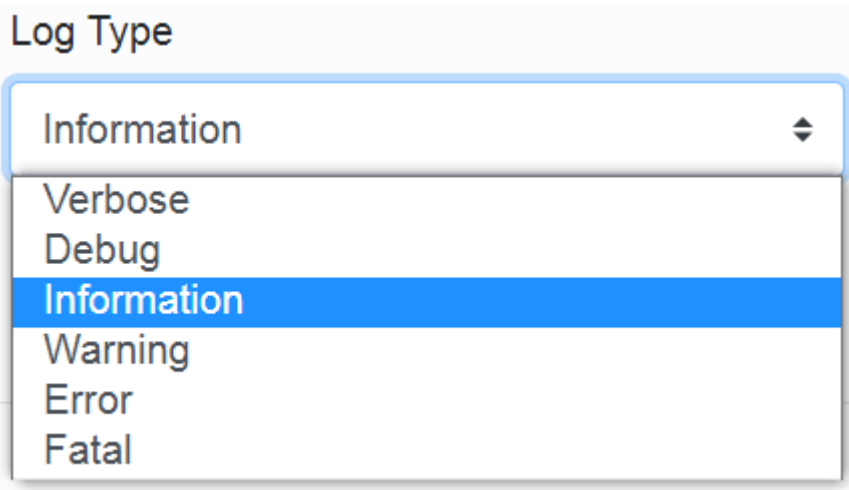
V druhé položce volíme relativní cestu na ukládání logů.

LogPath

logs

V Log Type položce vybíráme úroveň logování.

(Každá úroveň je popsána v tabulce, doporučujeme logování Information).

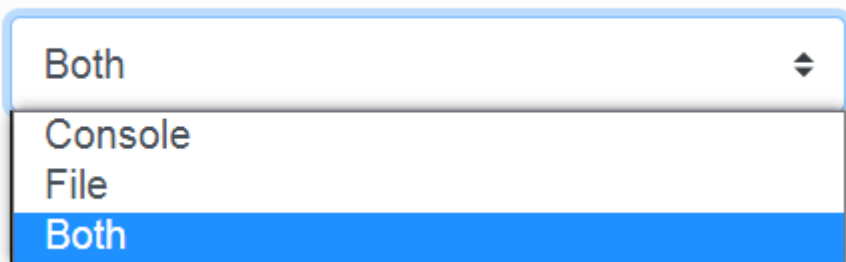


Tabulka pro úrovně logování.

| Úroveň (od nejpodrobnějšího k nejméně podrobnému) | Popis  |
|---|--|
| Verbose   | Pro informace, které slouží pro ladění. Tyto zprávy mohou obsahovat citlivá data aplikace, a proto by neměly být povoleny v produkčním prostředí. Ve výchozím nastavení zakázáno.  |
| Debug   | Informace, které mohou být užitečné při vývoji a ladění.   |
| Information                                       | Pro sledování celkového toku aplikace. Tyto protokoly mají obvykle určitou dlouhodobou hodnotu. Příklad: Požadavek přijatý pro path/api/todo   |
| Warning   | Pro abnormální nebo neočekávané události v toku aplikace. Může jít o chyby nebo jiné stavy, které nezpůsobí zastavení aplikace, ale je třeba je prozkoumat. Obsluhované výjimky jsou běžným místem pro použití úrovně protokolu Varování. Příklad: Příklad: FileNotFoundException pro soubor quotes.txt. |
| Error   | Pro chyby a výjimky, které nelze zpracovat. Tyto zprávy označují selhání v aktuální aktivitě nebo operaci (například aktuální http požadavek), nikoli selhání celé aplikace. Příklad zprávy protokolu: Nelze vložit záznam z důvodu porušení duplicitního klíče.   |
| Fatal   | V případě poruch, které vyžadují okamžitou pozornost. Příklad: scénáře ztráty dat, nedostatek místa na disku.  |

V položce Service Log Write To vybíráme, kam chceme, aby se logy zapisovaly. Máme tři možnosti: Konzole, Soubor nebo Obojí.

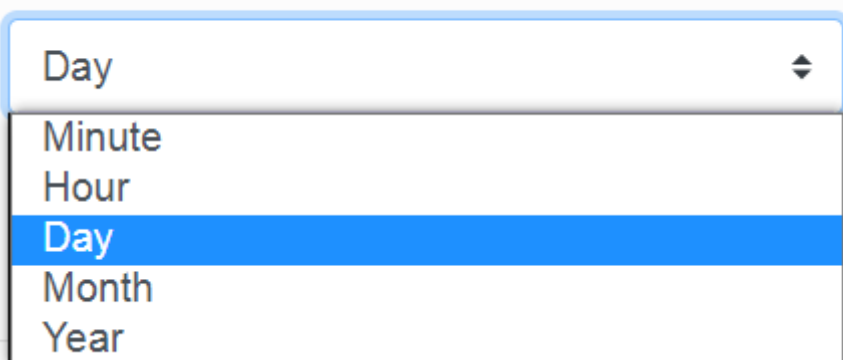
## Service Log Write To



A dropdown menu with a light blue border. The current selection is 'Both'. The menu is open, showing three options: 'Console', 'File', and 'Both'. The 'Both' option is highlighted with a blue background.

V položce RollingInterval volíme, jak často se má logovací soubor uzavírat.

## RollingInterval



A dropdown menu with a light blue border. The current selection is 'Day'. The menu is open, showing five options: 'Minute', 'Hour', 'Day', 'Month', and 'Year'. The 'Day' option is highlighted with a blue background.

Zde můžeme vidět zvolený den. Znamená to, že se nám každý den vytvoří nový soubor s logy pro portál. Logy z minulých dnů zůstávají na disku.

Následuje několik zaškrťovacích boxů:



A row of five checkboxes, all of which are checked. Below the checkboxes is a green button with a white checkmark and the text 'CHECK'.

- Audit for login/logout
- Audit for Enterprise Architect Database modifications
- Audit for HTTP status codes
- Audit for Infoport permissions
- Audit for Access Keys

## Audit for login/logout

Logují se události `"/Account/Login"` a `"/Account/Logout"` a to jak úspěšné (`StatusCode == 302`), tak i ty neúspěšné.

## Audit for Enterprise Architect Database modifications

Logují se změny, které uživatelé provádějí na datech repozitory. Přidávání, editace a mazání Packages, Element, Diagram, Attribute, Operation apod.

## Audit for HTTP status codes

Logují se nepodařené/nepovolené přístupy a to konkrétně "403 Forbidden for user ...", "404 NotFound for user ...", "401 Unauthorized for user ...". K těmto událostem dochází především při ruční úpravě (podvržení) url, kdy je vyměněno id nebo guid artefaktu ke kterému nemá uživatel přístup.

## Audit for Infoport permissions

Do logu se zapisují schválené i zamítnuté přístupy. Ty jsou počítány vždy pro požadovaný Package a to zvlášť pro osobní a zvlášť pro skupinová práva.

Pozor: těchto záznamů může být v logu velké množství.

Dále se také logují se změny uživatelských a skupinových oprávnění prováděné administrátory. Z těchto záznamů je dohledatelné, kdo kdy komu jaké právo přidělil či odebral.

## Audit for Access Keys

Vytvoření či smazání klíče pro přístup je logováno tak, aby se dalo zjistit, kdo kdy vytvořil klíč, který se následně používá pro přímý přístup (kdy není potřeba explicitní logování uživatele)



Po vyplnění stačí stisknout tlačítko

a manager Vám zhlásí, jestli je vše

v pořádku.

---

Revision #10

Created 15 March 2022 13:50:43

Updated 9 June 2025 13:43:22 by Karolína Kavanová