Tényleg jól ismeri a Confluence jogosultsági rendszerét? - Hogyan előzzük meg az információszivárgást

Ultimate Permission Manager has been acquired

Atlassian has acquired the Ultimate Permissions Manager app. For more details, please see the Atlassian blog post and META-INF blog post

Effective May 3, 2019, this app has been removed from the Marketplace and is no longer available for purchase or maintenance renewal. In accordance with Atlassian's End of Life policy, the Ultimate Permissions Manager app will have support for two years, with an end of life date of May 3, 2021. While the app is supported, please raise issues with Atlassian directly via support.atlassian.com.

A "*Tényleg* jól ismeri a Confluence jogosultsági rendszerét?" egy cikksorozat, mely a Confluence jogosultsági rendszerének kevésbé ismert, nem triviális, vagy akár meghökkentő aspektusaira fókuszál. Olvasson tovább, hogy megismerje mindazt, amit felfedeztünk a részletek felkutatásához bejárt izgalmas utazásunk során.

Némi háttér információ

Jogosan merül fel a kérdés, hogy mi az olyan érdekes a Confluence jogosultsági rendszerében, szépen ledokumentált, néhány pipa a felhasználókhoz, a csoportokhoz, és már készen is vagyunk. Ennek ellenére mi azt tapasztaltuk, hogy ez az állítás messze van a valóságtól.

A Confluence jogosultsági rendszerének nemcsak több szintje van (globális, munkaterület, oldal), de ezeknek még egymásra hatása is jelentős, ugyanis előfordulhat, hogy egy jogosultság beállítása vagy hiánya hatással van egy másik jogosultságra, melyek eredményeképpen létrejövő valós (effektív) jogosultságok felderítése gyakran nehézkessé válik.

Más szóval, a valós (effektív) jogosultságok néha a felhasználóknak kiosztott különálló jogosultságok implicit kombinációiként jönnek létre, de előfordul, hogy effektíven olyan jogosultság birtokába jut egy-egy felhasználó, mely közvetlenül nem is feltétlenül lett beállítáva.

A (valós) jogosultságok és oldal korlátozások komplexitása, melyek a tucatnyi, vagy akár több száz munkaterületen, oldalon, átívelve olyan véletlen hozzáféréseket okozhatnak felhasználók, vagy csoportok számára, melyek információ szivárgás kockázatát rejtik magukban. Ez csak egy példa arra, hogy miért kiemelten fontos a Confluence jogosultsági rendszer alapos ismerete egy közepes vagy nagy installáció üzemeltetése, bevezetése során.

Ebben cikksorozatban feltárunk néhány rejtett titkot a Confluence jogosultsági rendszeréből, és megmutatjuk azt is hogyan lehet mégis kézben tartani a jogok kiosztását. Kezdjünk is hozzá!

Információszivárgás a szervezetben

Egy Confluence rendben tartásához három dolog kell: megtartani a titkos információkat, megtartani a titkos információkat, és végül megtartani a titkos információkat... de néha mégis kiszivárog valami.

A Wikipedia szerint: Akkor beszélünk információszivárgásról, ha egy rendszerből jogosulatlan személyek mégis hozzáférhetnek bizonyos zártnak szánt információkhoz.

Vajon ez a szervezetek egy általános problémája? Úgy véljük igen. Nézzünk néhány példát:

- rákeresve a Google-ban az *information leakage policy* kifejezésre rengeteg találatot kapunk: ~ 7.760.000 oldal
    - csak mókás összehasonlítás kedvéért az Atlassian szóra keresve ~ 9.330.000 oldal szerepel a találatok között
- számtalan cikket találunk az interneten nagy adatvesztésekről és a történelem ismert információszivárgással kapcsolatos eseteiről
    - ahogy ezt a szép infografikát böngészve láthatjuk még egészen nagy cégeknek (mint pl. British Airways, Mozilla, NASDAQ, AT&T...) is szembe kellett nézniük ezzel a problémával
- 51%-a az alkalmazottaknak azt gondolja, hogy a céges információvagyon védelme nem az ő feladatuk, hanem az IT részlegé tudhatjuk meg a Symantec felméréséből
- Mik az okai az információszivárgásnak, adatvesztésnek? 42%-ban olyan hibák vagy véletlen események, melyeket az alkalmazottak követtek el - látható a prot-on.com vizualizációjában.

Ügyfeleink gyakran kérnek tőlünk egyfajta állapotfelmérés jellegű szolgáltatást Atlassian szoftvereikkel kapcsolatban. Ezen együttműködések során találtunk néhány, bár egyszerűnek tűnő, de könnyen információszivárgáshoz vezető esetet. Ez a cikk négy olyan hasznos tippet foglal össze, amelyek segítségével a Confluence és munkaterület adminisztrátorok elkerülhetik az ebből adódó kellemetlen helyzeteket.

Egy új felhasználónak adódhatnak jogosultságai az alapértelmezett csoportok miatt

"A confluence-users az az alapértelmezett csoport, melybe minden újonnan létrehozott felhasználó bekerül. Minden olyan jogot létrehozáskor automatikusan megkapnak az új felhasználók, amelyek ehhez a csoporthoz hozzá vannak rendelve" - olvashatjuk a Confluence dokumentációjában a csoportokról szóló részben.

E miatt legyünk nagyon óvatosak, amikor pl. egy olyan együttműködő partner számára hozunk létre egy felhasználót, aki nem tagja szervezetünknek (pl. külső cég alkalmazottja). Vélhetően neki nem kellene rendelkeznie a confluence-users csoport tagsággal, ugyanis ez eredményezhet "nem várt" hozzáféréseket belső kollegák számára szánt tartalmakhoz.

> **Ne feledjük**
>
> Minden felhasználónak, aki be szeretne lépni a Confluence rendszerbe rendelkeznie kell a Can Use/Használhatja jogosultsággal. Tehát ha egy felhasználó egyetlen csoportnak sem tagja, akkor önálló felhasználóként kell ezt a jogosultságot megadni számára. További részletek ezzel a jogosultsággal kapcsolatban itt található.

Legyünk óvatosan az alapértelmezett munkaterület jogosultságokkal

A Confluence nagyon egyszerűen támogatja, hogy egy újonnan létrehozott munkaterülethez alapértelmezett jogosultságokat rendeljük, mely remekül fel tudja gyorsítani az adminisztrátorok munkáját. Ez a beállítás a Confluence adminisztráció, Munkaterület jogosultságok, Alapértelmezett munkaterület jogosultságok részben érhető el (a dokumentáció itt található).

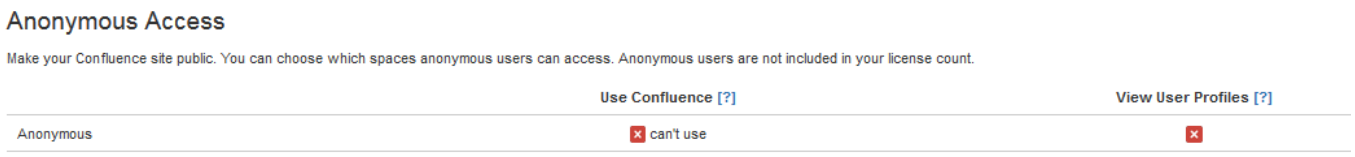
Alapértelmezés szerint a confluence-users csoportnak az alábbi jogosultságok vannak beállítva, melyek kiegészíthetőek, testre szabhatóak tetszőleges egyéb csoport jogosultságával:

A legtöbb esetben nem csak a Confluence adminisztrátorok, hanem projektvezetők, üzletág vezetők is jogosultak munkaterületek létrehozására a Confluence rendszeren belül. Ezzel csökkenthető az IT terheltsége, és felgyorsulhatnak az üzleti igények teljesítését célzó folyamatok, így aztán nagyon szeretjük ezt a funkciót. Nem szabad viszont elfeledni, alaposan átgondolni egy újonnan létrehozott munkaterület láthatóságának kérdéseit. Amennyiben egy nagyon érzékeny információknak szánt munkaterületet tervezünk létrehozni - és egyébként a legtöbb esetben amúgy ideális, megengedő alapértelmezett munkaterület jogosultsági beállításokat használjuk - akkor a legbiztosabb megoldás, ha a létrehozást követően kitörlünk minden létrejött jogosultságot, és egyesével kizárólag a legszükségesebb csoportokat, személyeket vesszük fel.

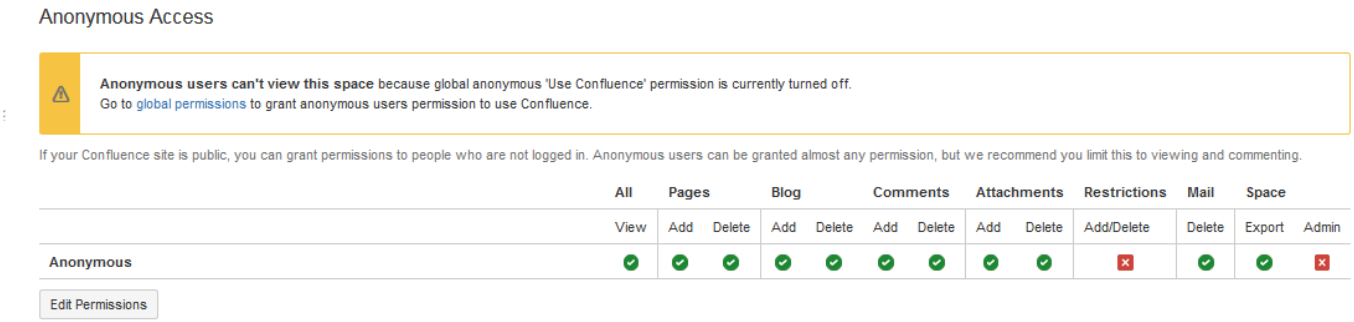
Amennyiben a szervezetben jellemzőek a különösen szenzitív adatok, akkor azt javasoljuk, hogy töröljön ki mindent, még a *confluence-users* csoportot is az alapértelmezett munkaterület jogosultság beállítások közül. Ezzel elkerülhető a létrehozáskor elfelejtett alapértelmezett jogokból adódó információszivárgás.

A globális beállításokban letiltható a bejelentkezés nélküli hozzáférés

A Confluence kiválóan alkalmas publikus tudásbázisok létrehozására is, ezért van egy olyan beállítási lehetőség, melynek segítségével egy adott tartalmat bárki elolvashat anélkül, hogy be kellene jelentkeznie a rendszerbe. Amennyiben viszont pl. a céges szabályzatok egyáltalán nem tesznek lehetővé belépés nélküli hozzáférést a tartalmakhoz, akkor a globális beállítások között érdemes kikapcsolni az Anonymous Can Use/Használhatja jogát, ahogy az alábbi ábrán láthatjuk:



Ez a beállítás megvédi a Confluence-ben a véletlen, bejelentkezés nélküli hozzáférésektől, ugyanis ha nincs az Anonymousnak Can Use/Használhatja globális joga, akkor garantáltan nem érhető el semmilyen tartalom az Anonymous (be nem lépett felhasználók) számára, akkor se, ha a Confluence vagy munkaterület adminisztrátor erre jogot adott (akár véletlenül akár szándékosan) bármely munkaterületen.



Mindig ellenőrizzük egy csoport jogosultságát mielőtt egy új felhasználót adunk hozzá

A csoportok - mint mindenhol - jelentősen felgyorsíthatják, és átláthatóbbá tehetik a jogosultsági beállítások menedzsmentjét. Az érem másik oldala viszont, hogy mindig érdemes alaposan ellenőrizni egy csoport jogosultságát új felhasználó hozzáadása előtt, ugyanis ezzel elkerülhetjük a véletlen adathozzáféréseket. A csoport jogosultságok ellenőrzése alapértelmezetten nem egyszerű egy Confluence rendszerben, mert sajnos egyesével végig kell menni az összes munkaterület jogosultsági beállítások szekcióján, de van egy kiegészítő az Atlassian Marketplace-n melynek segítségével ez sokkal egyszerűbb.

Tanulság

A Confluence-t információ megosztására és kollaboráció támogatására tervezték

- ne feledjük, hogy az új felhasználók kaphatnak létrehozáskor automatikusan jogosultságokat az alapértelmezett csoportok miatt
- az érzékeny adatokat tartalmazó oldalak, munkaterületek jogosultság beállításainál legyünk nagyon óvatosak, legtöbbször az alapértelmezett beállítások nem alkalmasak
- amennyiben a céges szabályok nem engedik a bejelentkezés nélküli (Anonymous) hozzáférést, akkor a globális beállításokban tiltsuk le azt
- mindig ellenőrizzük le kétszer egy csoport jogosultságait, mielőtt új felhasználót adunk hozzá, nehogy véletlen adathozzáférés keletkezzen

A META-INF Kft. az Ultimate Permission Manager for Confluence gyártója.

Ultimate Permission Manager has been acquired

Atlassian has acquired the Ultimate Permissions Manager app. For more details, please see the Atlassian blog post and META-INF blog post

Effective May 3, 2019, this app has been removed from the Marketplace and is no longer available for purchase or maintenance renewal. In accordance with Atlassian's End of Life policy, the Ultimate Permissions Manager app will have support for two years, with an end of life date of May 3, 2021. While the app is supported, please raise issues with Atlassian directly via support.atlassian.com.