

Základní vlastnosti přístupových oprávnění

Přístupová práva obecně

Přístupová práva v systému **Atollon Server Platform** (dále jen ASP) jsou spravována na serverové úrovni prostřednictvím modulu **mod.access**. Na klientské straně modul access zpřístupňuje administrační rozhraní pro definici přístupových práv systému. Samotná kontrola přístupových oprávnění probíhá z bezpečnostních důvodů pouze na serverové straně.

Přístupová práva jsou spravována ve stromové struktuře **Atollon Directory**. Stromová struktura obsahuje množství administračních složek, obsahujících rozličné definice či číselníky a složky obsahující data společnosti (např. kontakty, zprávy, dokumenty, apod.).

Viz schematicky [Atollon Tree Model.pdf](#)

Veškeré položky systému (jak koncové objekty (leaf object) - data tak složky (node)) mají svou vlastní definici přístupů (**ACL = Access Control List**), tedy seznam uživatelů, skupin nebo uživatelů přiřazených do role na projektu (klientovi, apod.), kteří mají svá přístupová oprávnění na danou položku. Systém při každé žádosti o akci na položce, u které je definována ACL, kontroluje přístupová oprávnění uživatele, pod jehož přihlášením je žádost podávána. (Např. pokud chce uživatel položku v seznamu, musí mít na ní LIST práva. Pokud chce položku smazat, musí na ní mít DELETE práva, apod.)

Uživatel systému

Uživatel je definován svým uživatelským jménem a heslem.

Uživatel v systému získává přístupová práva k jednotlivým položkám buď přímým přiřazením uživatele k dané položce, případně děděním uživatelských práv, přiřazením uživatele do role na projektu nebo složky klienta nebo přiřazením uživatele do skupiny, která má daná přístupová oprávnění. Specifickou vlastností je přidělení práv "v zastoupení". Lze poskytnout plnou moc uživateli na jiného uživatele a tak předávat práva definovaná individuálně jednotlivým uživatelům, např. v době nepřítomnosti, apod.

[detail-uzivatele-nastaveni-prav.png](#)

Doporučení

Výchozí práva v systému na jednotlivé objekty (typy složek, projektů, funkce - fakturace, formuláře, apod.) by se měla definovat ideálně vůči uživatelským skupinám (např. "Fakturace - schvalovatelé" nebo "Přehled klientů") - tak, aby se zachovala flexibilita při případných změnách v uživatelských oprávněních, jako jsou příchod nového zaměstnance, změna v oprávněních stávajícího uživatele, apod.

Skupiny je vhodné vytvářet pro každé právo, které vyžaduje speciální pozornost (např. "Obchodní případy - čtení" nebo "Obchodní případy - plná práva", apod.)

Více o nastavení uživatelů najdete v dokumentaci [Správa uživatelů](#).

Uživatelské skupiny

Uživatelská skupina je seznam uživatelů systému, kterým jsou přidělena stejná práva. Skupině je možné přiřadit libovolná práva pro kteroukoli položku systému, přičemž uživatelé přiřazení do dané skupiny tato práva automaticky získávají.

Uživatelské role

Ve speciálním nastavení je možné např. k složkám klientů a projektům přiřazovat uživatele do rolí. Díky přiřazení uživatele do definované role pak uživatel získává práva dané role. Práva role mohou být definovaná obecně pro veškeré projekty nebo složky klientů, přičemž uživatel získává práva pouze na konkrétních subjektech a projektech, ke kterým byl (do dané role) přiřazen.

Na kartě uživatele se určuje, do kterých rolí může být daný uživatel zařazen. Pokud uživatel nemá danou roli uvedenou ve svém nastavení, nemůže být do role obsazen.

Upozornění

Práva na role u složek klientů nebo projektů musí být definována v šabloně složky nebo projektu **před vytvořením** konkrétní složky nebo role. Pokud chcete definovat práva dodatečně, je nutné do **existujících projektů** a složek práva rolí zadat ručně nebo pomocí hromadných změn v reportingu.

Úrovně uživatelských oprávnění

New / Nový

Umožňuje uživateli založit novou položku (právo je aplikovatelné pouze pro složky nebo objekty, pod kterými lze něco nového založit)

List / Seznam	Umožňuje uživateli zobrazit název a některé základní atributy položky, bez zobrazení obsahu položky.
View / Zobrazit	Umožňuje uživateli zobrazení obsahu položky. Toto právo je většinou nutné kombinovat s právem list.
Edit / Upravit	Umožňuje uživateli měnit obsah dané položky (pokud je položka upravitelná). Toto právo však může být v různých částech systému omezeno v případě nutnosti schvalování, apod.
Delete / Smazat	Umožňuje uživateli smazat danou položku (pokud mazání položky umožňuje systém).
Authorize / Schválit	Umožňuje uživateli schvalovat danou položku (aplikováno pouze u některých položek systému).
Admin / Správa	Specifické právo, které může být definováno pouze uživatelem root . Pokud je toto právo v systému nastaveno, práva pro daného uživatele nebo skupinu nemohou být jakýmkoli uživatelem systému měněna. Toto právo se nastavuje zejména z důvodu zamezení náhodného odejmutí práv správcům systému (uživatelům, kteří jsou ve skupině Administrátoři).
Rights / Práva	Umožňuje uživateli měnit práva dané položky.
Finalize / Ukončit	Specifické právo, jež označuje zákaz dědění tohoto konkrétního nastavení v ACL. Využívá se např. při potřebě listovat složky / projekty. S tím, že je následně zakázáno dědění práv do zpráv na projektu, dokumentů, apod.

Další vlastnosti

Dědění práv

Z důvodu snadnější správy přístupových práv systém umožňuje dědění práv ve stromové struktuře. Výchozí dědění práv je nastaveno dle stromové struktury **Atollon Directory**, přičemž práva podřízených položek jsou vytvořena na základě **šablonových práv položky**.

Některé objekty dědí práva a podmiňují zobrazení z **vícero nadřazených objektů**. Např. faktura dědí všechna svá práva z nastavení administračního uzlu **Fakturace** + požaduje práva LIST na **Kontext**, ve kterém je faktura uložena + VIEW práva na **Deník**, do kterého faktura náleží.

Výchozí nastavení systému definuje, že všechny zakládáné objekty dědí práva ze své nadřazené složky.

Příklad dědění práv ke zprávě "Poznámka" / e-mailu / dokumentu

Když napíšete poznámku na projekt u klienta, tento je umístěn na kartě klienta, klient je umístěn v organizaci, organizace v instanci a instance v rootu stromové struktury. Dokud se v celé této cestě

práva dědí, tak všechny nadřazené složky ovlivňují práva dané zprávy.

[dedeni-prav-poznamky.png](#)

Strom dědění práv může být košatý, jelikož např. práva projektu jsou ovlivněna právy uživatelů na Typ projektu + na složku klienta, ve které je projekt umístěn.

Obrázek výše znázorňuje cestu práv dané zprávy:

1. ACL dané zprávy (zde by bylo možné nastavit práva jednotlivým uživatelům, kteří mohou danou zprávu vidět/smazat, apod.)
2. ACL složky zpráv pro daný projekt
3. ACL projektu
4. ACL složky klienta
5. Proklik na: a) Definicí typu složky Klient (PROJ...), b) ACL organizace ... a šlo by pokračovat na instanci + kořen stromu (top level)

Nastavení vlastních práv pro objekt = zakázání dědění

Pokud chcete nastavit na objekt zcela jiná oprávnění, než určuje nadřazená složka, je nutné zrušit dědění. Dědění je možné zastavit tím, že se odkazy na nadřazené uzly vymažou. Poté je možné nastavit práva pro každý objekt v Atollonu individuálně.

[dedeni-prav-zrusit-dedeni.png](#)

Práva na jednotlivé funkcionality

Níže naleznete odkazy na dokumentaci k nastavení práv jednotlivých modulů. Neváhejte kontaktovat svého konzultanta v Atollonu se žádostí o případné rozšíření / doplnění a vysvětlení kroků.

Práva na kontext

Definujte práva na typy složek (klienty), typy projektů (obchodní případy, služby, podpora, ...) nebo typy aktivit.

Práva na dokumenty

Definujte práva na dokumentové složky nebo dokumenty samotné.

Revision #13

Created 24 July 2020 04:55:08 by safka

Updated 24 July 2020 12:55:21 by safka