IMPLEMENTACE IDENTITY AND ACCESS MANAGEMENTU

Jakub Balada
Doktorand KIT FIS VŠE, jakub.balada@siemens.com

ABSTRAKT:

Na implementaci systémů Identity a Access Managementu jsou kladeny stále větší požadavky, které již nelze namapovat na standardní RBAC model. Tento článek navrhuje rozšíření hierarchického RBAC modelu na základě zkušeností s implementací rozsáhlých IAM řešení. Současně popisuje opakující se požadavky zadavatelů, pro které navrhuje možné řešení. Dále popisuje zajímavé řešení Single-Sign-On autentizace pro organizaci s informačními systémy založenými na webových aplikacích.

ABSTRACT:

Typical IT environment in large organization is much more complicated than it was few years ago. More and more processes and administration are going under IT solutions. That causes that number of new applications, web services, databases etc. grows rapidly. The increasing overhead of a heterogeneous environment administration can be reduced by implementation of an identity and user access right management.

This article focuses on a core of IAM products – the RBAC model. More and more requirements cause that standard RBAC model in not enough for typical implementation of IAM. Therefore this article shows some solutions for repetitious requirements and tries to define new type of RBAC model.

Model defined in this article is in an implementation phase of complex solution of IAM in Czech Republic for an organization with more than 16 thousands employees.

Last part of an article describes solution of an access management using single-sign-on authentication.

KLÍČOVÁ SLOVA:

Identity management, Access management, RBAC model

ÚVOD

Identity a Access Management (IAM) je jednou z rychle se rozvíjejících oblastí systémové integrace. Jeho hlavním cílem je správa uživatelů a jejich přístupových oprávnění do informačních systémů organizace. Těmito uživateli nemusejí být pouze zaměstnanci, ale například také zákazníci, dodavatelé apod. Typicky se implementuje společně se Single-Sign-On autentizací, kdy se uživatel přihlašuje do systému pouze jednou. Ostatní systémy napojené na IAM poté tuto autentizaci přebírají.

Stále více velkých organizací věnuje této problematice větší pozornost a přechází od proprietárních řešení k implementaci standardních produktů, které nabízejí širší funkcionalitu. Na druhou stranu ani tyto systémy ve většině případů nepokryjí veškeré požadavky organizace, a proto se rozšiřují o speciální funkcionality. Některé z nich jsou natolik zajímavé, že by mohly rozšířit základní Role Based Access Control (RBAC) model IAM systémů.

Tento autorizační model byl prvně popsán v článku [2] v roce 1992. Jde o alternativní přístup k definici přístupových oprávnění. Je založen na přiřazení jednotlivých oprávnění do informačních systémů organizace ne přímo uživateli, ale přes role. Těmi se většinou myslí byznys role organizace, jako je obchodník, auditor, administrátor apod. Nejsou tedy definovány vazby mezi uživateli a jejich oprávněními, ale tyto vazby jsou dány tranzitivně – vazbami mezi uživateli a jejich rolemi v organizaci a následně mezi rolemi a jejich oprávněními.

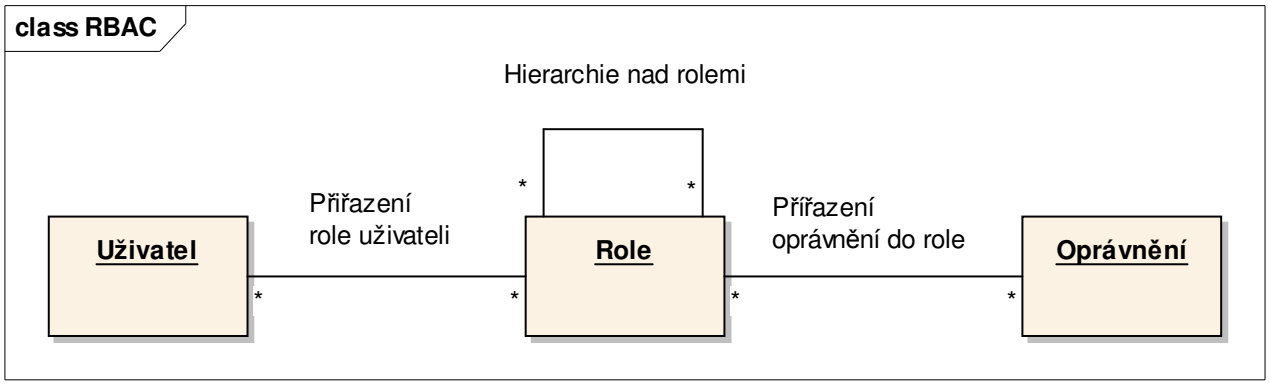
V roce 2000 byly v rámci standardu NIST [3] definovány 4 základní úrovně RBAC modelu:

- Flat RBAC – základní model
- Hierarchical RBAC – základní model rozšířený o hierarchii nad rolemi
- Constrained RBAC – přidání statického vyloučení práv (tzv. separation of duties - SOD)
- Symmetric RBAC – přidání dynamického vyloučení práv

Tento článek se zabývá možným rozšířením hierarchického modelu o další funkcionality, které byly požadovány při implementaci IAM systémů u velkých organizací. Příklad takové implementace byl publikován v [1] a [4].

HIERARCHICKÝ RBAC MODEL

Tento model rozšiřuje základní RBAC model o hierarchii nad rolemi, která přináší možnost dědit práva mezi rolemi, viz obrázek 1.



Obrázek 1. Hierarchický RBAC model podle [3]

Vztahy mezi objekty lze popsat teorií množin následovně:

$$RO \subseteq R \times O,$$

kde RO je přiřazení oprávnění do role, R role a O oprávnění,

$$UR \subseteq U \times R,$$

kde UR je přiřazení role uživateli a U uživatel a nakonec

$$RH \subseteq R \times R,$$

kde RH je částečné uspořádání nad rolemi.

Při běžné implementaci IAM řešení je snaha realizovat tento model v prostředí organizace. Tato snaha ovšem vede v lepším případě k značné redukci požadavků, v horším k proprietárnímu rozšíření tohoto modelu. Důvodem většinou bývá neochota organizace k reingeneeringu procesu přidělování oprávnění z důvodu návaznosti na ostatní systémy či speciální požadavky na tento proces.

Běžný požadavek na rozšíření hierarchického RBAC modelu

Jedním z častých požadavků je možnost přiřazení oprávnění přímo uživateli. Jedná se o hrubé porušení tohoto modelu, který se zakládá právě na přiřazování zásadně přes role. V praxi je ovšem často potřeba řešit operativně například dočasné přiřazení oprávnění pro nutný zásah delegované osoby, která nemá přístup k potřebným datům. Ve standardním modelu by bylo potřeba vytvořit speciální roli s tímto jediným oprávněním, či přiřadit existující roli obsahující toto oprávnění. V prvním případě se jedná o proces, který většinou podléhá schvalování, a tudíž je časově náročnější, v druhém se může jednat o bezpečnostní riziko, kdy uživatel dostane přidělena oprávnění, ke kterým nemá mít nárok.

Z těchto důvodů většina IAM produktů umožňuje toto přiřazení, i když se jedná o porušení základního RBAC modelu. V množinovém zápise je jedná o vztah

$$UO \subseteq U \times O,$$

kde UO je přiřazení oprávnění přímo uživateli.

NÁVRH NOVÉHO TYPU RBAC MODELU

Jelikož některé požadavky překračující základní RBAC model jsou zajímavé a hlavně se vyskytují u více organizací, nabízí se možnost vytvoření nového typu RBAC modelu. Návrh nového typu popsaného níže je hlavním cílem tohoto článku.

Jedním z těchto požadavků je možnost přiřazení rolí také k pracovním pozicím. Ty jsou v rámci organizace vytvořeny pro každé pracovní místo, tedy běžně namapovány na uživatele (zaměstnance organizace) 1:1. Obecně má však tato vazba kardinalitu m:n, jelikož zaměstnanec může mít více pracovních pozic (například generální ředitel a předseda představenstva) a na jedné pozici může být více zaměstnanců (například při krátkodobém záskoku).

Jedná se tedy o vytvoření nového objektu Pozice (P) a definování vazby

$$UP \subseteq U \times P,$$

kde UP je vazba mezi uživatelem a pracovní pozicí. Pokud by bylo umožněno přiřazení role na pozici, mohl by mít uživatel přiřazené role nepřímo přes pozici.

Na druhou stranu by bylo třeba nadefinovat a spravovat vazbu mezi pozicí a rolemi. Jelikož pozicí je přibližně stejné množství jako zaměstnanců a pozice na jedné úrovni v organizační jednotce mají typicky nadefinována tatáž oprávnění, přichází v úvahu jejich sjednocení.

K tomuto účelu lze definovat Sadu (S), která bude mít následující vazby:

$$PS \subseteq P \times S,$$

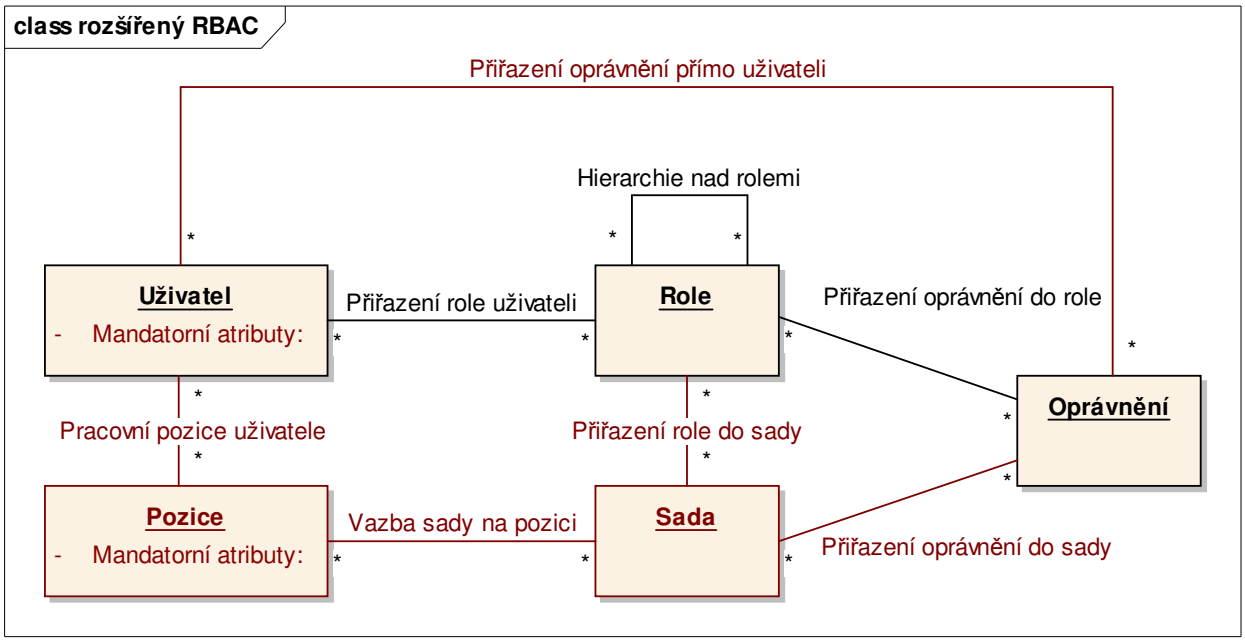
kde PS je přiřazení sady na pozici,

$$SR \subseteq S \times R,$$

kde SR je přiřazení role do sady a nakonec

$$SO \subseteq S \times O,$$

kde SO je přiřazení oprávnění do sady. Sadu tedy tvoří množina oprávnění přiřazených napřímo nebo přes role a tato sada je přiřazena k pozici. Sady navíc oproti rolím umožňují sjednocení rolí a oprávnění napříč hierarchií nad rolemi, což je také častý požadavek. Při nasazení řešení se počítá s namapováním sad na pozice 1:1 a poté s optimalizací počtu sad a tím k přechodu na 1:n. Celkové schéma rozšířeného RBAC modelu je znázorněno na obrázku číslo 2.



Obrázek 2. Návrh nového typu RBAC modelu

Jedním z velkých přínosů tohoto řešení je automatické přiřazení sady a potažmo rolí a oprávnění pro nového zaměstnance, který je přijat na již existující pozici. Touto automatizací se ušetří čas nutný k definování oprávnění pro nového zaměstnance a jejich schválení. Ke stejné optimalizaci dojde při vytváření nové pozice, kdy stačí pouze napojit tuto pozici na sadu.

Také personální procesy, jako krátkodobý záskok nebo například souběh na jedné pozici při zaškolování nového zaměstnance odcházejícím, se obejdou bez zdlouhavého definování a schvalování rolí pro dané zaměstnance.

MANDATORNÍ ATRIBUTY

Dalším častým požadavkem na systém IAM je potřeba spravovat speciální atributy pro přístupové účty do informačních systémů. Typicky se jedná o speciální atributy uživatele, které nejsou přebírány z autoritativního zdroje identit (typicky personální systém), ale jsou potřeba pro vytváření účtů daných uživatelů v systémech napojených na IAM. Například se jedná o jazykové dovednosti uživatele či jeho jiné znalosti.

Základní problém je v nemožnosti realizace těchto informací pomocí základních oprávnění, jelikož se většinou jedná o číselníkové položky a pro každou takovou položku by muselo existovat oprávnění. V některých případech se může jednat dokonce o hodnotu z daného rozsahu, což by vedlo k neúměrnému množství spravovaných oprávnění.

Elegantním řešením je rozšíření objektů uživatel a pozice o seznam těchto atributů, jak je znázorněno taktéž na obrázku 2. Při vytváření účtu v systému napojeném na IAM (standardně při přidělení prvního oprávnění pro daný systém), který vyžaduje mandatorní

atributy, jsou tyto atributy převzaty z informací uživatele, které většinou musí sám zadat. Pokud se ovšem jednalo o oprávnění přiřazené přes sadu a pozici, uživatel nemusí tyto atributy zadávat, jelikož se automaticky převezmou z pozice.

V praxi to znamená další optimalizaci procesu příchodu nového zaměstnance za odcházejícího, kdy se většinou přijímá zaměstnanec se shodnými dovednostmi na stejnou pozici. Technicky se jedná o zrušení přístupových účtů odcházejícího zaměstnance a vytvoření nových pro přijímaného, ovšem tento proces může proběhnout plně automaticky bez zásahu nadřízeného, schvalovatele či administrátora.

VIDITELNOST

Zajímavou oblastí v rámci modelu uživatelských oprávnění a jejich přiřazovaní uživatelům je tzv. viditelnost. Jedná se o nastavení práv umožňujících žádat o oprávnění (role, sady) ať už uživatelem pro sebe sama, či nadřízeným pro svého podřízeného. Jde v podstatě o zúžení rozsahu možných oprávnění pro daného uživatele.

Většina IAM systémů řeší tuto problematiku pomocí tzv. access policies, které jsou založeny na access control listech nad jednotlivými objekty. Jenže správa těchto práv pro všechny potřebně objekty je velmi náročná, navíc jsou často kladeny další požadavky na viditelnost, které nejsou z principu realizovatelné pomocí access policies.

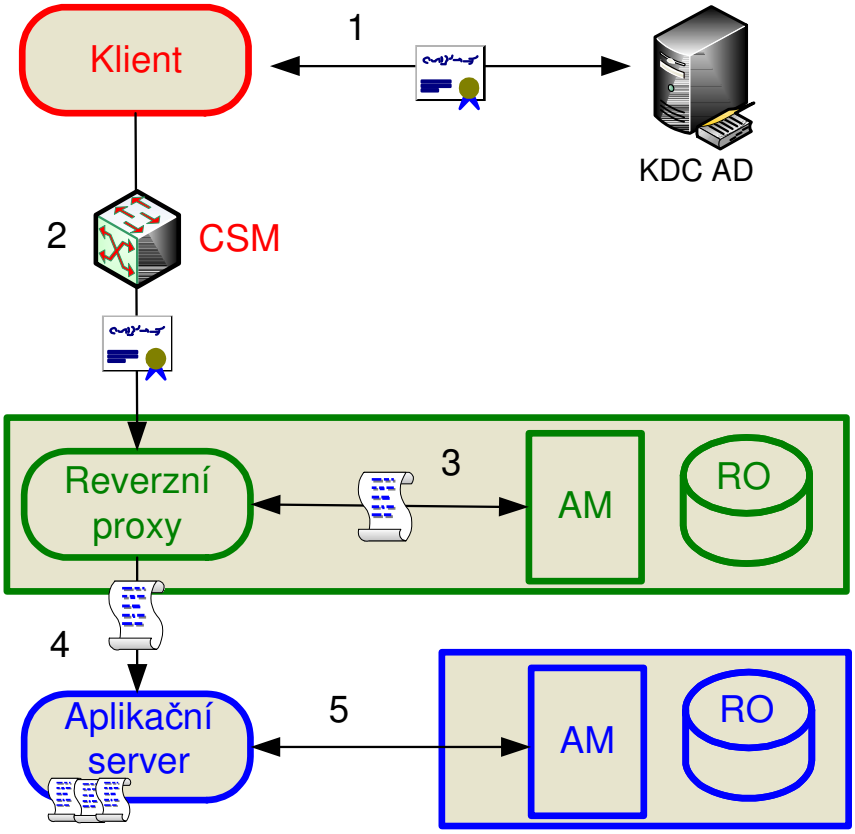
Typickým požadavkem na viditelnost je omezení možnosti přidělit některá oprávnění na základě informací uživatele přebíraných z personálního systému. Jedná se například o místo výkonu práce, profesi, typ zaměstnaneckého poměru apod.

Jako řešení se nabízí přidání těchto atributů také k objektům, ke kterým je třeba řídit přístup, a poté nastavit pravidla pro vyhodnocování viditelnosti. Tento dílčí postup je podobný logice mandatory access control, což je předchůdce RBAC modelu používaného zejména u operačních systémů.

Dalším požadavkem na viditelnost může být rozhodování podle umístění garanta daného práva (oprávnění, role, sady) v organizačním stromě. Tato pozice je poté nastavena v atributu tohoto práva a možnost zažádat o něj mají pouze zaměstnanci v organizačním podstromě této pozice a všichni nadřízení v přímé linii. Vyhodnocení těchto pravidel probíhá vždy při vytváření seznamu práv pro žádost nadřízeného či samotného zaměstnance.

ACCESS MANAGEMENT

Do této doby se článek zabýval identity managementem, který spravuje uživatele a jejich přístupová práva, ale již je nestará o samotnou autentizaci a autorizaci uživatelů. Práce Identity Manageru končí propagací uživatelů a jejich práv buď přímo do cílových systémů (jednotlivých informačních systémů organizace) nebo do tzn. Access manageru. A právě využití tohoto nástroje pro řešení autentizace a následně autorizace uživatelů do všech webových aplikací organizace si ukážeme na následujícím řešení.



Obrázek 3. Proces autentizace a autorizace uživatelů

Jak je znázorněno na obrázku 3, toto řešení využívá tzn. reverzní proxy, která ověřuje identitu uživatele předávanou v tomto případě Kerberos tiketem (provádí autentizaci uživatele) a následně z uložiště Access Manageru zjišťuje, zda daný uživatel má alespoň jedno oprávnění do aplikace, ke které chce přistupovat (autorizace uživatele). V kladném případě propustí požadavek na aplikační server s identifikací uživatele v hlavičce požadavku.

Celkový proces probíhá následujícím způsobem:

1. Klientská část aplikace si z KDC vyžádá Kerberos tiket pro komunikaci se serverovou částí
2. Klient pošle http požadavek rozšířený o tiket na reverzní proxy přes content switch
3. Reverzní proxy verifikuje tiket a zažádá Access Manager o seznam přístupových práv pro daného uživatele a požadovanou aplikaci
4. Proxy přidá identitu uživatele (logon name) do hlavičky http požadavku a ten přepošle na serverovou část aplikace (pokud má uživatel alespoň jedno právo pro danou aplikaci)
5. Aplikační server si může dotáhnout další informace o uživateli a jeho přístupových právech

Toto řešení je typickým příkladem implementace Single-Sign-On, kdy se uživatel autentizuje pouze jednou (například přihlášením do domény) a následně může pracovat s jednotlivými aplikacemi bez nutnosti další autentizace.

ZÁVĚR

Rozšířený RBAC model popsaný v tomto článku je právě ve fázi implementace v organizaci s více jak 16 tisíci zaměstnanci. V rámci proof of concept nebyly nalezeny žádné překážky k jeho plnému nasazení. Bohužel standardní IAM produkty jsou založeny striktně na RBAC modelu a je potřeba je proprietárně rozšiřovat podle požadavků popsaných výše. Je na zvážení, zda některé z nich nejsou natolik odůvodnitelné, aby je tyto produkty zvaly na vědomí a rozšířily svoji funkcionalitu implementací nového typu RBAC modelu, například výše definovaného.

Popsané řešení autorizace uživatelů bylo použito při implementaci IAM systému pro organizaci ve státní správě s více jak 9 tisíci uživateli a je úspěšně v produkci již přes dva roky.

LITERATURA

[1] Vohnoutová M.: Identity and Access Manager. 30th Europen konference, (2007).

[2] Ferraiolo, D.F., Kuhn, D.R.: Role Based Access Control. 15th National Computer Security Conference, (October 1992) 554-563.

[3] Sandhu, R., Ferraiolo, D.F., Kuhn, D.R.: The NIST Model for Role Based Access Control: Toward a Unified Standard. 5th ACM Workshop Role-Based Access Control, (July 2000) 47-63.

[4] Balada J.: Implementace Workflow pro Identity Management, 30th Europen konference, (2007).