Explozívne roly

Riadenie prístupov na základe rolí (Role-Based Access Control, RBAC) je veľmi často používaná a odporúčaná bezpečnostná praktika. Pri praktickom použití však počet rolí veľmi rýchlo rastie, až nakoniec exploduje. Dá sa tomu zabrániť? Je možné RBAC efektívne použiť aj v rozsiahlych a zložitých systémoch?

Explózia rolí je vážny problém komplexných riešení pre správu identít a prístupov (IAM). Počet rolí potrebných na správu privilégií skupiny používateľov môže veľmi rýchlo narásť na niekoľkonásobok počtu používateľov. Toto tvrdenie môže byť prekvapivé pre ľudí, ktorí ešte neimplementovali zložitý IAM projekt. Samotný princíp RBAC [1] bol predsa navrhnutý na uľahčenie a nie na skomplikovanie správy privilégií. To je však teória. V realite je niekoľko dôvodov, prečo sa počet rolí ľahko vymkne spod kontroly:

- Karteziánsky súčin: Typické príklady rolí v bankovom prostredí sú teller a supervisor. Ak má banka pobočky v Londýne a Bratislave, tak veľmi rýchlo vzniknú roly london teller, london supervisor, bratislava teller, bratislava supervisor a podobne.

- Atomizácia: Karteziánsky súčin môže byť niekedy eliminovaný alebo aspoň zmiernený rozdelením rolí na menšie časti a ich následným rekombinovaním. Bezpečnostný princíp najmenších privilégií však spôsobuje tendenciu atomizovať tieto roly na malé časti, pričom každá časť obsahuje len veľmi špecifické privilégiá. Preto narastá celkový počet rolí.

- Unikátnosť: V bežných prípadoch má podstatná časť používateľov systému kombináciu privilégií, ktorú nepoužíva nikto iný. Pre takých používateľov RBAC model neprináša žiadne podstatné zjednodušenie.

Dôsledkom je, že v bežných prípadoch počet rolí prekračuje počet používateľov. To znamená, že relatívne ťažký problém správy používateľov sa zmenil na oveľa ťažší problém správy rolí.

Naivným riešením sú rôzne pokusy o manažérske zvládnutie vzniknutej situácie. Bežným prístupom je zavedenie procesu žiadostí a schvaľovaní a procesu riadenia životného cyklu rolí. Pri veľkom počte rolí však schvaľovatelia rýchlo stratia prehľad o tom, čo je správne, a schvália každú žiadosť, ktorá „vyzerá dobre“. Racionálne hľadisko je potlačené a rozhodnutia sa vykonávajú intuitívne. Tento prístup niekedy skutočne vedie k relatívne funkčnému pracovnému procesu. Ale je zrejmé, že v takomto prípade bezpečnosť celého systému ťažko trpí.

Hybridný RBAC model

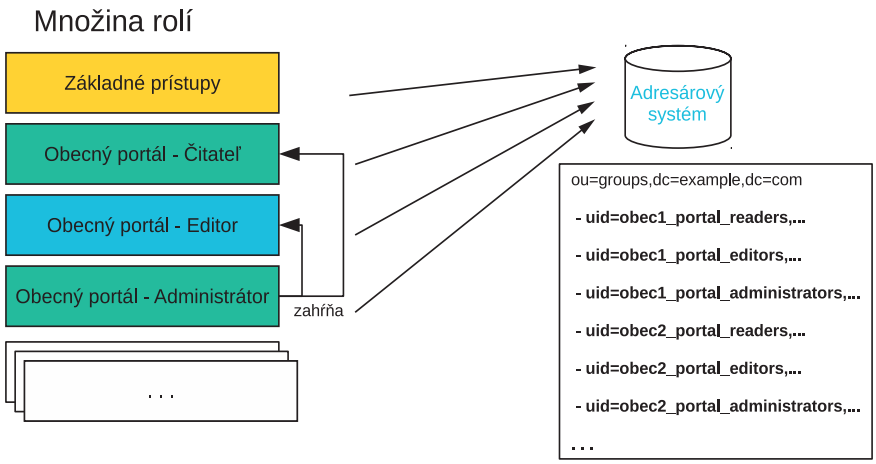
Samotný RBAC model v jeho čistej podobe nedokáže tieto problémy uspokojivo zvládnuť. Je zrejmé, že potrebujeme zmeniť prístup k problému. O takýto nový prístup sa pokúša model ABAC (Attribute-Based Access Control) [2]. Model ABAC nepoužíva koncept roly a je založený výhradne na výrazoch (algoritmoch). ABAC je veľmi flexibilný model, má však podstatné praktické obmedzenia. Z pohľadu IAM riešení je problematický najmä chýbajúci koncept roly. Pri ABAC aplikáciách chýba niečo, o čo je možné žiadať a čo sa dá schváliť, analyzovať a auditovať. Toto predstavuje obrovskú prekážku pre praktické IAM riešenia.

Hybridné RBAC modely sa snažia skombinovať výhody modelov RBAC a ABAC. V hybridných RBAC systémoch existujú roly podobne ako v čistých RBAC modeloch. Rola však už nie je statická deklaratívna entita. Roly môžu obsahovať výrazy, ktoré sú veľmi podobné výrazom z ABAC modelov[3]. Výrazy poskytujú obrovskú flexibilitu, ich združenie do rolí však poskytuje formalizmus potrebný na zvládnutie zložitosti celého systému.

Hybridné RBAC modely sú veľmi silné, ak sa použijú správne. Je to však relatívne slabo preskúmaná oblasť. Zdá sa, že v tejto oblasti udávajú rytmus najmä systémy na správu identít (IDM systémy). Implementácia hybridných RBAC modelov bola v tejto oblasti bežná už pred desaťročím a dnes sa považuje za úplnú nutnosť. Jednoduché hybridné RBAC modely však tiež majú svoje obmedzenia, preto súčasné špičkové IDM systémy implementujú pokročilé hybridné RBAC modely. Tieto modely umožňujú parametrizáciu rolí pri ich priraďovaní, podmienenú hierarchiu rolí, časové ohraničenia (platnosť „od – do“), podporu pre organizačné štruktúry, legalizáciu výnimiek z RBAC pravidiel a podobne.

Prípadová štúdia

Hybridný RBAC model sme s úspechom použili v niekoľkých projektoch. Tento model sa ukázal ako obzvlášť užitočný pri tvorbe takzvaných „cloud“ aplikácií. Tieto aplikácie sú multitenantné, čo znamená, že rovnaká aplikácia je poskytovaná množstvu organizácií („tenantov“), pričom jednotlivé organizácie sú od seba čiastočne alebo úplne izolované. Špecifikom tohto prostredia je to, že pre všetkých tenantov sa používajú roly, ktoré sú vo svojej podstate rovnaké. Tieto roly sa pre každého tenanta líšia len v detailoch, ako je napríklad práve identifikátor tenanta, pre ktorého daná rola umožňuje prístup. Je zrejmé, že v jednoduchom RBAC modeli táto situácia vedie k explózii rolí. V hybridnom RBAC modeli je však možné tieto roly efektívne implementovať. Toto je dosiahnuté použitím výrazu, ktorý ako vstup použije identifikátor tenanta z používateľského profilu (pri úplnej izolácii tenantov), alebo je tento identifikátor špecifikovaný ako parameter pri prideľovaní roly (pri čiastočnej izolácii tenantov).



Obr. 1: Obecný portál s tromi definovanými prístupovými právami

Tento multitenantný prístup skombinovaný s modelom organizačnej štruktúry bol použitý pri dvoch projektoch v oblasti služieb pre samosprávy vo dvoch rôznych európskych krajinách. Obe riešenia boli implementované s použitím špičkového IDM systému s otvoreným zdrojovým kódom (open source), ktorý podporuje pokročilý hybridný RBAC model. Práve využitie špičkového produktu a veľmi flexibilného RBAC modelu umožnilo implementovať komplexné bezpečnostné požiadavky za relatívne krátky čas. Nasledujúca prípadová štúdia popisuje jeden z týchto projektov.

Cieľom projektu bolo vytvorenie „cloud“ prostredia, ktoré slúži na poskytovanie rôznorodých služieb samosprávam. Súčasťou riešenia je aj IAM subsystém, ktorého úlohou je spravovať komplexnú štruktúru prístupových práv používateľov k jednotlivým obciam, aplikáciám a systémovým funkciám.

Jednotlivé obce (tenanti) sú v riešení modelované ako organizačné jednotky. Používatelia sú typicky zaradení v jednej organizačnej jednotke zodpovedajúcej obci, ktorá požiadala o vytvorenie prístupov pre používateľa. V tejto organizačnej jednotke sa používateľ zobrazuje pri prezeraní organizačnej štruktúry. Roly slúžia na špecifikáciu rôznych úrovní prístupu a umožňujú vytvárať a udržiavať prístupové práva používateľov v pripojených systémoch.

Požiadavkou projektu bola čiastočná izolácia tenantov a zdieľanie identity: jeden používateľ môže mať iba jednu identitu v IDM systéme, ale môže mať oprávnenie na prístup k viacerým tenantom (ak pracuje pre viacero obcí), pričom pre každého tenanta môže mať iné prístupové práva. Preto sú roly navrhnuté ako parametrické a identifikátor obce (tenant) je špecifikovaný ako parameter pri prideľovaní roly. Tento parameter sa potom používa vo výrazoch v rolách pre nastavenie atribútov účtov alebo prístupových práv v aplikácii (napr. zaradenie do skupín v adresárovom serveri). Výrazy sú väčšinou veľmi jednoduché, napr. priradenie požadovanej skupiny v adresárovom systéme na základe jej mena, v ktorom sa používa identifikátor obce.

Ako príklad si možno predstaviť aplikáciu Obecný portál s tromi definovanými prístupovými právami: čitateľ (skupina „<tenant>_portal_readers“), editor (skupina „<tenant>_portal_editors“) a administrátor (skupina „<tenant>_

portal_administrators“). Tieto skupiny existujú v adresárovom systéme pre každého tenanta v riešení, roly v IDM systéme sú však vďaka hybridnému RBAC modelu iba tri: Obecný portál – Čitateľ, Obecný portál – Editor a Obecný portál – Administrátor, a tieto sa priraďujú používateľom s príslušným parametrom identifikátora obce (viz Obr. 1).

Roly sa v IDM systéme vytvoria typicky pri požiadavke na pripojenie novej aplikácie do riešenia.

V adresárovom systéme existujú pre aplikáciu Obecný portál skupiny s identifikátormi (napr. atribút „uid“):

1. obec1_portal_readers
2. obec1_portal_editors
3. obec1_portal_administrators
4. obec2_portal_readers
5. obec2_portal_editors
6. obec3_portal_administrators

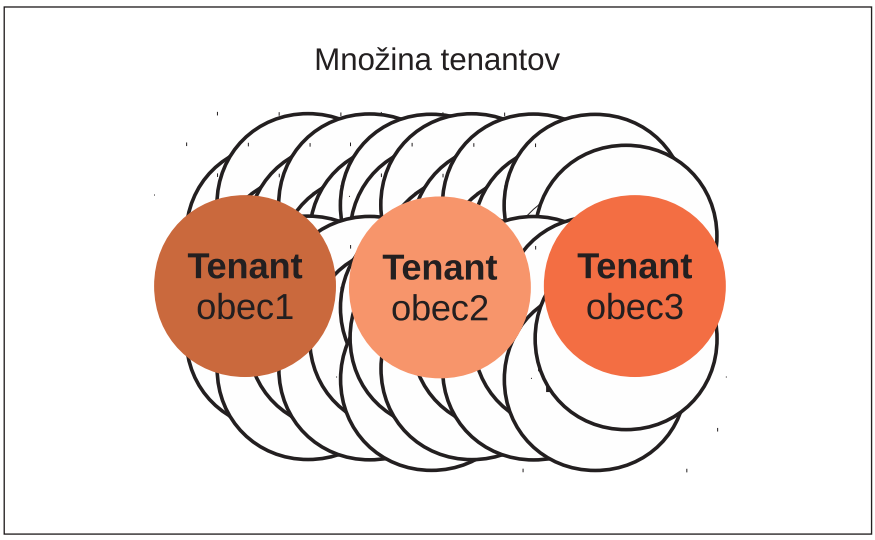
atď. Analogicky existujú aj skupiny pre ďalšie aplikácie, ktoré sú integrované s adresárovým systémom. Tieto skupiny spravuje samotný IDM systém, takže pri pripojení nového tenanta do riešenia sa vytvoria potrebné skupiny automaticky. Následne je možné priradiť roly s parametrom nového tenanta používateľom (viz Obr. 2).

Priradenie rolí s parametrom tenant (IDM systém umožní vybrať iba existujúceho tenanta) znázorňuje obrázok 3.

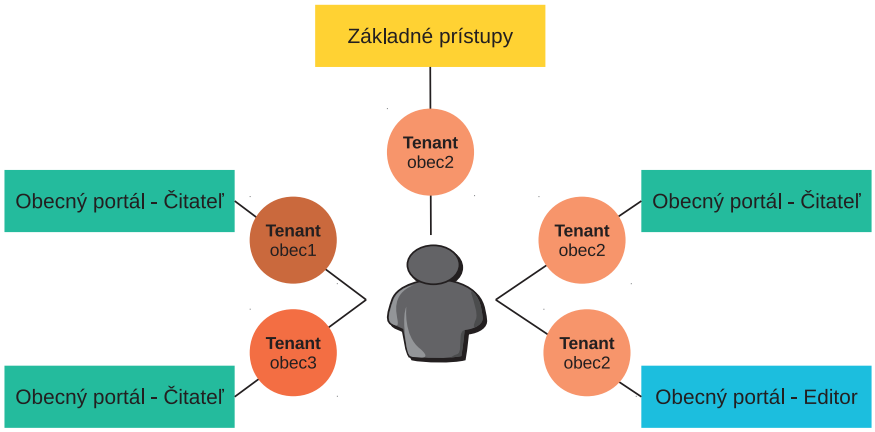
Dôsledkom uvedeného priradenia rolí bude členstvo používateľa v nasledujúcich portálových skupinách adresárového systému:

- obec1_portal_readers
- obec2_portal_readers
- obec2_portal_editors
- obec3_portal_readers

Okrem týchto rolí môže mať používateľ samozrejme aj ďalšie roly, napr. Základné prístupy.



Obr. 2: Tenanty v IDM systéme



Obr. 3: Priradenie rolí s parametrom tenant.

Logika aplikovaná v rolách na podporu multitenantnosti je veľmi jednoduchá. Parameter s identifikátorom tenanta je označený ako tenant. Výsledkom priradenia roly má byť asociácia používateľa so skupinou (členstvo v skupine). Skupina sa vyhľadáva na koncovom systéme podľa podmienky pre atribút „uid“ skupiny tak, že sa hľadá skupina s identifikátorom s hodnotou „tenant_portal_readers“.

```
<role>
<name>Obecný portál - Čitateľ</name>
<associationTargetSearch>
<equal>
<path>attributes/uid</path>
<expression>
        if (!basic.isEmpty(tenant)) {
          return tenant + '_portal_readers'
        }
</expression>
</equal>
</associationTargetSearch>
</role>
```

Analogicky sme implementovali ostatné portálové roly, ako aj roly pre viacero ďalších aplikácií. Hoci nie všetky aplikácie využívajú na autorizáciu adresárový systém, multitenantné roly sa dajú rovnakým spôsobom aplikovať aj pre ne. Model je dostatočne univerzálny, či už ide o priraďovanie skupín v adresárovom systéme, alebo vytváranie riadkov v relačnej databáze.

Roly môžu byť hierarchické, napr. rola Obecný portál – Administrátor zahŕňa aj roly Obecný portál - Čitateľ a Obecný portál – Editor, pričom parameter tenant z priradenia roly sa vzťahuje aj na nižšie roly v hierarchii. Alebo je možné jednoduchou konfiguráciou rolí dosiahnuť stav, kedy rola Základné prístupy priradená používateľovi pre tenanta obec1 zahrnie aj rolu Obecný portál – Čitateľ pre tenanta obec1. Takto je možné znížiť námahu na priraďovanie prístupov.

Roly je možné priebežne dopĺňať o nové prístupové práva, výrazy či zahrnuté roly. Na prepočítanie prístupových práv používateľov rolí po ich zmenách slúžia funkcie použitého IDM systému.

Výhodou je aj možnosť použitia podmienených výrazov v rolách: rovnaká rola priradená iným typom používateľov (napr. pracovník obce a pracovník dodávateľa) majú za následok vytvorenie odlišných účtov – rôzne menné konvencie pre identifikátory účtov, rôzne umiestnenie v adresárovom strome a pod. Rovnaký mechanizmus zabraňuje operátorovi priradiť pracovníkovi obce rolu určenú iba pre administrátorov riešenia.

Pokiaľ ide o správu rolí, okrem ich relatívne malého počtu prispieva k použiteľnosti riešenia aj ich rýchle vytváranie vzhľadom na jednoduchosť použitých výrazov. Často ide o záležitosť niekoľkých minút. V systéme sú samozrejme aj „netenantné“ roly, ktoré sa používajú pre systémy bez konceptu tenantov. Schopnosť pokryť veľmi široké spektrum požiadaviek pomocou jedného modelu robí celé riešenie značne flexibilným.

Keďže sa dáta v riešení v čase menia (okrem nových používateľov vznikajú v systéme aj noví tenanti), IDM systém pri vytvorení novej obce vytvorí aj príslušné objekty v koncových systémoch, napr. kontajnery v hierarchickej štruktúre adresárového systému, skupiny pre prístup k portálu obce spomenuté v príklade a pod.

Bez IDM systému by bolo potrebné tenantov, príslušné skupiny, kontajnery a ďalšie objekty – predovšetkým používateľské účty - spravovať ručne. Navyše bez koncepcie rolí by bolo riešenie zahltené správou množstva skupín pre všetky aplikácie. Pre tieto skupiny poskytuje IDM systém zjednodušujúci pohľad vo forme rolí. Počet rolí však nerastie priamo úmerne so zvyšovaním počtu tenantov, ale len prirodzeným spôsobom pri pridávaní nových aplikácií do systému.

Záver

Jednoduchý RBAC model je dobre formalizovaný, ustálený a ľahko použiteľný model pre správu identít. Jeho jednoduchosť je však aj jeho slabinou. RBAC model naráža v praktických situáciách na svoje limity a veľmi často vedie k explózii rolí. Na druhej strane spektra sú veľmi flexibilné modely ABAC, ktorých praktické použitie je však obmedzené slabou formalizáciou bezpečnostných konceptov. Hybridné RBAC modely kombinujú výhody oboch prístupov, preto sme sa rozhodli takýto model použiť pre naše IAM riešenia. Praktické skúsenosti z IAM projektov jednoznačne ukazujú prínos hybridných RBAC modelov. Tento prínos je zrejmý v bezpečnostnej oblasti. Správne použitý hybridný RBAC model vedie k prehľadnejším štruktúram rolí a výrazov. Prehľadné štruktúry sa lepšie udržiavajú, sú menej náchylné na chyby a je oveľa jednoduchšie ubezpečiť sa o ich správnosti (audit).

Ako naše projekty ukazujú, jednoduchosť, ktorú hybridné RBAC modely prinášajú, má však aj priamy ekonomický prínos: projekty je možné implementovať za kratší čas a s nižšími nákladmi. A je to práve ekonomická náročnosť, ktorá je jednou z najväčších prekážok použitia IAM technológií. Preto si myslíme, že hybridné RBAC modely majú pred sebou jasnú budúcnosť.

Ivan Noris
ivan.noris@evolveum.com

Radovan Semančík
radovan.semancik@evolveum.com

Ing. Ivan Noris

Absolvoval odbor softvérové inžinierstvo na Slovenskej technickej univerzite v Bratislave. V oblasti IAM pôsobí od roku 2003. V súčasnosti pracuje v spoločnosti Evolveum ako hlavný inžinier pre nasadzovanie IAM riešení.

Ing. Radovan Semančík, PhD.

Absolvent Slovenskej technickej univerzity v Bratislave. Pracuje v spoločnosti Evolveum ako softvérový architekt pre vývoj produktov na správu identít. Prispievateľ do niekoľkých open source projektov.

POUŽITÉ ZDROJE

[1] Role Based Access Control (RBAC) and Role Based Security, NIST, http://csrc.nist.gov/groups/SNS/rbac/
[2] Attribute-Based Access Control (ABAC) – Overview, NIST, http://csrc.nist.gov/projects/abac/
[3] Advanced Hybrid RBAC, Evolveum, https://wiki.evolveum.com/display/midPoint/Advanced+Hybrid+RBAC