Používateľské skupiny

Windows Server

Úvod

- Používatelia i počítače vo firme sa menia viac, či menej často, ale jednotlivé pozície a oddelenia zostávajú stabilné

- Z toho dôvodu je neefektívne aplikovať bezpečnostné politiky a práva na jednotlivých používateľov a počítače, ale na vyššie – všeobecnejšie úrovne, ktoré nazývame používateľské skupiny

Správa per user (neefektívna)

- Ak by sme mali prideľovať práva napr. na zdieľané zložky po jednotlivých používateľoch, bolo by to pri vysokom počte používateľov neefektívne
- Zároveň pri vymazaní práv by vznikol neplatný odkaz v zozname prístupových práv, čo by v budúcnosti mohlo spôsobiť problémy

Správa per group (efektívna)

- Ak priradíme používateľov resp. počítače do skupín, práva a povolenia môžeme aplikovať na skupinu
- Keďže práva sú aplikované na skupinu, po vymazaní používateľa nezostane neplatný odkaz v zozname prístupových práv, pretože tie sú aplikované na skupinu a nie na používateľa

Možnosti zoskupovania skupín

- Skupiny je možné zoskupovať do iných skupín pre efektívnejšiu správu zdieľania
- Pri vytvorení skupín podľa spôsobu prístupu k zdieľaným zložkám, potom stačí do skupín s pridelenými právami vložiť jednotlivé skupiny vytvorené na základe rolí

Možnosti používateľských skupín

- Identifikácia administratívnych a používateľských rolí
- Filtrovanie skupinových politík zabezpečenia
- Prideľovanie práv a povolení k zdieľaným zdrojom
- Prideľovanie jedinečných politík hesiel
- A podobne ...

Typy a pôsobnosť skupín

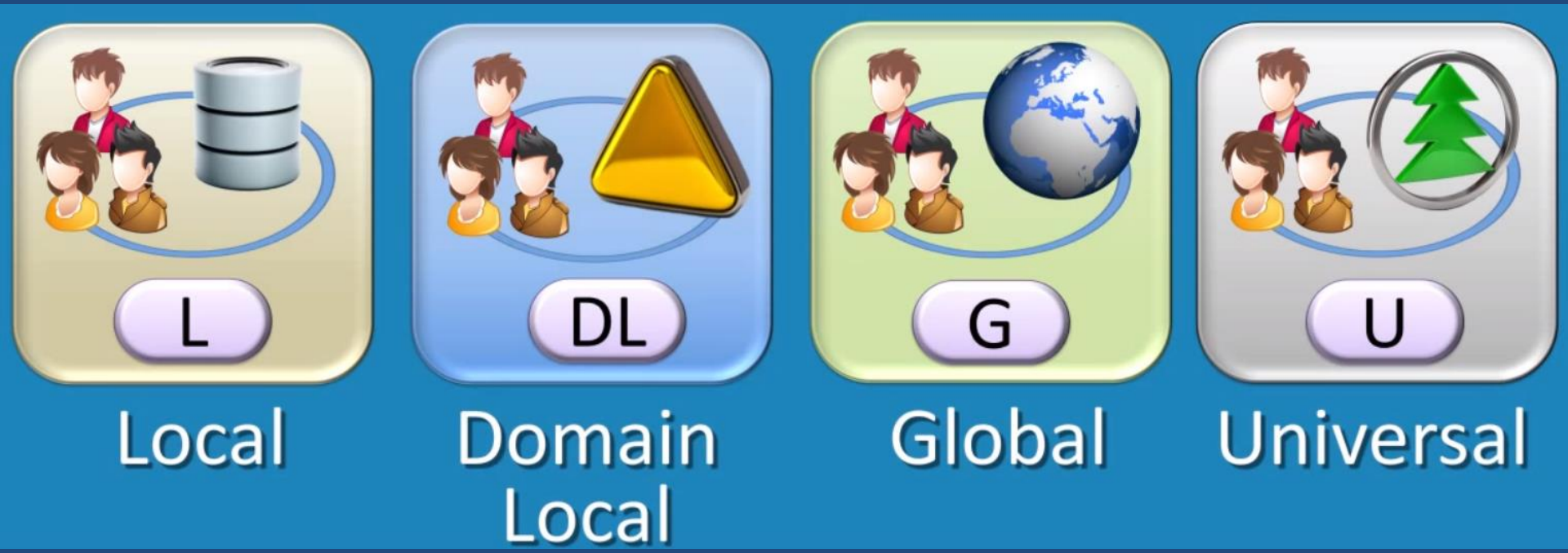
Typy používateľských skupín

- Distribučné (distribution) skupiny – slúžia pre e-mailové aplikácie a nedajú sa použiť pre prideľovanie práv a povolení. Poslaním e-mailu na distribučnú skupinu sa prepošle e-mail všetkým členom skupiny.

- Bezpečnostné (security) skupiny – slúžia pre prideľovanie práv a povolení a riadenie bezpečnosti pre zdieľané zdroje. Môžu sa použiť aj pre preposielanie e-mailov.

Pôsobnosť skupín

- Členom skupín môžu byť používatelia, počítače, či iné skupiny



Lokálne skupiny

- Pôsobnosť majú len na lokálnom počítači – môžem teda pomocou nich prideľovať práva len zdrojom (súborom, zložkám, hardvéru) na jednom počítači
- Nereplikujú sa v rámci domény ani v rámci lesa
- Jej členom môžu byť používatelia, počítače, globálne, univerzálne a doménovo-lokálne skupiny z domény, v ktorej je zaradený počítač
- Viditeľná len v rámci počítača

Globálne skupiny

- Tieto skupiny môžu byť použité na prideľovanie práv na objekty (napr. zdieľanú zložku) v doméne, strome a lese (je viditeľná všade), kde bola skupina vytvorená
- Členom globálnej skupiny však môže byť len objekt (používateľ, počítač, skupina) z domény, v ktorej bola globálna skupina vytvorená
- Pretože sa, narozdiel od ostatných typov skupín, nereplikujú do celého lesa, sú vhodné na správu členov, ktorí sa často menia a neovplyvnia tak množstvo a frekvenciu replikovaných dát v doméne

Doménové lokálne skupiny

- Práva sa prostredníctvom DL skupín dajú prideliť len na objekty (napr. zložky) v doméne, kde bola DL vytvorená
- Členom DL skupiny môžu byť používateľské a počítačové účty, globálne a univerzálne skupiny z ľubovoľnej domény v lese
- Členom DL skupiny môžu byť DL skupiny len v rámci domény, v ktorej bola vytvorená

Univerzálne skupiny

- Používajú sa tam, kde je potrebné prideľovať práva pre objekty v lese zloženom z viacerých domén
- Členom U skupín môžu byť používateľské a počítačové účty, globálne a univerzálne skupiny v celom lese
- Práva prostredníctvom U skupín sa môžu prideľovať na ľubovoľné objekty v lese

Group Scope	Members from the same domain	Members from another domain in the same forest	Members from a trusted external domain
Local	Users Computers Global groups Universal groups Domain local groups Local users defined on the same computer as the local group	Users Computers Global groups Universal groups	Users Computers Global groups
Domain Local	Users Computers Global groups Domain local groups Universal groups	Users Computers Global groups Universal groups	Users Computers Global groups
Universal	Users Computers Global groups Universal groups	Users Computers Global groups Universal groups.	N/A
Global	Users Computers Global groups	N/A	N/A

		Can have members from		
Group	**Scope**	**Same Domain**	**Domain in forest**	**External domain**
Local	Local			
Domain Local	Domain			
Global	Forest/s			
Universal	Forest			

Zdieľanie zdrojov a riadenie prístupu

Zdieľanie zdrojov a riadenie prístupu

- Pri zdieľaní zdrojov (priečinkov, tlačiarní a pod.) je potrebné nastaviť práva pre prístup k týmto zdrojom

- Microsoft odporúča pri menších environmentoch využiť stratégiu A G DL P a pri väčších environmentoch stratégiu A G U DL P

Stratégia A G DL P

- Stratégia A G DL P vraví, že používateľské účty (Accounts) zaradíme do globálnych bezpečnostných skupín (Global), jednotlivé globálne skupiny potom pridáme do doménovo lokálnych bezpečnostných skupín (Domain Local), na ktoré potom priradíme oprávnenia (Permissions) pre daný zdroj

- Takáto hierarchia nám umožní spravovať prístup k zdrojom cez serverového admina a separátnu správu členov skupín cez skupinového admina

Stratégia A G U DL P

- Vo väčších environmentoch, kde máme vytvorené trusty medzi lesmi, je potrebné spravovať prístup k zdrojom z rôznych miest, rôznych domén, stromov a lesov, preto pridávame medzi globálne a doménovo lokálne skupiny ešte jeden krok – vložíme globálne skupiny do univerzálnych, ktoré sú viditeľné aj medzi lesmi v truste


A GOOD DOG
LOVES PEOPLE


ALWAYS GIVE DRAMA
LLAMAS POPCORN

Členstvo vo viacerých skupinách a konflikt povolení

- Ak je používateľ členom viacerých skupín s rôznymi konfliktnými právami (pri jednej je napr. zápis povolený, pri druhej je zakázaný) platí vždy prísnejšie pravidlo, teda zákaz

- Povolenia môžu byť aktívne (Allow), zakázané (Deny) alebo neurčené

- Najčastejšie pre priečinky sú povolenie na čítanie, zápis, spustenie a modifikovanie súboru

```
P + Z = Z
Z + Z = Z
Z + N = Z

N + N = Z
P + P = P
P + N = P

P - povolené
Z - zakázané
N - neurčené
```

NTFS vs. sieťové povolenia

- Na serveri vieme nastaviť dve úrovne prístupu k zdieľaným priečinkom
  - Lokálny prístup = NTFS práva umožňujú špecifikovať, čo môžu s daným súborom/priečinkom vykonávať lokálne resp. cez RDP prihlásení používatelia
  - Sieťový prístup = práva na zdieľanie cez sieť umožňujú špecifikovať, čo môžu s daným súborom/priečinkom vykonávať používatelia, ktorí pristupujú k priečinku cez sieť

NTFS vs. sieťové povolenia

- Štandardne sa pri zdieľaní priečinka nastavia konkrétne NTFS práva a sieťové práva sa nastavia na plný prístup pre všetkých
- Tieto práva sa neskôr dajú zmeniť cez možnosť Vlastnosti/Properties po pravom kliknutí na zložku
- V prípade konfliktu platia už spomínané pravidlá (Deny vyhráva)
- Priečinky je možné zdieľať aj pomocou príkazu net share (popis príkazu v zdrojoch)

Special permissions	Full Control	Modify	Read & Execute	List Folder Contents (folders only)	Read	Write
Traverse Folder/Execute File	x	x	x	x		
List Folder/Read Data	x	x	x	x	x	
Read Attributes	x	x	x	x	x	
Read Extended Attributes	x	x	x	x	x	
Create Files/Write Data	x	x				x
Create Folders/Append Data	x	x				x
Write Attributes	x	x				x
Write Extended Attributes	x	x				x
Delete Subfolders and Files	x					
Delete	x	x				
Read Permissions	x	x	x	x	x	x
Change Permissions	x					
Take Ownership	x					
Synchronize	x	x	x	x	x	x

NTFS práva

Sieťové práva

- Full control – umožní používateľovi čítať, zapisovať a meniť súbory/zložky a tiež meniž prístupové práva a prevziať vlastníctvo zložky/suboru
- Change – používateľ môže čítať, spúšťať, zapisovať a mazať súbory/zložky v rámci zdieľaného priečinka
- Read – umožní používateľovi len prezerať obsah priečnikov a súborov

Vstavané skupiny a špeciálne identity

Vstavané skupiny

- Account Operators – členovia tejto skupiny môžu vytvárať, upravovať a mazať používateľské účty a skupiny v OU okrem administrátorských účtov, nemôžu vytvárať nové OU a reštartovať ani vypínať DC

- Administrators – členovia tejto skupiny majú všetky práva na serveri

Vstavané skupiny

- Backup Operators – členovia tejto skupiny majú práva na zálohovanie a obnovu všetkých súborov a zložiek na serveri bez ohľadu na práva pridelené týmto súborom, môžu vypínať a reštartovať server

- Cert Publishers – skupina počítačov, ktoré slúžia ako firemná certifikačná autorita pre overovanie verejných kľúčov

Vstavané skupiny

- Domain Admins – členovia tejto skupiny môžu spravovať doménový radič a služby Active Directory a môžu meniť členstvo používateľských a počítačových účtov v OU alebo skupinách, majú aj administrátorský prístup na počítače v doméne
- Enterprise Admins – podobne ako Domain admins ale pre celý les
- Domain Computers – jej členom sú všetky počítače v doméne okrem radičov domény

Vstavané skupiny

- Domain Controllers – obsahuje všetky doménové radiče v doméne, pričom sa novovytvorené doménové radiče automaticky pridávajú do tejto skupiny

- Domain Users – táto skupina obsahuje všetky používateľské účty v doméne, pričom sa novovytvorené účty automaticky pridávajú do tejto skupiny

Vstavané skupiny

- Group Policy Creators Owners – členovia tejto skupiny majú práva na vytváranie, úpravu, mazanie a prepájanie GPO
- Network Configuration Operators – členovia tejto skupiny môžu upravovať nastavenia sieťových adaptérov počítača
- Remote Desktop Users – členovia tejto skupiny majú právo pripájať sa na počítač cez vzdialenú plochu

Vstavané skupiny

- Server Operators – členovia tejto skupiny sa môžu pripájať na server, vytvárať, meniť a mazať zdieľané súbory a zložky, spúšťať, zastavovať a reštartovať služby, zálohovať a obnovovať súbory, formátovať disky a vypnúť počítač ale nemôžu meniť členstvá v skupinách, vytvárať účty a pod.

- Print Operators – členovia tejto skupiny majú právo spravovať tlačové fronty na DC a majú tiež právo prihlásiť sa na server lokálne a vypnúť resp. reštartovať počítač

Vstavané skupiny

- DHCP Administrators – členovia tejto skupiny môžu meniť nastavenia DHCP servera
- DHCP Users – používatelia, ktorí majú práva na prezeranie nastavení a stavu DHCP servera
- DNSAdmins – členovia tejto skupiny majú právo meniť nastavenia DNS servera

Špeciálne identity

- Sú to skupiny, ktoré kontroluje operačný systém
- Nie sú viditeľné cez žiadny snap-in (AD U&C)
- Nie je možné meniť ich členov ani ich nemožno pridať ako člena žiadnej inej skupiny
- Môžeme ich použiť na prideľovanie práv a povolení

Špeciálne identity

- Anonymous Logon – reprezentujú prepojenia s počítačom bez zadania prihlasovacích údajov
- Authenticated Users – reprezentujú všetkých prihlásených používateľov v doméne (neobsahuje Guest účet)
- Everyone – Authenticated User + Guests

Špeciálne identity

- Interactive – reprezentujte všetkých používateľov pristupujúcich k zdrojom počítača lokálne (nie cez sieť)

- Network – reprezentuje všetkých používateľov pristupujúcich k zdrojom cez sieť (nie lokálne)

Linky

- http://technet.microsoft.com/en-us/library/cc722455.aspx
- http://technet.microsoft.com/en-us/library/cc755925(v=ws.10).aspx
- http://technet.microsoft.com/en-us/library/bb490712.aspx

- https://www.youtube.com/watch?v=CRQXrA0J4lo&list=PLBBA04BF566F0E0D6&index=25
- https://www.youtube.com/watch?v=aPh8_RB8XEU&list=PLBBA04BF566F0E0D6&index=26
- https://www.youtube.com/watch?v=ERjOx7Kl9bA&list=PLBBA04BF566F0E0D6&index=27
- https://www.youtube.com/watch?v=9jTfkkr5sDE&list=PLBBA04BF566F0E0D6&index=29
- https://www.youtube.com/watch?v=zHHzjjqVhTc&index=31&list=PLBBA04BF566F0E0D6