Macrosoft
Vzdelávanie s trvalým efektom

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava

tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

Administrátor Windows Server - efektívne a bezpečne

Spravujte Windows Server efektívne a bezpečne. Získajte nové uplatnenie na trhu práce ako systémový správca. Školenie je ukončené Certifikátom. V termíne je uvedený len začiatok kurzu, o ďalších termínoch Vás budeme informovať.

MODUL 1: Windows Server - inštalácia a správa systému

- Kurz o Windows Server predstavuje nevyhnutné minimum pre administrátora, správcu serverov či siete. Čaká na Vás veľa praktických úloh na precvičenie, teoretické princípy si vyskúšame v praxi. Každý účastník kurzu má k dispozícií svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Úvod do problematiky, inštalácia

- inštalácia operačného systému Windows server; možnosti licencovania pre konkrétne modely využitia
- inštalácia operačného systému Windows 10 (demonštračný počítač „zamestnanca“, ktorý pridáme do domény)
- inštalácia serverovej úlohy Active Directory Domain Services - vytvorenie firemnej domény spolu s DNS serverom (ukážeme si, prečo je nevyhnutné ho nastaviť pre účely domény)
- práca so Server Manager
- nastavenie času
- práca s konzolou Active Direcotry Users and Computers, získanie prehľadu o jej možnostiach a využití
- pridanie počítača Windows 10 do našej domény
- vytváranie používateľov domény

Pripomenutie si základných znalostí z počítačových sietí

- práca s ovládacím panelom Centrum sietí (Network and Sharing Center)
- nástroje na riešenie sieťových problémov: ping, tracert, ipconfig
- vzdialená správa servera - vzdialená pracovná plocha (Remote Desktop) a jej úskalia

Súborové systémy, disky

- správa diskov: rozdiel medzi basic a dynamic diskami, prehľad druhoch partícií (simple, spanned, mirrored, striped a RAID-5)

Stratégie zdieľania založené na rolách (zdieľané prostriedky a RBAC)

- nastavenie zdieľania, nastavovanie prístupových práv na zdieľaný prostriedok

prehľad vybraných nástrojov pre administrátorov Windows Server z množstva nástrojov

- zálohovanie - možné scenáre a best-practices
- nástroj Windows Server Backup, nastavenie plánovaného zálohovania
- základný prehľad nástrojov a nastavení v ovládacom paneli

Ďalšie využitie Windows Server

- DHCP server, File server, Print server - nastavenie zdieľanej tlačiarne

Úvod do skupinových politík, nastavenie bezpečného hesla v Default Domain Policy

- Každý účastník kurzu používa svoju vlastnú inštaláciu Windows Server a Windows 10 vo virtuálnom prostredí, nemá nič zakázané a má právo si svoje počítače „rozhasiť“ :) ?

MODUL 2: Windows Server - Active Directory - Denné úlohy správcu systému

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava
tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

- Kurz Active Directory - Denné úlohy správcu systému je zameraný na úlohy, ktoré správcovia domén denne vykonávajú na serveroch a klientskych počítačoch. Frekventant získa vedomosti o koncepte Active Directory, vie samostatne zhodnotiť účelnosť jeho použitia v konkrétnom prípade, vie vytvoriť prvý doménový kontroler a bezpečne ho nakonfigurovať. Frekventant je otvorený možnostiam centralizovanej správy množiny výpočtovej techniky využitím nástrojov dostupných v Active Directory a Windows Server, vie pridať používateľa do domény a začleniť ho do skupín podľa jeho pracovného postavenia. Uvedomujúc si dôležitosť svojej profesie dbá na bezpečnú konfiguráciu svojej domény.
- Každý účastník kurzu má k dispozícií svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Systémy prepojenia (zoskupenia) množiny počítačov v miestnej sieti

- Zopakovanie konceptu Workgroup - pracovná skupina systému Windows
- Výhody a obmedzenia pracovnej skupiny, možnosti využitia

Koncept Domény - teória

- Predstavenie konceptu ako nosného bodu centralizovanej správy počítačov, používateľov a nastavení
- Štruktúra domény, strom a les domén
- Protokol LDAP a jeho využitie v doméne a mimo nej
- Scenáre, v ktorých domény nie je vhodný, možné alternatívne riešenia domény, napr. na UNIXe
- Úlohy typu Operation Master - čo ktorá úloha zabezpečuje a ako sledovať, ktorý server ju vykonáva

Active Directory - teória

- Pochopenie konceptu LSA a SAM na platforme Windows v spojení s doménou, odlišnosť tohto konceptu v pracovnej skupine
- Scenáre vhodného použitia
- Pojmy SID, GUID, OU

Práca s Active Directory

- Vytvorenie prvého doménového kontrolera na existujúcej inštalácií Windows Server
- Práca s nástrojom Active Directory Users and Computers
- Koncepty tvorby OUs (organizačné jednotky) s ohľadom na efektívnu správu a škálovateľnosť domény, best practices z praxe, vytváranie OUs v testovacej doméne s ohľadom na dlhodobú udržateľnosť a jednoduchosť ďalšej správy a administrácie
- Objekty v Active Directory - vytváranie počítačov, serverov, pridávanie používateľov - denné úlohy administrátora
- Vlastnosti používateľa domény, nastavenie prvotného hesla, reset hesla, obmedzenie prihlasovania v čase, deaktivovanie používateľa, zistenie členstva a právomocí používateľa, atribúty používateľského konta v doméne
- Rozdiel medzi lokálnym a doménovým používateľským kontom, lokálny vs doménový administrátor
- Nastavenie doménového neprivilegovaného používateľa ako doménového administrátora
- Koncept vlastností objektu (používateľa) ako súčasť schémy domény, možnosti rozšírenia vlastností - atribútov o nové prvky a ich nastavenie v Active Directory
- Rozdiel medzi Skupinou a OU

Nasadzovanie (deploying) active directory v praxi

- Pridávanie počítača do domény
- Pridávanie nového počítača, podmienky pridania nového počítača do domény
- Riešenie problémov s pripojením do domény na strane pracovnej stanice
- pridávanie servera do domény

Riadenie prístupu k sieťovým zdrojom využitím konceptu Active Directory, riadenie prístupu na základe rolí - RBAC

- Typy skupín používateľov a ich právomoci, vstavané skupiny
- Zásady bezpečného používania skupín - stratégie ALP, AGDLP a AGUDLP
- Zásady bezpečného používania skupín v praxi - na zdieľanom sieťovom prostriedku
- Diskusia - ako sa vyhnúť bezpečnostnému riziku v tejto oblasti

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava
tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

Dlhodobá udržateľnosť spravovanej množiny výpočtových zdrojov použitím technológie Active Directory

- Prihlasovacie skripty, písanie jednoduchého skriptu

Skupinové politiky GPO ako mocný nástroj na centralizované nastavenie spravovaných počítačov

- Vysvetlenie pojmu skupinová politika, rozdiel medzi používateľskou a počítačovou politikou
- Politika bezpečnosti používateľských účtov v doméne pomocou Default Domain Policy
- Lokálna politika
- Doménová politika
- Rozdiel medzi lokálnou a doménovou politikou
- Poradie aplikovania a dedičnosť politík
- Stránky a linky

Zistenie aktuálne aplikovaných nastavení skupinovej politiky

- Zistenie aktuálne aplikovaných nastavení na počítač / používateľa
- Zistenie aktuálne aplikovaných nastavení z klientskeho PC a z prostredia Active Directory na Windows Server
- Obnovenie pravidiel skupinovej politiky
- Bezpečnostné opatrenia s využitím Group Policy
- Možnosti využitia Group Policy: presmerovanie priečinkov, automatické pripojenie sieťových jednotiek, upravenie registrov systému Windows
- Cestovný používateľský profil
- Nastavenie skupinovej politiky pre aplikácie tretích strán, napr. internetový prehliadač
- Vypublikovanie tlačiarne

Pokročilé informácie o databáze domény

- Základný prehľad o databáze domény, obnove zmazaných objektov a témy s tým súvisiace

Delegovanie správy Active Directory na dispečing / helpdesk

- Prípadové štúdie, diskusia
- Pridanie delegácie
- Zistenie, kto má právomoci na delegáciu

Diskusia a best practices z praxe

- Vzdialená správa Active Directory bez nutnosti práce na Windows Serveri
- Vzdialená správa Active Directory z počítača, ktorý nie je pripojený v doméne
- Importovanie zoznamu používateľov z iných zdrojov
- Bezpečnosť Active Directory
- Záver kurzu - posolstvo do praxe, záverečné zhrnutie a diskusia

MODUL 3: Windows Server - Bezpečnosť serveru a domény Active Directory

- Kurz o bezpečnosti systému Windows, Windows Server a Active Direcotry prepája teoretické základy z princípov informačnej bezpečnosti do praxe. Precvičíte si široké možnosti bezpečnostných opatrení na konkrétne hrozby. Predstavíme Vám medzinárodné odporúčané systémové nastavenia, ktoré budete v rámci praktických úloh samostatne realizovať na svojich virtuálnych serveroch. V neposlednom rade nás čaká veľa spoločného brainstormingu a diskusií. Tvorivou, pútavou formou si priblížime dôležité aspekty práce bezpečnostného administrátora, ktorý plní azda najzodpovednejšiu úlohu vo firemnej sieti.
- Každý účastník kurzu má k dispozícii svoj vlastný virtuálny počítač - server, ktorý si po skončení môže „odniesť“ domov a ďalej skúmať jeho možnosti.

Terminológia základných pojmov informačnej bezpečnosti a ich prepojenie s opatreniami v praxi

Macrosoft s.r.o.
Štefánikova 47
811 04 Bratislava

tel: 02/ 55 410 308,
0948 88 40 88
e-mail: macrosoft@macrosoft.sk

Riadenie, manažment informačnej bezpečnosti s ohľadom na prostredie Windows, Windows Server a Active Directory

Bezpečnostné mechanizmy systému Windows Server

- diskusia o službách a prvkoch systému Windows, ktoré môžu prestavovať vektory útokov
- bezpečná inštalácia a konfigurácia systému Windows

Základné koncepty bezpečnosti Windows Server

- aktualizácia operačného systému
- aktualizovanie kritických aplikácií
- antivírusová ochrana
- fyzická ochrana servera

Skupinová politika ako nástroj na bezpečné jednotné prostredie

- zásady pri nastavovaní hesiel v doméne
- pravidlá používania a distribúcie hesiel, politika hesiel a zamkýnanie účtov
- lokálna vs doménová skupinová politika
- samostatná aplikácia skupinovej politiky na vlastný server podľa medzinárodných štandardov

Aktualizácie Windows

- diskusia o rizikách spojených s (ne)aktualizovanými systémami
- využitie služby WSUS (software update service), použitie aplikácie WSUS server

Firewall

- základný koncept brány firewall a jej implementácia vo Windows Server
- softvérové a hardvérové riešenia, ich výhody, nevýhody a využitie
- zásady správnej konfigurácie, umiestnenie servera do DMZ

Používateľské účty a skupiny používateľov

- rozdiel medzi doménovým a lokálnym účtom
- typy skupín a ich využitie
- stratégie prideľovania prístupových práv RBAC - skupiny typu ALP, AGDLP, AGUDLP

Prístupové práva k súborom

- zásady bezpečnosti pri zdieľaní súborov
- rozdiel medzi povoleniami pre zdieľané prostriedky a prístupové práva na úrovni súborového systému (NTFS)
- auditovanie prístupu, koncept referenčného monitora ako nástroja na riadenie a auditovanie podľa princípov RBAC

Koncept vzdialenej súkromnej siete - VPN

- možnosti implementácie vzdialenej siete podľa úrovne bezpečnosti
- implementácia PPTP, IPSec, OpenVPN
- scenáre využitia a účelnosti

Záverečné zhrnutie

- diskusia o možných ďalších opatreniach na zvýšenie bezpečnosti lokálnej siete
- záver