kapitola

15

# Auditování událostí zabezpečení Microsoft Windows

**Obsah kapitoly:**



Žádná bezpečnostní strategie nemůže být úplná bez vyčerpávající strategie auditování neboli sledování událostí. Organizace jsou v tomto ohledu velmi často nepoučitelné a často začínají s důkladným auditem až po skutečně závažném bezpečnostním incidentu. Bez auditního záznamu operací, které v systému prováděl vetřelec, je ale úspěšné vyšetřování bezpečnostního incidentu prakticky nemožné. V rámci celkové strategie zabezpečení musíme stanovit, které události budeme auditovat, jaká úroveň auditu bude v daném prostředí nejvhodnější, jak budeme auditované události shromažďovat a jak je kontrolovat. Pro odpovídající auditování a sledování protokolů auditu máme hned několik důvodů:

- Vytvoříme tak srovnávací základnu normálního provozu sítě i počítačů.
- Detekujeme pokusy o prolomení do sítě či počítače.
- V případě bezpečnostního incidentu rychle zjistíme, které systémy a která data byla nebo jsou napadena.

Při pravidelném sledování záznamů či protokolů auditu, zejména pomocí nástrojů automatického sledování událostí, můžeme navíc zmírnit rozsah dalšího poškození sítí a počítačů po případném proniknutí útočníka do sítě.

Konkrétní organizace může podléhat určitým oborovým, vládním nebo zákonným nařízením, která nejenže stanovují rozsah povinného auditu událostí, ale také popisují způsoby zpracování auditních záznamů a délky jejich archivace. Je proto vhodné ověřit u firemních právníků, jestli je navrhovaná strategie auditu v souladu s těmito zákony, normami a předpisy.

# 15.1 Které události budou podléhat auditu

Prvním krokem při vytvoření strategie auditování operačního systému je stanovení typu akcí neboli operací, které budou záznamu podléhat. Které události budeme v operačním systému zaznamenávat? Nejjednodušší odpověď je, zaznamenávat *všechny*. Audit úplně všech událostí operačního systému by ale naneštěstí znamenal také zbytečně velké obsazení systémových prostředků a mohl by mít negativní vliv na výkonnost systému. Pamatujte si, že čím větší rozsah auditu provádíte, tím více událostí je vygenerováno a tím obtížnější je vyhledání kriticky důležitých událostí.

Jestliže budete auditované události sledovat ručně, nebo jestliže neumíte příliš dobře v záznamech auditu číst, může být rozlišení neškodných událostí od škodlivých opravdu hodně obtížné. Rozsah zaznamenávaných událostí v operačním systému budete

proto muset stanovit ve spolupráci s dalšími bezpečnostními specialisty – nejlépe s těmi, kteří se zabývají činnostmi jako forenzní audit, sběr důkazních materiálů nebo vyšetřování počítačového zločinu, a také s pracovníky, kteří mají ve firmě v oblasti IT rozhodovací pravomoci. V rámci auditu zaznamenávejte jen ty události, které budete určitě někdy v budoucnu potřebovat. Toto tvrzení se lehko řekne – i když hodně událostí můžeme charakterizovat skutečně snadno a auditu rozhodně musí podléhat například události správy účtů a události přihlášení.

Pokud v organizaci neexistuje žádná bezpečnostní politika auditu, můžete při stanovení rozsahu auditovaných událostí velice efektivně začít tím, že svoláte všechny zúčastněné osoby do jedné místnosti a vedete skupinovou diskusi neboli brainstorming. V rámci diskuse pak stanovíte:

- Které akce neboli operace budete sledovat.
- Na jakých systémech budete tyto události sledovat.

Například:

- Budeme sledovat všechny události přihlášení do domény a přihlášení k místnímu počítači, a to na všech počítačích.
- Budeme sledovat veškerý přístup ke všem souborům ze mzdové složky na serveru osobního oddělení.

Později je vhodné dát takto stanovená pravidla do souladu se zásadami auditu a konkrétními nastaveními operačního systému.

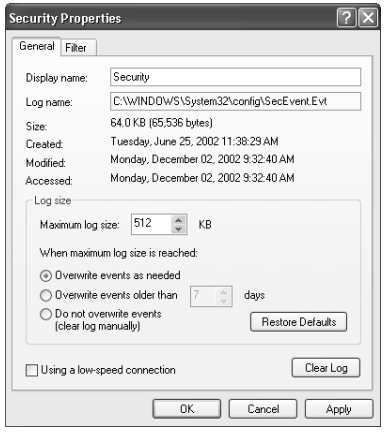
V systémech Microsoft Windows Server 2003, Windows 2000 a Windows XP můžeme události auditu rozdělit do dvou základních kategorií, a sice *úspěšné události* a *neúspěšné události*. Úspěšná událost vyjadřuje úspěšné dokončení dané akce neboli operace v operačním systému, zatímco selhání neboli neúspěšná událost znamená, že pokus o danou akci či operaci skončil neúspěchem. Při sledování pokusů o útoky proti danému prostředí jsou přitom užitečné zejména neúspěšné události, zatímco interpretace událostí úspěchu bývá často obtížná. Drtivá většina úspěšných auditovaných událostí je sice běžným projevem naprosto normální aktivity, ale může se mezi ně dostat také útočník, kterému se podaří úspěšně proniknout do systému. Často jsou přitom důležité nejen události samotné, ale také vzorek neboli posloupnost několika událostí. Několik neúspěšných událostí v řadě, za nimiž následuje úspěšná událost, může například znamenat útok, který po několika nezdařených pokusech vedl k úspěšnému prolomení. Na podezřelé aktivity může poukazovat také jakákoli odchylka od běžného vzorku normálního chování. Dejme tomu, že se například určitý uživatel v naší společnosti podle záznamů auditu přihlašuje do sítě každý pracovní den mezi osmou a desátou hodinou ranní, ale najednou se přihlásí ve tři hodiny ráno. Toto chování může být sice neškodné, ale je natolik neobvyklé, že je velice vhodné případ pečlivě vyšetřit.



# 15.2 Práce s Prohlížečem událostí

Všechny události zabezpečení operačního systému Windows Server 2003, Windows 2000 a Windows XP se zaznamenávají do protokolu Security (Zabezpečení), který se zobrazuje v Event Viewer (Prohlížeč událostí). Další bezpečnostní události se mohou nacházet také v protokolech Applications a System (Aplikace a Systém).

Před zapnutím zásad auditu musíme posoudit, jestli je výchozí konfigurace souborů s protokoly v Event Viewer (Prohlížeč událostí) vhodná také pro prostředí dané konkrétní organizace. Výchozí nastavení protokolu událostí Security (Zabezpečení) vidíme na obrázku 15.1.




**OBRÁZEK 15.1:** Výchozí nastavení protokolu událostí Security

U každého z protokolů událostí tak především musíme stanovit:

- Umístění souboru s protokolem
- Maximální velikost souboru s protokolem
- Chování při přepisování

## Stanovení místa pro ukládání protokolu

Výchozím umístěním protokolu událostí Security (Zabezpečení) je složka `%systemroot%\system32\config\` a soubor s názvem `SecEvent.evt`. Pod systémy Windows Server 2003, Windows 2000 a Windows XP můžeme umístění jednotlivých souborů s protokoly změnit prostřednictvím registru; cesta a název souboru s protokolem Security (Zabezpečení) se nachází v registrační hodnotě `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security`.

Podle výchozího nastavení smí k protokolu událostí Security (Zabezpečení) přistupovat pouze účet System a členové skupiny Administrators, aby se normální uživatelé (kromě správců systému) nedostali ke čtení, zápisu a především odstraňování bezpečnostních událostí. Jestliže soubor s protokolem přesunete do jiného místa, nezapomeňte zkontrolovat, má-li i nový soubor pod souborovým systémem NTFS potřebná oprávnění. Službu záznamu do protokolu Event Log (Protokol událostí) nelze zastavit, a proto se změny v nastaveních protokolu uplatní až po restartu systému.

**Poznámka** Ve Windows Serveru 2003 můžeme změnit oprávnění u protokolů událostí Application a System, avšak nikoli u protokolu Security (Zabezpečení). Podrobné informace o změně přístupových práv k souboru s aplikačním a systémovým protokolem najdete v článku databáze znalostí Microsoft Knowledge Base číslo 323076, „How to Set Event Log Security Locally or by Using Group Policy in Windows Server 2003", na adrese `http://support.microsoft.com/kb/323076`.

## Stanovení maximální velikosti souboru protokolu

Výchozí hodnota maximální velikosti souboru s protokolem událostí Security (Zabezpečení), po jejímž dosažení se spustí chování při přepisování, je pod systémem Windows Server 2003 16 MB a pod Windows 2000 a Windows XP 512 KB. Dnes již máme na počítačích k dispozici podstatně více volného diskového prostoru než dříve, a proto je vhodné tuto prahovou hodnotu zvýšit. Konkrétní cílová hodnota závisí na typu chování při přepisování, ale obecně je dobré uvažovat systémový protokol nejméně o velikosti 50 MB. Vzhledem k architektuře záznamové služby Event Log (Protokol událostí) nesmí celková kumulovaná velikost všech souborů s protokoly událostí překročit 300 MB. Každá bezpečnostní událost zabírá zhruba 350 až 500 bajtů, takže protokol událostí o velikosti 10 MB pojme přibližně 20 000 až 25 000 bezpečnostních událostí.

Maximální velikost souboru s protokolem událostí na jednotlivém počítači změníme buďto v dialogovém okně vlastností protokolu událostí, nebo zásahem do registru. Prostřednictvím Group Policy (Zásady skupiny) a jejích šablon zabezpečení můžeme také změnit maximální velikost souboru s protokolem událostí na několika počítačích současně. Maximální velikost souboru s protokolem událostí Security (Zabezpečení) je uložena v hodnotě registru `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security\MaxSize`.

## Konfigurace chování při přepisování

Při konfiguraci nastavení protokolu událostí Security (Zabezpečení) musíme také stanovit, co se stane po dosažení definované maximální velikosti souboru s protokolem – hovoříme o takzvaném *chování při přepisování*. Ve Windows Serveru 2003, Windows 2000 a Windows XP máme k dispozici celkem tři možná chování:

- **Overwrite events as needed (Přepisovat události podle potřeby).** Nové události se do protokolu budou beze změny zapisovat i po jeho zaplnění. Každá nová událost nahradí nejstarší události v protokolu.
- **Overwrite events older than (Přepisovat události starší než [x] dnů).** Události v protokolu se uchovávají po stanovený počet dní a teprve po jeho uplynutí se smí začít přepisovat. Výchozí hodnota je 7 dní.
- **Do not overwrite events (clear log manually) (Nepřepisovat události – protokol vymazávat ručně).** Nové události se zaznamenávat nebudou a protokol událostí bude nutné vymazat ručně.

Navíc můžeme v konfiguraci operačního systému stanovit, že se při zaplnění protokolu událostí Security (Zabezpečení), kdy do něj nelze zapisovat nové události, zastaví chod systému. V takovém případě znamená zaplnění protokolu chybu se zastavením systému, označovanou jako *modrá obrazovka smrti*, konkrétně s touto zprávou:

```
STOP: C0000244 {Audit Failed}
An attempt to generate a security audit failed
```

Po vzniku této chyby se do systému smí přihlásit pouze členové místní skupiny Administrators, kteří mohou zjišťovat příčiny selhání záznamu do protokolu. Dokud se nepodaří záznam událostí do protokolu obnovit, nemůže počítač pokračovat v normální práci. Toto nastavení je důležité především v prostředích s vysokými ná-

roky na bezpečnost, protože takto se v systému zaručeně zaznamenají všechny bezpečnostní události. Jestliže ale v systému vznikne velké množství bezpečnostních událostí, například z důvodu vstupu útočníka nebo problému v síti, může dojít k situaci s odepřením služeb. Navíc, popisované zastavení chodu serveru může být v rozporu s požadovanou nebo smluvně zajištěnou úrovní dostupnosti služby. Pokud má daná organizace vysoké nároky na bezpečnost i na dostupnost systémů, musíme implementovat vhodnou metodu programového odstraňování starších auditovaných událostí z protokolů.

**Poznámka** Automatické ukončení chodu systému Windows 2000 a novějšího v situaci, kdy nelze zaznamenávat události zabezpečení, je možné konfigurovat pomocí registrační hodnoty `HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\CrashOnAuditFail`, do níž zapíšeme 1.

Jakmile skutečně dojde k ukončení chodu počítače z důvodu nefunkčnosti záznamu do protokolu, změní se uvedená hodnota na 2; člen místní skupiny Administrators musí po přihlášení do systému vrátit hodnotu na 1. Zapíšeme-li do registrační hodnoty 0, bude funkce `CrashOnAuditFail` pro automatické ukončení chodu systému vypnuta.

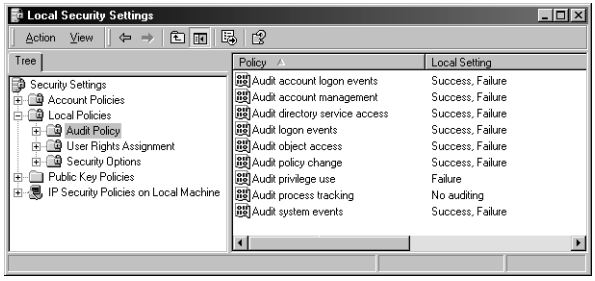
Nemáte-li v síti centralizovaný systém auditu, například Microsoft Operations Manager, musíte pečlivě zvážit, které z nabízených chování pro přepisování se v podmínkách dané organizace hodí nejlépe. Obvykle je nejrozumnější postarat se o dostatečnou velikost protokolu Security (Zabezpečení), který tak pojme všechny potřebné události od jedné archivace do druhé.

# 15.3 Konfigurace zásad auditování

Systémy Microsoft Windows Server 2003, Windows 2000 a Windows XP definují několik kategorií auditu bezpečnostních událostí. Při návrhu konkrétní strategie auditu ve firemní síti se proto musíme rozhodnout, jestli budou auditu podléhat události úspěchu a selhání v následujících kategoriích:

- Account logon events (Události přihlášení k účtu)
- Account management events (Události správy účtu)
- Directory service access (Události přístupu k adresářové službě)
- Logon events (Události přihlášení)
- Object access (Přístup k objektům)
- Policy change (Změny zásad)
- Privilege use (Oprávněné použití)
- Process tracking (Sledování procesů)
- System events (Systémové události)

Aktuální stav auditu v jednotlivých kategoriích zjistíme pod Windows Serverem 2003, Windows 2000 nebo Windows XP z modulu snap-in Local Security Policy (Místní zásady zabezpečení) konzoly MMC (Microsoft Management Console). Na obrázku 15.2 jsou zachycena nastavení zásad auditu pod Windows 2000.




**OBRÁZEK 15.2:** Nastavení zásad auditu v modulu snap-in Local Security Policy konzoly MMC pod Windows 2000

## Auditování událostí přihlášení k účtu

Jestliže se uživatel přihlašuje do domény, zpracuje se jeho žádost o přihlášení v řadiči domény. Pokud zapneme auditování událostí přihlášení k účtu na všech řadičích domény, zaznamenají se pokusy o přihlášení do domény na tom řadiči domény, který provádí ověření účtu. Události přihlášení k účtu se generují v okamžiku ověření zadaných pověření (přihlašovacích údajů) uživatele nebo počítače uvnitř ověřovacího balíku – ať už je toto ověření úspěšné či nikoli. Použije-li se doménové pověření, generují se události přihlášení k účtu jen v protokolech událostí na řadičích domény. Jestliže k ověření předkládáme pověření z místního počítače, zapíší se události přihlášení k účtu do místního protokolu událostí Security (Zabezpečení) přímo na daném serveru nebo pracovní stanici.



**Tip** Protože událost přihlášení k účtu může být zaznamenána na libovolném platném řadiči v doméně, musíte při analýze událostí přihlášení k účtu v doméně sloučit všechny protokoly událostí Security (Zabezpečení) z jednotlivých řadičů domény.

Při definování této zásady můžete stanovit, jestli mají auditu podléhat úspěšné nebo neúspěšné pokusy o přihlášení. Audit úspěšných pokusů znamená, že se událost auditu vygeneruje v okamžiku úspěšného přihlášení, zatímco při auditu neúspěšných pokusů se událost auditu generuje po neúspěšném pokusu o přihlášení.

Z auditu úspěšných pokusů o přihlášení k účtu zjistíme, kdy se uživatelé a počítače úspěšně přihlásili do domény nebo místního počítače. Pokud budeme auditovat také neúspěšné pokusy o přihlášení, můžeme detekovat pokusy o útok s napadením účtu. Detekce stovek nebo i tisíc neúspěšných pokusů o přihlášení k jednomu uživatelskému účtu během několika sekund tak například zcela jasně poukazuje na pokus o prolomení hesla uživatele metodou hrubé síly.

Prozkoumáním úspěšných událostí přihlášení k účtu můžeme zjistit nejen účet, jehož přihlášení se zdařilo nebo nezdařilo (respektive jeho bezpečnostní identifikátor SID), ale také následující informace:

- Název počítače, z něhož byl pokus o přihlášení veden. Útočníci používají v názvech počítačů často *netištitelné znaky*, tedy znaky z rozšířené znakové sady, a tím pádem jsou v Prohlížeči událostí skrytí.
- Doménový nebo počítačový název použitého účtu, z něhož byl na počítači v pracovní skupině útok veden.

- Typ pokusu o přihlášení, kterým může být libovolná z hodnot uvedených v tabulce 15.1.

**TABULKA 15.1:** Typy pokusů o přihlášení

| Typ přihlášení | Název | Popis |
|---|---|---|
| 2 | Interactive | Přihlášení uživatele z Terminálových služeb Windows 2000 nebo přihlášení uživatele fyzicky přítomného u počítače |
| 3 | Network | Obvykle slouží pro přístup k souborům a tiskárnám |
| 4 | Batch | Přihlášení bylo zahájeno z procesu s právy dávkového přihlášení |
| 5 | Service | Přihlášení bylo zahájeno prostřednictvím služby, která má právo Logon as a Service (Přihlásit se jako služba) |
| 6 | Proxy | Tento typ není implementován v žádné verzi operačního systému Windows |
| 7 | Unlock Workstation Logon | Tento typ se zaznamenává v okamžiku odemknutí konzoly počítače |
| 8 | NetworkCleartext | Vyhrazeno pro přihlášení přes síť ve formátu prostého textu |
| 9 | NewCredentials | Přihlášení bylo zahájeno z příkazu RunAs s přepínačem /netonly |
| 10 | RemoteInteractive | Tento typ se zaznamenává při přihlášení Terminálových služeb v systému Windows Server 2003 a Windows XP |
| 11 | CachedInteractive | Tento typ se zaznamenává při místním přihlášení k počítači prostřednictvím pověření uloženého v mezipaměti cache |
| 13 | CachedUnlock | Tento typ se zaznamenává v případě, že byl počítač odemknut a pověření uživatele bylo ověřeno porovnáním s dříve uloženým pověřením v mezipaměti |

- Proces, který přihlášení zahájil; může jím být některý z následujících procesů:
  - **Advapi** Pro volání API funkce LogonUser
  - **Microsoft Internet Information Services (IIS)** Pro přihlášení pod anonymním účtem Anonymous a pro pokusy o přihlášení se základním ověřením nebo s ověřením otisku (digest)
  - **LAN Manager Workstation Service** Pro pokusy o přihlášení protokolem LAN Manager (LM)
  - **Kerberos** Pro volání z poskytovatele Kerberos Security Support Provider (SSP)
  - **KsecDD** Pro síťová připojení
  - **MS.RADIU** Pro pokusy o přihlášení, vedené z ověřovací služby Microsoft Internet Authentication Service (IAS)

  - **NT LAN Manager (NTLM) nebo NTLM Security Support Provider (NtLmSsp)** Pro pokusy o přihlášení v protokolu NTLM
  - **Service Control Manager (SCMgr)** Pro přihlášení pod účtem služby
  - **Seclogon** Pro pokusy o přihlášení s příkazem RunAs
  - **User32 nebo WinLogon\MSGina** Pro pokusy o interaktivní přihlášení
- Ověřovací balík, jehož prostřednictvím se ověřuje pokus o přihlášení; platné hodnoty jsou:
  - Kerberos
  - Negotiate
  - NTLM
  - Microsoft_Authentication_Package_v10
- IP adresa a zdrojový port pokusu o přihlášení – pouze v systému Windows Server 2003

Vždy nezapomeňte zaznamenávat v rámci auditu jak úspěšné, tak i neúspěšné pokusy o přihlášení do systému. Události úspěšného přihlášení jsou velmi důležité pro sestavení srovnávací základny běžného chování uživatelů a mohou být podstatné i při vyšetřování bezpečnostních incidentů. Neúspěšné události pak mohou být projevem pokusu útočníka o proniknutí do sítě. Včasným (proaktivním) sledováním neúspěšných událostí můžeme zabránit i útokům s rozsáhlými škodlivými následky v síti. Nejběžnější události přihlášení k účtu jsou shrnuty v tabulce 15.2.



**TABULKA 15.2:** Nejběžnější události přihlášení k účtu

| ID události | Popis |
|---|---|
| 672 | Lístek ověřovací služby Authentication Service byl úspěšně vydán a ověřen. |
| 673 | Lístek služby Ticket Granting Service byl udělen. |
| 674 | Nositel zabezpečení (principal) obnovil lístek ověřovací služby Authentication Service nebo lístek služby Ticket Granting Service. |
| 675 | Předběžné ověření v protokolu Kerberos selhalo. |
| 676 | Žádost o ověřovací lístek selhala. Tato událost není ve Windows XP ani ve Windows Serveru 2003 implementována. |
| 677 | Lístek služby Ticket Granting Service nebyl udělen. Tato událost není ve Windows XP ani ve Windows Serveru 2003 implementována. |
| 678 | Účet byl úspěšně mapován na doménový účet. |
| 679 | Mapování účtu na doménový účet selhalo. |
| 680 | Byl identifikován účet použitý při úspěšném pokusu o přihlášení. Tato událost současně vyznačuje, pomocí kterého ověřovacího balíku byl účet ověřen. |
| 681 | Neúspěšný pokus o přihlášení k doménovému účtu. Tato událost není ve Windows XP ani ve Windows Serveru 2003 implementována a zaznamenává se místo ní událost 672. |
| 682 | Uživatel se znovu připojil k odpojené relaci terminálových služeb. |
| 683 | Uživatel se odpojil z relace terminálových služeb. |

Při selhání pokusu o přihlášení pod Windows 2000 se navíc zaznamenává událost s ID 681, která zároveň obsahuje dekadický kód s důvodem selhání. Přehled kódů selhání v dekadickém a hexadecimálním formátu spolu s textovým popisem uvádí tabulka 15.3.

**TABULKA 15.3:** Kódy důvodů selhání u události ID 681

| Dekadická hodnota | Hexadecimální hodnota | Důvod |
|---|---|---|
| 3221225572 | C0000064 | Uživatel zadal při přihlášení nesprávně zapsané nebo chybné jméno uživatelského účtu. |
| 3221225578 | C000006A | Uživatel zadal při přihlášení nesprávně zapsané nebo chybné heslo. |
| 3221225583 | C000006F | Uživatel se pokoušel přihlásit mimo povolené hodiny. |
| 3221225584 | C0000070 | Uživatel se pokoušel přihlásit z nepovolené pracovní stanice. |
| 3221225585 | C0000071 | Uživatel se pokoušel přihlásit s heslem, jehož platnost vypršela. |
| 3221225586 | C0000072 | Uživatel se pokoušel přihlásit na účet, který byl správcem zablokován. |
| 3221225875 | C0000193 | Uživatel se pokoušel přihlásit k účtu, jehož platnost vypršela. |
| 3221226020 | C0000224 | Uživatel se pokoušel přihlásit za platnosti příznaku Change Password At Next Logon (Při dalším přihlášení musí uživatel změnit heslo). |
| 3221226036 | C0000234 | Uživatel se pokoušel přihlásit pod uzamknutý účet. |

## Auditování událostí správy účtu

Každý, kdo má přístup k účtu pro správu systému, má také oprávnění udělovat jiným účtům zvýšená práva a oprávnění v systému a může vytvářet nové účty, a proto je nedílnou součástí každého návrhu a implementace síťové bezpečnosti také auditování událostí správy účtu. Bez vyspělých biometrických či jiných opatření špičkového zabezpečení je dosti obtížné nebo dokonce úplně nemožné zaručit, že pod daným účtem skutečně pracuje ta osoba, které bylo právo k jeho používání vydáno. Auditování je mimo jiné jedním ze způsobů, jak správcům systému přiřadit a prokázat odpovědnost za provedené operace.

Zapnutí auditu událostí správy účtu umožňuje záznam následujících událostí:

- Vytvoření, změna nebo odstranění uživatelského účtu či skupiny
- Přejmenování, zablokování nebo odblokování uživatelského účtu
- Nastavení nebo změna hesla k účtu
- Změna zásad zabezpečení daného počítače

Změny uživatelských práv se sice na první pohled projevují jako události správy účtů, ale ve skutečnosti se jedná o události změny zásad. Pokud budou obě tyto zásady auditu vypnuté, může zlomyslný správce rozvrátit bezpečnost celé sítě, aniž by v auditu systému zanechal jakoukoli stopu. Jestliže například správce přiřadí uživatelský účet Sally za člena skupiny Backup Operators, zaznamená se událost

správy účtu. Pokud ale stejný správce systému uživateli Sally přímo udělí rozšířené právo Back Up Files And Folders, událost správy účtů se již nezaznamená. Pod auditováním správy účtů se zaznamenávají také změny zásad zabezpečení počítače; neočekávané změny těchto zásad mohou být předzvěstí možného napadení systému nebo zničení dat. Takto se například útočníkovi může podařit oslabení bezpečnosti systému počítače, zablokovat na něm určitý prostředek, a poté proti němu následně povede vhodný útok.

U událostí správy účtů je opět vhodné auditovat jak úspěšné, tak neúspěšné pokusy. Audit úspěšného pokusu znamená záznam úspěšného dokončení operace správy účtu, zatímco audit neúspěšných pokusů znamená záznam selhání těchto pokusů. Úspěšné pokusy o provedení operace správy účtu jsou sice v drtivé většině případů naprosto neškodné, ale v případě napadení sítě znamenají přímo nedocenitelný zdroj informací o proběhlých aktivitách. Při útoku zde například vidíme, které účty si útočník vytvořil jako nové a které pozměnil. Neúspěšné události (selhání) správy účtů představují často pokus správce systému na nižší úrovni o posílení svých oprávnění (nebo také stejný pokus útočníka, kterému se podařilo účet nižšího správce napadnout). Takto se například může stát, že se účet služby Backup pokusí sám sobě nebo jinému účtu udělit členství ve skupině správců domény. Sledování událostí správy účtů je proto opravdu kriticky důležité. Nejběžnější události správy účtů shrnuje tabulka 15.4.



**TABULKA 15.4:** Nejběžnější události správy účtů

| ID události | Popis |
|---|---|
| 624 | Vytvoření uživatelského účtu. |
| 627 | Pokus o změnu hesla; tato událost se zaznamenává při úspěšném i neúspěšném pokusu o změnu hesla. |
| 632 | Přidání nového člena globální skupiny. |
| 633 | Odebrání člena globální skupiny. |
| 634 | Odstranění celé globální skupiny. |
| 635 | Vytvoření místní skupiny (distribuční). |
| 636 | Přidání nového člena místní skupiny zabezpečení. |
| 637 | Odebrání člena místní skupiny. |
| 638 | Odstranění místní skupiny. |
| 639 | Změna místní skupiny. |
| 641 | Změna globální skupiny. |
| 642 | Změna uživatelského účtu. |
| 643 | Změna doménových zásad. |
| 644 | Uživatelský účet byl zablokován. Na primárním řadiči domény (PDC), který emuluje činnost hlavního operačního serveru, se při zablokování (uzamčení) účtu zaznamenají dvě události, a sice událost 644, která vyjadřuje jméno uzamčeného účtu, a dále událost 642, která vyjadřuje vlastní uzamčení. Událost se zaznamenává pouze na emulátoru primárního řadiče domény (PDC). |

| ID události | Popis |
|---|---|
| 645 | Vytvoření účtu počítače. |
| 646 | Změna účtu počítače. |
| 647 | Odstranění účtu počítače. |
| 648 | Vytvoření místní skupiny se zabezpečením (distribuční). |
| 649 | Změna místní skupiny se zabezpečením (distribuční). |
| 650 | Do místní skupiny se zabezpečením (distribuční) byl přidán nový člen. |
| 651 | Z místní skupiny se zabezpečením (distribuční) byl odebrán člen. |
| 652 | Odstranění místní skupiny (distribuční). |
| 653 | Vytvoření globální skupiny (distribuční). |
| 654 | Změna globální skupiny (distribuční). |
| 655 | Přidání nového člena do globální skupiny (distribuční). |
| 656 | Odebrání člena z globální skupiny (distribuční). |
| 657 | Odstranění distribuční globální skupiny. |
| 658 | Vytvoření univerzální skupiny se zabezpečením. |
| 659 | Změna univerzální skupiny se zabezpečením. |
| 660 | Přidání nového člena do univerzální skupiny se zabezpečením. |
| 661 | Odebrání člena z univerzální skupiny se zabezpečením. |
| 662 | Odstranění univerzální skupiny se zabezpečením. |
| 663 | Vytvoření distribuční univerzální skupiny. |
| 664 | Změna distribuční univerzální skupiny. |
| 665 | Přidání nového člena do distribuční univerzální skupiny. |
| 666 | Odebrání člena z distribuční univerzální skupiny. |
| 667 | Odstranění distribuční univerzální skupiny. |
| 668 | Změna typu skupiny. |
| 684 | Nastavení popisovače zabezpečení členů skupin pro správu. Ve všech řadičích domény běží na pozadí podproces, který každých 60 minut prohledá členy všech skupin pro správu, včetně správců domény, rozlehlé sítě a schématu, a znovu na ně aplikuje popisovač zabezpečení. Tato událost se zaznamenává v každém okamžiku inicializace přístupového seznamu (ACL). |
| 685 | Změna jména účtu. |

## Auditování událostí přístupu k adresářové službě

Zapneme-li auditování adresářové služby, můžeme sledovat změny provedené ve službě Active Directory. Změny v objektech účtů uživatelů, počítačů a skupin sledujeme sice již při zapnutí auditu událostí správy účtů, ale někdy je vhodné sledovat také změny jiných objektů a atributů služby Active Directory, například změny součástí infrastruktury Active Directory, jako jsou objekty sítí, a změny schématu služby Active Directory. Další množinou objektů, které se běžně sledují v rámci au-

ditu služby Active Directory, jsou objekty certifikačních úřadů (CÚ) rozlehlé sítě, uložené do konfiguračního kontejneru při instalaci infrastruktury veřejného klíče (Public Key Infrastructure, PKI) v rozlehlé síti pod Windows Serverem 2003 nebo pod Windows 2000.

Pro správný audit úspěšných a neúspěšných pokusů o změny objektů a atributů služby Active Directory musíme nejen zapnout auditování adresářových služeb na všech řadičích domény, ale také musíme pro všechny auditované objekty či atributy definovat příslušný systémový přístupový seznam (SACL). Kromě záznamu změn v objektech a atributech služby Active Directory se v rámci auditování adresářové služby provádí také záznam událostí služby Active Directory jako je replikace. Z toho vyplývá, že při zapnutí auditu úspěšných událostí přístupu k adresářové službě se výrazně zvýší počet událostí zaznamenávaných do protokolu Security (Zabezpečení); kromě zvýšení velikosti souboru to ale znamená, že jakékoli hledání smysluplných událostí bez vyspělých analytických nástrojů bude velmi obtížné.

Jestliže zapneme toto nastavení zásad, můžeme opět určit, jestli mají auditu podléhat úspěšné nebo neúspěšné události. Audit úspěšných událostí znamená záznam úspěšného přístupu uživatelů k objektům služby Active Directory, které mají definovaný přístupový seznam SACL. Audit neúspěšných událostí pak znamená záznam neúspěšného přístupu k těmto objektům.



**Tip** Služba Active Directory představuje databázi s několika hlavními servery, takže její změny mohou být zapsány na libovolném z řadičů domény. Požadovaný audit přístupu k adresářové službě musíme proto zapnout na všech řadičích domény současně. K tomu je nejlépe vytvořit na úrovni domény příslušný objekt Group Policy (Zásady skupiny) (GPO) se zásadou auditu.

Všechny události přístupu k adresářové službě, a to jak úspěšné, tak i neúspěšné, mají v protokolu událostí Security (Zabezpečení) definován ID události 565 nebo 566. Přesný výsledek konkrétní události (včetně jejího úspěchu či neúspěchu) je možné zjistit pouze bližším zkoumáním této události 565 nebo 566.

## Auditování událostí přihlášení

Při zapnutém auditu událostí přihlášení se budou zaznamenávat všechny události přihlášení a odhlášení uživatele od počítače. Tato událost se zaznamenává vždy do protokolu událostí Security (Zabezpečení) na tom počítači, kde se uživatel pokoušel přihlásit. Podobně pokud se uživatel nebo počítač pokusí o připojení ke vzdálenému počítači, vygeneruje se událost síťového přihlášení v protokolu událostí Security (Zabezpečení) na tomto vzdáleném počítači. Události přihlášení se vytvářejí v okamžiku vytvoření a zrušení přihlašovací relace a tokenu.

**Poznámka** Pod Windows 2000 se přihlášení přes Terminálové služby považuje za interaktivní přihlášení, a proto se při vzdáleném vytvoření relace terminálového serveru zaznamená událost přihlášení. Pokud je záznam událostí přihlášení zapnutý na počítači, kde běží terminálové služby, musíme rozlišit mezi přihlášením z konzoly a přihlášením k terminálové službě. V systémech Windows Server 2003 a Windows XP je již přihlášení přes terminálovou službu od interaktivního přihlášení oddělené.

V rámci auditu událostí přihlášení se zaznamenávají pokusy o přihlášení všech uživatelů i všech počítačů. Při pokusu o přihlášení po síťovém spojení z počítače se systémem Windows Server 2003, Windows 2000 nebo Windows XP se do protokolu zaznamenají události přihlášení účtu počítače i uživatelského účtu.

**Poznámka** Pokud se do domény přihlásí uživatel z počítače, kde běží systém Microsoft Windows 95 nebo Windows 98, zaznamená se pouze událost přihlášení uživatelského účtu. Počítače se systémy Windows 95 a Windows 98 nemají v adresářové službě definován účet počítače a při přihlášení ze sítě se u nich tudíž negeneruje událost přihlášení počítače.

Události přihlášení k účtu jsou užitečné nejen pro sledování pokusů o interaktivní přihlášení k serverům, ale také při šetření útoků vedených z určitého počítače. V rámci auditu úspěšných událostí se zaznamenávají pokusy, které skončily úspěšným přihlášením, zatímco v rámci neúspěšného auditu se sledují případy selhání pokusu o přihlášení.

Mezi auditem událostí přihlášení a událostí přihlášení k účtu je jeden drobný, ale velice důležitý rozdíl. Události přihlášení k účtu se zaznamenávají na tom počítači, jenž daný účet ověřil (autentizoval jej), zatímco události přihlášení se zaznamenávají na tom počítači, kde se účet bude používat. Pokud se například uživatel přihlásí do sítě ze svého počítače, který je součástí domény, a to prostřednictvím svého doménového účtu, zaznamená se událost přihlášení k účtu na tom řadiči, který provedl ověření účtu, zatímco událost přihlášení se zaznamená na počítači, přes který se uživatel do sítě přihlásil.

Na řadičích domény se zapnutým auditem událostí přihlášení se události přihlášení generují jen při pokusech o interaktivní a síťové přihlášení k samotnému řadiči domény – pokusy o přihlášení počítače se v rámci auditu nezaznamenávají. Při auditu úspěšných událostí se zaznamenávají pokusy, které skončily úspěšným přihlášením, zatímco v rámci neúspěšného auditu se sledují případy selhání pokusu o přihlášení.

V systému je vhodné zapnout vždy záznam úspěšných i neúspěšných pokusů o přihlášení. Úspěšné pokusy o přihlášení tvoří srovnávací základnu běžného chování uživatelů při přihlašování, podle níž můžeme následně rozpoznat podezřelé chování. Záznam úspěšných pokusů o přihlášení je důležitý také při každém šetření incidentu. Pokud budeme v organizaci sledovat i neúspěšné pokusy o přihlášení, můžeme včas proaktivně reagovat na jakékoli podezřelé chování a tím zabránit dalším síťovým útokům a dalšímu poškození sítě. Dejme tomu, že si například v týdenním přehledu auditovaných protokolů na serveru všimneme množství neúspěšných pokusů o přihlášení pod různými uživatelskými účty. Bližším šetřením zjistíme, že ačkoliv je server umístěn ve fyzicky dobře zabezpečené místnosti, probíhaly tyto pokusy o přihlášení přímo z jeho konzoly. Na toto podezřelé chování můžeme včas reagovat, zabránit poškozování uložených informací a začít také s vyšetřováním možného napadení fyzické bezpečnosti systému. Popis nejběžnějších událostí přihlášení je uveden v tabulce 15.5.

**TABULKA 15.5:** Nejběžnější události přihlášení

| ID události | Popis |
|---|---|
| 528 | Uživatel se úspěšně přihlásil k počítači. |
| 529 | Byl proveden pokus o přihlášení pod neznámým uživatelským jménem, nebo pod známým uživatelským jménem, ale s nesprávným heslem. |
| 530 | Uživatel se pokoušel přihlásit mimo povolené hodiny. |
| 531 | Uživatel se pokoušel přihlásit pod uzamknutý účet. |
| 532 | Uživatel se pokoušel přihlásit k účtu, jehož platnost vypršela. |
| 533 | Tento uživatel nemá povoleno přihlášení k tomuto počítači. |
| 534 | Uživatel se pokusil o přihlášení pod nedovoleným typem přihlášení, jako je například síťové přihlášení, interaktivní přihlášení, dávka, služba nebo vzdálené interaktivní přihlášení. |
| 535 | Platnost hesla k danému účtu vypršela. |
| 536 | Služba Netlogon není aktivní. |
| 537 | Pokus o přihlášení selhal z jiného důvodu. |
| 538 | Uživatel se odhlásil ze systému. |
| 539 | Účet byl v okamžiku pokusu o přihlášení uzamknutý. Tato událost se zaznamenává v případě, že se uživatel nebo počítač pokouší o ověření pod účtem, který byl dříve uzamknut. |
| 540 | Úspěšné síťové přihlášení. |
| 682 | Uživatel se znovu připojil k odpojené relaci terminálových služeb. |
| 683 | Uživatel se odpojil z relace terminálových služeb bez řádného odhlášení. |



## Auditování přístupu k objektům

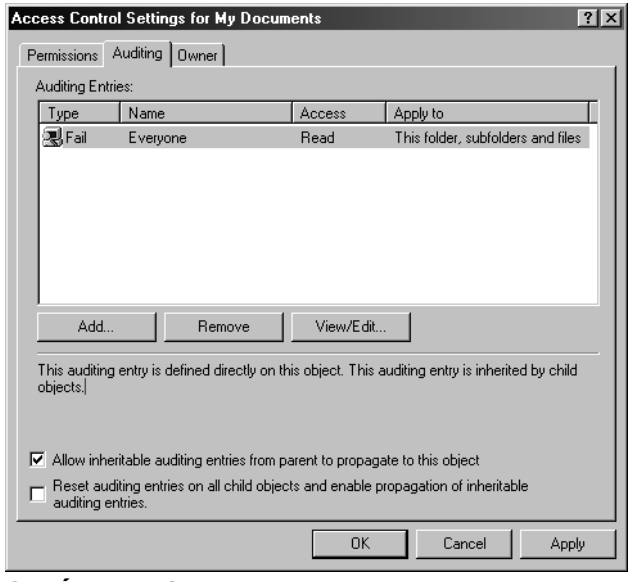
Auditování přístupu k objektům znamená sledování úspěšných a neúspěšných pokusů o přístup k prostředkům, tedy k souborům, tiskárnám a registru. Podobně jako u auditu adresářových služeb musíme přitom i při auditu objektů konfigurovat u každého sledovaného objektu příslušný systémový přístupový seznam SACL. Zapnutí auditu přístupu k souboru pod Windows XP je zachyceno na obrázku 15.3.

Systémový přístupový seznam (SACL) se skládá z položek řízení přístupu ACE. Každá takováto položka pak obsahuje tři informace:

- Auditovaný nositel zabezpečení (principal), tedy uživatel, počítač nebo skupina.
- Konkrétní typ auditovaného přístupu neboli *přístupová maska*.
- Příznak, jestli mají auditu podléhat neúspěšné události přístupu, úspěšný přístup, nebo obojí.

Zapínat audit přístupu k objektům a vytvářet nad danými prostředky (tedy soubory, klíči registru a tiskárnami) vhodné přístupové seznamy SACL má smysl jen v případě, že má daná organizace pro záznam pokusů o přístup k těmto prostředkům konkrétní věcné důvody. Při konfiguraci auditování souborů je třeba předem zvážit, jakých operací se bude audit týkat. Běžné otevření textového souboru, změna jediného řádku a opětovné uložení souboru znamená například pod Windows XP

více než 30 událostí, zapsaných do protokolu Security (Zabezpečení). (Tento počet platí v případě, že se u souboru rozhodneme pro audit úplného řízení.)




**OBRÁZEK 15.3:** Konfigurace auditu přístupu k souboru pod Windows XP

**Tip** Dávejte pozor také při auditu oprávnění Read & Execute nad spustitelnými soubory, protože tento typ auditu vyvolá záznam velkého množství událostí. Také kontrola souborového systému v antivirovém softwaru generuje při auditu Full Control tisíce událostí přístupu k souborům.

Při konfiguraci přístupových seznamů SACL je vhodné se omezit jen na ty operace, které skutečně potřebujeme sledovat. Nad spustitelnými soubory má například smysl zapnout audit událostí Write and Append Data a sledovat tak události případného nahrazení či změn souborů, způsobených mimo jiné počítačovými viry, červy a trojskými koňmi. Podobně je vhodné sledovat třeba změny v citlivých dokumentech nebo i jakýkoli přístup k nim (včetně pouhého čtení).

**Tip** Před zapnutím auditu souborů, klíčů registru a tiskáren si ověřte, jestli audit požadovaného prostředku nepovede ke zpomalení činnosti serveru nebo k takovému zhoršení výkonnosti prostředku, které by mohlo znamenat narušení běžné činnosti firmy.

V rámci auditu přístupu k objektům lze sledovat úspěšné i neúspěšné pokusy o přístup k souborům, složkám, klíčům registru a tiskárnám. Audit úspěšných událostí obsahuje záznam úspěšných přístupů uživatele k objektu s definovaným přístupovým seznamem SACL; audit neúspěšných událostí znamená záznam neúspěšných pokusů o přístup. Nejobvyklejší události přístupu k objektům shrnuje tabulka 15.6.

**TABULKA 15.6:** Běžné události přístupu k objektům

| ID události | Popis |
|---|---|
| 560 | Udělení přístupu k již existujícímu objektu. |
| 561 | Byl alokován popisovač objektu. |
| 562 | Byl uzavřen popisovač objektu. |
| 563 | Pokus o otevření objektu s cílem jeho odstranění. |
| 564 | Odstranění chráněného objektu. |
| 565 | Udělení přístupu k již existujícímu typu objektu. |
| 567 | Bylo použito oprávnění spojené s daným popisovačem.<br>Poznámka: Při vytvoření popisovače jsou v něm udělena určitá oprávnění (Read, Write a další). Jakmile tento popisovač použijeme, může použití každého z oprávnění vygenerovat jednu událost auditu. |
| 568 | Pokus o vytvoření pevného odkazu na auditovaný soubor. |
| 569 | Správce prostředků v Authorization Manageru se pokusil o vytvoření kontextu klienta. |
| 570 | Klient se pokusil o přístup k objektu.<br>Poznámka: Pro každý pokus o operaci nad objektem je generována samostatná událost auditu. |
| 571 | Aplikace Authorization Manageru odstranila kontext klienta. |
| 572 | Authorization Manager provedl inicializaci aplikace. |
| 772 | Certificate Manager (Správce certifikátů) odepřel nevyřízenou žádost o certifikát. |
| 773 | Služba Certificate Services (Certifikační služba) přijala znovu podanou žádost o certifikát. |
| 774 | Služba Certificate Services odvolala certifikát. |
| 775 | Služba Certificate Services přijala žádost o publikování seznamu odvolaných certifikátů (CRL). |
| 776 | Služba Certificate Services publikovala seznam odvolaných certifikátů (CRL). |
| 777 | Bylo provedeno rozšíření žádosti o certifikát. |
| 778 | Byl změněn jeden nebo více atributů žádosti o certifikát. |
| 779 | Služba Certificate Services přijala žádost o ukončení chodu. |
| 780 | Spuštění operace zálohování služby Certificate Services. |
| 781 | Dokončení operace zálohování služby Certificate Services. |
| 782 | Spuštění operace obnovení služby Certificate Services. |
| 783 | Dokončení operace obnovení služby Certificate Services. |
| 784 | Spuštění služby Certificate Services. |
| 785 | Zastavení služby Certificate Services. |
| 786 | Změna bezpečnostních oprávnění služby Certificate Services. |
| 787 | Služba Certificate Services přijala archivovaný klíč. |

| ID události | Popis |
|---|---|
| 788 | Služba Certificate Services importovala certifikát do své databáze. |
| 789 | Změna filtru auditování pro službu Certificate Services. |
| 790 | Služba Certificate Services přijala žádost o certifikát. |
| 791 | Služba Certificate Services schválila žádost o certifikát a vydala certifikát. |
| 792 | Služba Certificate Services odepřela žádost o certifikát. |
| 793 | Služba Certificate Services nastavila u žádosti o certifikát nevyřízený stav. |
| 794 | Změnila se nastavení Certificate Manageru pro službu Certificate Services. |
| 795 | Změna konfigurační položky ve službě Certificate Services. |
| 796 | Změna vlastnosti služby Certificate Services. |
| 797 | Služba Certificate Services provedla archivaci klíče. |
| 798 | Služba Certificate Services provedla import archivovaného klíče. |
| 799 | Služba Certificate Services publikovala certifikát certifikačního úřadu (CÚ) do služby Active Directory. |
| 800 | Z certifikační databáze byl odstraněn jeden nebo více řádků. |
| 801 | Bylo zapnuto oddělení rolí. |

Událost s číslem 772 až 801 je možné vygenerovat jen na počítači, kde běží operační systém Windows Server 2003 a služby Certificate Services.

## Auditování změny zásad

Pomocí auditování změn zásad lze sledovat změny v následujících třech oblastech:

- User Rights Assignment (Přiřazování uživatelských práv)
- Audit Policy (Zásady auditu)
- Trusted Domains (Vztahy důvěryhodnosti mezi doménami)

Z označení *auditování změn zásad* by sice vyplývalo, že se tato událost zaznamenává se změnou zásad zabezpečení počítačů, ale ve skutečnosti se zapisuje do protokolu při povolení auditu správy účtů, a to s ID události 643. Pokud je zapnuté auditování změn zásad, zaznamenávají se také změny přiřazení uživatelských práv. Útočník může přitom při pokusu o napadení systému povýšit svoje oprávnění, nebo oprávnění jiného účtu – může si například přidat oprávnění Debug nebo oprávnění Back Up Files And Folders. Součástí auditu změn zásad jsou také pokusy o změny samotných zásad auditu a změny ve vztazích důvěryhodnosti.

Opět je vhodné zapnout audit jak úspěšných, tak neúspěšných pokusů o změny zásad a sledovat tak veškeré udělování a odebírání uživatelských práv i změn zásad auditu. Záznam úspěšných i neúspěšných pokusů znamená audit pokusů o změny zásad zabezpečení, zásad přiřazování uživatelských práv a zásad důvěryhodnosti. Popis nejběžnějších událostí změny zásad je uveden v tabulce 15.7.

**TABULKA 15.7:** Nejběžnější události změny zásad

| ID události | Popis |
|---|---|
| 608 | Uživatelské právo bylo přiřazeno. |
| 609 | Uživatelské právo bylo odebráno. |
| 610 | Byl vytvořen vztah důvěryhodnosti s jinou doménou. |
| 611 | Vztah důvěryhodnosti s jinou doménou byl odstraněn. |
| 612 | Provedena změna zásad auditu. |
| 613 | Spuštěn agent zásad protokolu IPSec (Internet Protocol Security). |
| 614 | Zablokování agenta zásad IPSec. |
| 615 | Změna agenta zásad IPSec. |
| 616 | Agent zásad IPSec narazil na potenciálně závažnou chybu. |
| 617 | Změna zásad modulu Kerberos verze 5. |
| 618 | Změna zásad obnovení dat (Encrypted Data Recovery). |
| 620 | Proběhla změna vztahu důvěryhodnosti s jinou doménou. |
| 621 | Účtu bylo uděleno právo přístupu k systému. |
| 622 | Účtu bylo odebráno právo přístupu k systému. |
| 623 | Nastavení zásad auditu pro jednotlivého uživatele. |
| 625 | Obnovení zásad auditu pro jednotlivého uživatele. |
| 671 | Změna nebo obnovení zásad zabezpečení (dvě pomlčky v poli Changes Made znamenají, že během obnovení nebyly provedeny žádné změny). |
| 768 | Detekována kolize mezi prvkem názvového prostoru v jedné doménové struktuře (lese) a prvkem názvového prostoru v jiné doménové struktuře. |
| 769 | Byla přidána informace o důvěryhodné doménové struktuře (lesu). |
| 770 | Byla odstraněna informace o důvěryhodné doménové struktuře. |
| 771 | Byla změněna informace o důvěryhodné doménové struktuře. |
| 805 | Služba Event Log přečetla konfiguraci protokolu Security pro danou relaci. |



## Auditování používání oprávnění

Povolíme-li audit používání oprávnění, můžeme zaznamenávat případy, kdy uživatelé a služby použijí pro výkon své práce určitá uživatelská práva, pouze s výjimkou několika uživatelských práv, která auditu nepodléhají. Zmíněné výjimky tvoří tato uživatelská práva:

- Bypass Traverse Checking (Obejít křížovou kontrolu)
- Debug Programs (Ladit programy)
- Create A Token Object (Vytvořit objekt tokenu)
- Replace Process Level Token (Nahradit token úrovní procesu)
- Generate Security Audits (Generovat audity bezpečnosti)
- Back Up Files And Directories (Zálohovat soubory a adresáře)

- Restore Files And Directories (Obnovit soubory a adresáře)

Pod systémy Windows Server 2003, Windows 2000 a Windows XP se v Group Policy (Zásady skupiny) pod Security Options (Možnosti zabezpečení) nachází nastavení označené Audit Use Of Backup And Restore Privilege (Auditovat použití oprávnění zálohovat a obnovovat soubory), které umožňuje sledovat užití oprávnění Back Up And Restore Files And Folders.

Pomocí auditu používání oprávnění můžeme detekovat události spojené s mnoha různými útoky. Mezi tyto události patří:

- Ukončení chodu místního nebo vzdáleného systému
- Zavedení nebo odstranění ovladačů zařízení
- Prohlížení protokolu událostí Security (Zabezpečení)
- Přebírání vlastnictví k objektům
- Jednání jako součást operačního systému

U používání oprávnění (uživatelských práv) je vhodné zapnout přinejmenším záznam neúspěšných pokusů, které obvykle naznačují problémy v síti a často mohou být známkou pokusu o prolomení bezpečnosti systému. Audit úspěšného použití uživatelských práv je vhodné zapínat jen tehdy, pokud k tomu máme skutečný věcný důvod. Úspěšné události znamenají auditní záznam každého úspěšného použití uživatelských práv, zatímco při neúspěšných událostech podléhá auditu jejich selhání. Nejběžnější události použití oprávnění shrnuje tabulka 15.8.

**TABULKA 15.8:** Události použití oprávnění

| ID události | Popis |
|---|---|
| 576 | Do přístupového tokenu uživatele byla přidána požadovaná oprávnění. (Tato událost se generuje v okamžiku přihlášení uživatele.) |
| 577 | Uživatel se pokusil o provedení privilegované činnosti systémové služby. |
| 578 | Použití oprávnění nad již otevřeným popisovačem chráněného objektu. |

## Auditování sledování procesů

Výsledkem auditu sledování procesů je podrobný záznam provádění procesů, tedy události jako aktivace programu, ukončení procesu, zdvojení popisovače a nepřímý přístup k objektům. Sledování procesu generuje přinejmenším událost aktivace a ukončení každého procesu; po zapnutí auditu úspěšných událostí se proto do protokolu událostí Security (Zabezpečení) zapisuje velký objem dat.

Zapnutí auditu sledování procesů je vynikající při řešení problémů a při zjišťování podrobné činnosti aplikací; tento audit ale rozhodně zapínejte jen tehdy, pokud k němu máte skutečně pádný důvod. Protokoly Security (Zabezpečení) se zapnutým auditem sledování procesů je také vhodné analyzovat pomocí příslušného automatického nástroje. Při záznamu úspěšných událostí se zapisuje úspěšné sledování procesů, zatímco neúspěšné události znamenají selhání sledování procesů. Obvyklé události sledování procesů shrnuje tabulka 15.9.

**TABULKA 15.9:** Nejběžnější události sledování procesů

| ID události | Popis |
|---|---|
| 592 | Vytvoření nového procesu. |
| 593 | Ukončení procesu. |
| 594 | Zdvojení (duplikace) popisovače objektu. |
| 595 | Získání nepřímého přístupu k objektu. |

## Auditování systémových událostí

Při auditu systémových událostí můžeme sledovat případy, kdy uživatel nebo proces změní různé vlastnosti prostředí v počítači. Mezi běžné systémové události patří vymazání protokolu událostí Security (Zabezpečení), ukončení chodu (vypnutí) místního počítače a provedení změn v ověřovacích balících, které na počítači pracují.

V rámci auditu úspěšných systémových událostí je vhodné sledovat restarty systému; neočekávaný restart může být jednak projevem bezpečnostního incidentu, jednak ale každopádně bývá indikátorem určitého problému, který s bezpečností může, ale nemusí souviset. Audit úspěšných událostí generuje události při úspěšném dokončení systémové události, audit neúspěšných událostí znamená záznam selhání těchto operací.

Úspěšný výmaz protokolu událostí Security se zaznamenává bez ohledu na zapnutí auditu systémových událostí. Popis nejběžnějších typů systémových událostí je uveden v tabulce 15.10.



**TABULKA 15.10:** Nejběžnější systémové události

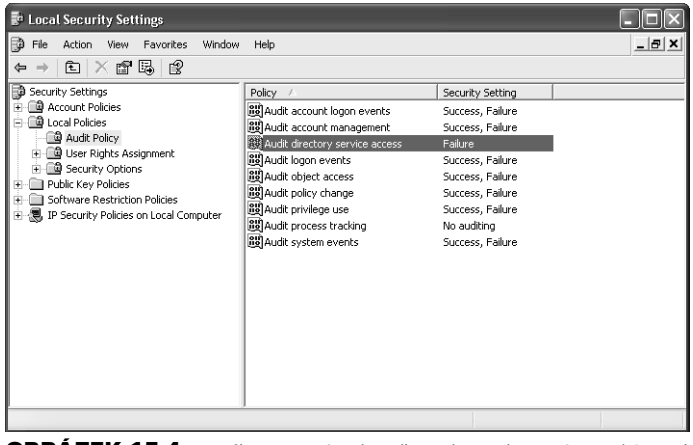
| ID události | Popis |
|---|---|
| 512 | Spouštění operačního systému Windows. |
| 513 | Ukončování operačního systému Windows. |
| 514 | Místní úřad zabezpečení (Local Security Authority, LSA) zavedl nový ověřovací balík. |
| 515 | Důvěryhodný přihlašovací proces se zaregistroval u místního úřadu zabezpečení (LSA). |
| 516 | Byly vyčerpány vnitřní prostředky alokované pro frontu zpráv bezpečnostních událostí; to znamená ztrátu některých zpráv s bezpečnostními událostmi. |
| 517 | Protokol Security (Zabezpečení) byl vymazán. |
| 518 | Správce zabezpečení účtů (Security Accounts Manager, SAM) zavedl oznamovací balíček. |
| 520 | Změna systémového času. |

## Jak povolit zásady auditování

Zásady auditování je možné v systému Windows Server 2003, Windows 2000 a Windows XP zapnout místně prostřednictvím konzoly MMC Local Security Policy (Místní zásady zabezpečení), nebo aplikací vhodné šablony zabezpečení. Na počítače se systémem Windows Server 2003, Windows 2000 a Windows XP můžeme zásady audito-

vání aplikovat také vzdáleně, prostřednictvím Group Policy (Zásady skupiny). V níže uvedených krocích si řekneme, jak zapnout zásady auditování místně v konzole MMC Local Security Policy (Místní zásady zabezpečení); příslušnou obrazovku vidíme na obrázku 15.4. Zapnutí auditu provedeme následovně:

1. Otevřete konzolu MMC Local Security Policy (Místní zásady zabezpečení).
2. Poklepáním rozbalte podstrom Local Policy (Místní zásady) a poté poklepáním rozbalte podstrom Audit Policy (Zásady auditu).
3. V podokně na pravé straně poklepejte na zásadu, kterou chcete zapnout nebo vypnout.
4. Zatrhněte zaškrtávací políčka Success (Úspěšné pokusy) a Failed (Neúspěšné pokusy), a to podle typů událostí, které mají podléhat sledování.
5. Nakonec konzolu MMC uzavřete.




**OBRÁZEK 15.4:** Konfigurace zásad auditu v konzole MMC Local Security Policy (Místní zásady zabezpečení)

Tabulka 15.11 popisuje zásady auditu, které je vhodné zapnout při sledování událostí zabezpečení. Spolu s událostmi přístupu k objektům a přístupu k adresářové službě nezapomeňte nad objekty nebo nad jednotlivými atributy, jejichž činnost budete sledovat, nastavit také odpovídající přístupové seznamy SACL.

**TABULKA 15.11:** Základní okruh zapnutých zásad auditu

| Zásada auditu | Auditované události |
|---|---|
| Audit Account Logon Events (Auditování událostí přihlášení k účtu) | Úspěšné, neúspěšné |
| Audit Account Management (Auditování událostí správy účtu) | Úspěšné, neúspěšné |
| Audit Directory Service Access (Auditování událostí přístupu k adresářové službě) | Úspěšné, neúspěšné |
| Audit Logon Events (Auditování událostí přihlášení) | Úspěšné, neúspěšné |

| Zásada auditu | Auditované události |
|---|---|
| Audit Object Access (Auditování přístupu k objektům) | Úspěšné, neúspěšné |
| Audit Policy Change (Auditování změny zásad) | Úspěšné |
| Audit Privilege Use (Auditování používání oprávnění) | Neúspěšné |
| Audit Process Tracking (Auditování sledování procesů) | Žádné |
| Audit System Events (Auditování systémových událostí) | Úspěšné |

**Další informace** Podrobnější informace ke konfiguraci zásad auditu prostřednictvím šablon zabezpečení a Group Policy (Zásady skupiny) jsou uvedeny v kapitole 11.



# 15.4 Monitorování auditovaných událostí

Události zapsané do protokolu Security (Zabezpečení) můžeme prohlížet pomocí několika různých metod. K dispozici tak máme na jedné straně ruční procházení protokolu v Prohlížeči událostí, ale na druhé straně také vyspělé, automatizované softwarové nástroje pro slučování a monitorování událostí, jako je Microsoft Operations Manager. Každá z těchto metod je určena pro jiné účely, takže si i vy sami zvolte takovou, která se pro dané prostředí a pro danou situaci hodí nejlépe. Monitorování událostí můžeme provádět pomocí čtyř základních metod:

- Event Viewer (Prohlížeč událostí)
- Vlastní skripty
- Nástroj Event Comb
- Plně automatizované nástroje, jako je Microsoft Operations Manager

Výklad plně automatizovaných nástrojů pro sledování událostí je mimo rámec této knihy; nyní se proto věnujeme zbývajícím třem.

## Práce s Prohlížečem událostí

Nejjednodušší metodou sledování bezpečnostních událostí v operačním systému je práce s Event Viewer (Prohlížeč událostí). Tento nástroj umožňuje:

- Prohlížet detailní informace o události
- Řadit události podle typu, zásad auditu a času
- Vyhledávat události podle hodnot běžných polí
- Filtrovat události podle hodnot běžných polí
- Exportovat protokoly událostí do souborů formátu `.evt`, `.csv` nebo `.txt`
- Pro prohlížení a správu protokolu událostí se připojit ke vzdálenému počítači

Event Viewer (Prohlížeč událostí) neumožňuje ale slučování (konsolidaci) událostí. Jestliže se tedy události zaznamenávají na několika různých serverech, například události přihlášení účtu (ty se u doménových účtů zapisují na ověřujícím řadiči domény), může být jejich kontrola v prohlížeči událostí dosti obtížná. Event Viewer dále neumí vyhledávat podle detailních informací o události. Vybrané události můžeme ale exportovat do souboru a poté je importovat do databáze, nebo exportované soubory z různých počítačů zpracovat ve vhodném vlastním skriptu.

## Vlastní skripty

Pro správu událostí je k dispozici několik skriptů. Seznámíme se alespoň s některými:

- **Dumpel.exe** Označovaný také jako Dump Event log; jedná se o skript, který z příkazového řádku provádí výpis protokolu událostí z místního nebo vzdáleného počítače do tabulátory odděleného textového souboru. Tento výsledný soubor pak můžeme importovat například do tabulkového procesoru nebo do databáze k dalšímu zpracování a šetření. Pomocí nástroje `Dumpel.exe` můžeme také filtrovat určité typy událostí, nebo ve filtru určité události vyřadit. (Nástroj `Dumpel.exe` najdete na doprovodném CD k této knize, ve složce Tools.)
- **Eventlog.pl** Tento perlový skript maže a kopíruje soubory protokolů a dále zobrazuje a mění vlastnosti souborů s protokoly na místním nebo vzdáleném počítači se systémem Windows 2000. Pomocí tohoto skriptového nástroje můžeme:
  - Měnit vlastnosti protokolu událostí
  - Zálohovat protokoly událostí (ukládat je)
  - Exportovat seznam událostí do textového souboru
  - Vymazat protokol událostí (odstranit z něj všechny události)
  - Dotazovat se na vlastnosti protokolů událostí
- **Eventquery.vbs** Skript v jazyce Microsoft VBScript, který zobrazuje události z protokolů událostí na místním nebo vzdáleném počítači se systémem Windows Server 2003 či Windows XP. Pod systémem Windows 2000 můžete kromě výše uvedeného skriptu `Eventlog.pl` použít také perlový ekvivalent tohoto skriptu, který je součástí *Microsoft Windows 2000 Server Resource Kitu*, Supplement One (Computer Press, 2000).
- **Logparser 2.2** Univerzální nástroj pro analýzu textových souborů a dalších zdrojů dat textového typu, jako jsou soubory auditovaných protokolů; kromě toho vytváří sestavy zadané pomocí podobných příkazů jako v jazyce T-SQL. V tomto nástroji můžeme také importovat soubory auditovaných protokolů do robustnějších aplikací pro práci s daty, jako je Microsoft SQL Server. Nástroj Logparser 2.2 si můžete stáhnout z webových stránek společnosti Microsoft, z adresy `http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx`.

## Nástroj Event Comb

Nástroj Event Comb provádí analýzu protokolů událostí z mnoha serverů současně, přičemž pro každý ze serverů, zahrnutých do vyhledávacích kritérií, vytvoří samostatný podproces. Pomocí nástroje Event Comb můžeme shromažďovat události

z několika počítačů, na kterých běží systémy Windows Server 2003, Windows 2000 a Windows XP. Mezi záznamy událostí v shromážděných souborech protokolů můžeme také vyhledávat konkrétní události podle libovolných polí. Event Comb umí také prohledávat archivované soubory protokolů.

**Na CD** Nástroj Event Comb (s názvem `EventcombMT.exe`) se nachází na doprovodném CD k této knize. Můžete jej stáhnout také z webových stránek společnosti Microsoft, z adresy `http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e`.

V nástroji Event Comb můžeme:

- **Definovat hledání podle jednoho ID událostí nebo podle několika ID událostí.** Potřebujeme-li vyhledávat několik ID událostí současně, oddělíme je mezerami.
- **Definovat interval hledaných událostí.** Intervaly jsou definovány jako uzavřené, tedy včetně příslušných hraničních bodů. Zápisem 528<ID<540 vyjádříme například hledání všech událostí s ID rovným od 528 do 540 včetně. Tato funkce je velice užitečná, protože většina aplikací zapisuje do protokolů události s jistého spojitého intervalu.
- **Omezit vyhledávání na konkrétní protokoly událostí.** Prohledávat můžeme protokoly Systém, Aplikace a Security (Zabezpečení). Při místním spuštění nástroje na řadiči domény můžeme kromě protokolů Systém, Aplikace a Security (Zabezpečení) prohledávat také protokol služby replikace souborů (FRS), protokol služby DNS (Domain Name System) a protokol služby Active Directory.
- **Omezit vyhledávání jen na události určitých typů.** Vyhledávání je možné omezit jen na chybové zprávy, informativní zprávy, upozornění, audit úspěšných událostí, audit neúspěšných událostí nebo obecné úspěšné události.
- **Omezit hledání jen na určité zdroje událostí.** Prohledávání můžeme omezit také na události z určitých konkrétních zdrojů, a tím celou operaci urychlit.
- **Vyhledávat určitý text v popisu události.** U jednotlivých událostí můžeme vyhledávat také text popisu. Tato funkce je užitečná především při hledání operací určitých uživatelů či skupin.
- **Definovat zpětné prohledávání určitého časového intervalu od aktuálního času.** Takto můžeme omezit vyhledávání na události z předešlého dne, týdne nebo měsíce.

Jako první musíme ovšem v nástroji Event Comb vybrat počítače, na nichž budeme události vyhledávat. Počítače v nástroji Event Comb přidáme do prohledávaného seznamu následujícím způsobem:

1. Nejprve zkontrolujeme, jestli nástroj Event Comb v poli Domain automaticky detekoval správnou doménu. Chcete-li prohledávat protokoly událostí z jiné domény, zapište do pole Domain ručně název nové domény.
2. Pro přidání počítače do prohledávaného seznamu klepneme na pole pod volbou Select To Search/ Right Click To Add. K dispozici jsou zde následující možnosti:
   - **Get DCs In Domain** Do seznamu přidá všechny řadiče domény v aktuální doméně.

- **Add Single Server** Do seznamu přidá server nebo pracovní stanici zadanou názvem.
- **Add All GCs In This Domain** Umožňuje přidání všech řadičů domény ve vybrané doméně, které jsou podle své konfigurace servery globálního katalogu.
- **Get All Servers** Přidá všechny servery, které v doméně vyhledá služba Browser, kromě všech řadičů domény.
- **Get Servers From File** Provede import souboru se seznamem prohledávaných serverů. Každý server musí být v tomto textovém souboru uveden na samostatném řádku.

3. Po vytvoření seznamu serverů musíme vybrat, nad kterými z nich bude vyhledávání probíhat. Vybrané servery jsou v seznamu zvýrazněny; jestliže při klepnutí na další servery podržíme klávesu Ctrl, přidáme je tak do seznamu vyhledávaných serverů.

Jakmile vybereme servery, jejichž protokoly událostí se budou prohledávat, můžeme dále zúžit rozsah hledání a vybrat konkrétní protokoly, typy hledaných událostí a další důležitá kritéria pro vyhledávání. Pod nástrojem Event Comb můžeme také definované hledání uložit a později je znovu načíst; to je užitečné zejména v případě, že často vyhledáváme události stejného typu. Vyhledávací kritéria se ukládají do registru pod větví `HKLM\SOFTWARE\Microsoft\EventCombMT`.

Výsledky hledání se podle výchozího nastavení ukládají do složky `C:\Temp`. Protože na mnoha počítačích mají v této složce oprávnění ke čtení souborů všichni uživatelé, a to zejména z důvodu podpory starších aplikací, je vhodné tuto cestu změnit. Součástí výsledků je souhrnný soubor s názvem `EventCombMT.txt`. Pro každý počítač v požadované množině prohledávaných protokolů událostí se dále vygeneruje samostatný textový soubor s názvem `NázevPočítače-NázevProtokolu_LOG.txt`; tyto jednotlivé textové soubory již obsahují všechny události z požadovaných protokolů událostí, které odpovídají zadaným kritériím.

# 15.5 Doporučené postupy

- **Určete, které události se budou zaznamenávat.** Společně s pracovníky, kteří mají obchodní a technické pravomoci, zajistěte audit všech požadovaných akcí a operací. Protože každý audit znamená snížení výkonu systému, je třeba sledovat jen ty události, na které se určitě budeme potřebovat v budoucnu odvolávat.
- **Na všech počítačích a síťových zařízeních synchronizujte systémový čas.** Pro správné svázání souvisejících událostí, které probíhají na různých počítačích a síťových zařízeních, musíte zajistit odpovídající synchronizaci času. Ideální je, pokud zajistíme synchronizaci všech počítačů a síťových zařízení s jedním stejným zdrojem času.
- **Vytvořte si srovnávací základnu událostí.** Nejprve si vytvořte srovnávací základnu bezpečnostních událostí za normálního stavu systému, s níž můžete později srovnávat případné vzorky podezřelého chování. Pokud se nemůžete odvolat na soubor protokolu se srovnávací základnou pořízenou za normálního stavu, je rozlišení běžných a škodlivých událostí dosti obtížné.

- **V souborech protokolů sledujte podezřelé chování.** Má-li být audit událostí účinným bezpečnostním opatřením, musíme v souborech auditovaných protokolů sledovat veškeré podezřelé chování. Vhodným řešením je také vytvoření zkušebního prostředí, na kterém nasimulujeme běžné útoky a následně provedeme analýzu souborů s protokoly. Tak můžeme zmíněné útoky snáze detekovat v ostrém, provozním prostředí. Události, které jsou obvyklým projevem podezřelého chování, je vhodné v souborech protokolů vyhledávat pomocí automatizovaného softwaru nebo vlastních skriptů.

# 15.6 Další informace

Následující články databáze znalostí (Knowledge Base):

- 300549: „How to Enable and Apply Security Auditing in Windows 2000“, `http://support.microsoft.com/kb/300549`
- 814595: „How to Audit Active Directory Objects in Windows Server 2003“, `http://support.microsoft.com/kb/814595`
- 314955: „How to Audit Active Directory Objects in Windows 2000“, `http://support.microsoft.com/kb/314955`
- 246120: „How to Determine Audit Policies from the Registry“, `http://support.microsoft.com/kb/246120`
- 232714: „How to Enable Auditing of Directory Service Access“, `http://support.microsoft.com/kb/232714`
- 299475: „Windows 2000 Security Event Descriptions (Part 1 of 2)“, `http://support.microsoft.com/kb/299475`
- 301677: „Windows 2000 Security Event Descriptions (Part 2 of 2)“, `http://support.microsoft.com/kb/301677`
- 824209: „How to Use the EventcombMT Utility to Search Event Logs for Account Lockouts“, `http://support.microsoft.com/kb/824209`
- 323076: „How to set event log security locally or by using Group Policy in Windows Server 2003“, `http://support.microsoft.com/kb/323076`
- Nástroj EventCombMT, ke stažení na Microsoft Download Center, `http://www.microsoft.com/downloads/details.aspx?displaylang=en&familyid=7af2e69c-91f3-4e63-8629-b999adde0b9e`
- Nástroj Logparser 2.2, ke stažení na Microsoft Scripting Center, `http://www.microsoft.com/technet/scriptcenter/tools/logparser/default.mspx`