



Auditování událostí v doméně



Mgr. Josef Horálek, Ph.D.

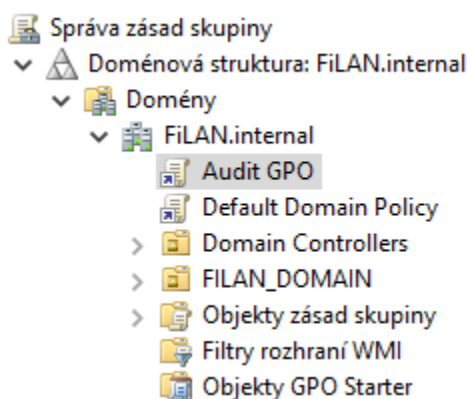
Auditování událostí v doméně

Zadáním úlohy 6 je konfigurace auditování bezpečnostních událostí v doméně, kde bude nastaveno základní logování chování objektů. Do této konfigurace budou spadat běžné události, jako je uzamčení uživatelských účtů a události s žádostí o vyšší oprávnění přístupu.

Vytvoření Audit Policy

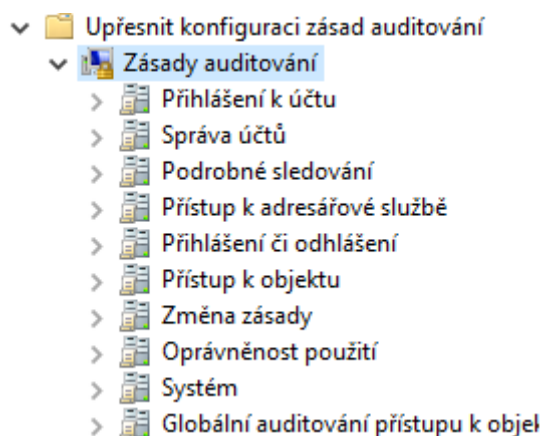
K reportování probíhajících událostí v doméně Active Directory je potřeba nejprve určit jaké události a za jakých podmínek mají být sledovány. Tohoto nastavení lze dosáhnout vytvořením GPO, propojeným s požadovanou skupinou objektů, u kterého bude zvoleno, jaké chování bude monitorováno.

V této úloze bude vytvořen objekt zásad skupiny pojmenovaný „**Audit GPO**“ a bude aplikován na všechny objekty v doméně FiLAN.internal, stejně jako Default Domain Policy.



Obr. 1 Vytvoření Audit GPO

Dalším krokem je konfigurace vytvořeného GPO, ve kterém bude určeno, jaké události mají být administrátorem domény sledovány. Pro potřeby tohoto prostředí jsou zvoleny zásady auditování **Správy účtů** a **Oprávněnosti použití**. Pomocí těchto zásad budou sledovány události při změnách účtů v počítačích, dále při vytvoření, změně, odstranění a uzamčení účtu uživatele a události s žádostí o povolení vyšší úrovně oprávnění. Cesta k nalezení těchto zásad v editoru je: Konfigurace počítače\ Zásady\ Nastavení systému Windows\ Nastavení zabezpečení\ Upřesnit konfiguraci zásad auditování\ Zásady auditování.



Obr. 2 Cesta k zásadám auditování

V podkategorii **Správa účtů** jsou nastaveny audity pro správu účtů počítače a pro správu účtů uživatelů. U obou těchto možností budou sledovány pouze úspěšné kontroly auditu.

Podkategorie	Události auditování
Auditovat správu skupin aplikací	Není nakonfigurováno
Auditovat správu účtů počítače	Úspěch
Auditovat správu skupin distribuce	Není nakonfigurováno
Auditovat jiné události správy účtu	Není nakonfigurováno
Auditovat správu skupiny zabezpečení	Není nakonfigurováno
Auditovat správu účtů uživatelů	Úspěch

Obr. 3 Auditování účtů počítačů a uživatelů

V podkategorii **Oprávněnost použití** bude zvoleno monitorování úspěšných i neúspěšných událostí v případě použití citlivých oprávnění. Po nakonfigurování této možnosti bude docházet k informování administrátora o každé události s žádostí o oprávnění správce. Taková volba je vhodná k upozornění administrátora před možnými útoky a nastavení potřebné úrovně zabezpečení.

Podkategorie	Události auditování
Auditovat použití oprávnění, která nejsou citlivá	Není nakonfigurováno
Auditovat události použití jiných oprávnění	Není nakonfigurováno
Auditovat použití citlivých oprávnění	Úspěchy a chyby

Obr. 4 Auditování použití citlivých oprávnění

Výsledkem použitých zásad auditování by měl být stejný stav, jako na Obr. 80.

Souhrn	
Kategorie	Konfigurace
Přihlášení k účtu	Není nakonfigurováno
Správa účtů	Nakonfigurováno
Podrobné sledování	Není nakonfigurováno
Přístup k adresářové službě	Není nakonfigurováno
Přihlášení či odhlášení	Není nakonfigurováno
Přístup k objektu	Není nakonfigurováno
Změna zásady	Není nakonfigurováno
Oprávněnost použití	Nakonfigurováno
Systém	Není nakonfigurováno
Globální auditování přístupu k objektům	Není nakonfigurováno

Obr. 5 Přehled nastavených zásad auditování

Zaznamenané události je poté možné sledovat v Prohlížeči událostí na doménových řadičích mezi protokoly zabezpečení.

Prohlížeč událostí (Místní)		Zabezpečení Počet událostí: 193 835			
Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy	
Úspěšný audit	02.09.2018 18:25:01	Microsoft Windows security auditing.	4719	Změna zásad auditu	
Úspěšný audit	02.09.2018 18:23:13	Microsoft Windows security auditing.	4767	Správa uživatelských účtů	
Úspěšný audit	02.09.2018 18:13:15	Microsoft Windows security auditing.	4740	Správa uživatelských účtů	
Úspěšný audit	02.09.2018 18:02:29	Microsoft Windows security auditing.	4719	Změna zásad auditu	
Úspěšný audit	02.09.2018 17:52:28	Microsoft Windows security auditing.	4817	Změna zásad auditu	
Úspěšný audit	02.09.2018 17:52:28	Microsoft Windows security auditing.	4719	Změna zásad auditu	
Úspěšný audit	30.08.2018 18:45:07	Microsoft Windows security auditing.	4817	Změna zásad auditu	
Úspěšný audit	30.08.2018 18:45:06	Microsoft Windows security auditing.	4719	Změna zásad auditu	
Úspěšný audit	30.08.2018 18:45:06	Microsoft Windows security auditing.	4719	Změna zásad auditu	

Obr. 6 Prohlížeč událostí na DC

Prvním příkladem ověření funkčnosti nastaveného auditu může být událost s ID 4740, která oznamuje, že došlo k **uzamčení** uživatelského účtu **manager1** na počítači **FILANPC**.

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	02.09.2018 18:25:01	Microsoft Windows security auditing.	4719	Změna zásad auditu
Úspěšný audit	02.09.2018 18:23:13	Microsoft Windows security auditing.	4767	Správa uživatelských účtů
Úspěšný audit	02.09.2018 18:13:15	Microsoft Windows security auditing.	4740	Správa uživatelských účtů
Úspěšný audit	02.09.2018 18:02:29	Microsoft Windows security auditing.	4719	Změna zásad auditu

Událost 4740, Microsoft Windows security auditing.	
Obecné	Podrobnosti
Účet uživatele byl uzamčen.	
Předmět:	
ID zabezpečení:	SYSTEM
Název účtu:	FILANDC1\$
Doména účtu:	FILAN
ID přihlášení:	0x3E7
Uzamčený účet:	
ID zabezpečení:	FILAN\manager1
Název účtu:	manager1
Další informace:	
Název počítače volajícího:	FILANPC

Obr. 7 Úspěšný audit uzamčeného uživatelského účtu

Přibližně 10 minut po této události došlo k manuálnímu odemčení uživatelského účtu **manager1** účtem **Administrator**, při kterém vznikla událost auditu s ID 4767.

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	02.09.2018 18:25:01	Microsoft Windows security auditing.	4719	Změna zásad auditu
Úspěšný audit	02.09.2018 18:23:13	Microsoft Windows security auditing.	4767	Správa uživatelských účtů
Úspěšný audit	02.09.2018 18:13:15	Microsoft Windows security auditing.	4740	Správa uživatelských účtů
Úspěšný audit	02.09.2018 18:02:29	Microsoft Windows security auditing.	4719	Změna zásad auditu

Událost 4767, Microsoft Windows security auditing.	
Obecné	Podrobnosti
Účet uživatele byl odemčen.	
Předmět:	
ID zabezpečení:	FILAN\administrator
Název účtu:	administrator
Doména účtu:	FILAN
Přihlašovací ID:	0xFA8B2
Cílový účet:	
ID zabezpečení:	FILAN\manager1
Název účtu:	manager1
Doména účtu:	FILAN

Obr. 8 Úspěšný audit administrátorem odemčeného účtu

Dalším příkladem můžou být události zaznamenávající použití **citlivých/privilegovaných** oprávnění. U GPO Audit Policy bylo nastaveno sledování takovýchto událostí v případě úspěchu i neúspěchu. Na Obr. 84 je zobrazen neúspěšný audit události s ID 4674, kdy došlo k zadání špatného hesla pro účet Administrator.

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4673	Použití citlivých oprávnění
Neúspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4674	Použití citlivých oprávnění
Neúspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4674	Použití citlivých oprávnění

Událost 4674, Microsoft Windows security auditing.	
Obecné	Podrobnosti
U privilegovaného objektu došlo k pokusu o operaci.	
Předmět:	
ID zabezpečení:	LOCAL SERVICE
Název účtu:	LOCAL SERVICE
Doména účtu:	NT AUTHORITY
ID přihlášení:	0x3E5
Objekt:	
Server objektu:	LSA
Typ objektu:	-
Název objektu:	-
Popisovač objektu:	0x0
Informace o procesu:	
ID procesu:	0x264
Název procesu:	C:\Windows\System32\lsass.exe
Požadovaná operace:	
Požadovaný přístup:	16777216
Oprávnění:	SeSecurityPrivilege

Obr. 9 Neúspěšný audit privilegovaného přístupu

Ve chvíli, kdy došlo k zadání správného hesla pro požadovaný privilegovaný přístup, vznikla událost s ID 4673, kde proběhl úspěšný audit této události.

Klíčová slova	Datum a čas	Zdroj	ID události	Kategorie úlohy
Úspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4673	Použití citlivých oprávnění
Neúspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4674	Použití citlivých oprávnění
Neúspěšný audit	03.09.2018 17:13:04	Microsoft Windows security auditing.	4674	Použití citlivých oprávnění

Událost 4673, Microsoft Windows security auditing.	
Obecné	Podrobnosti
Byla volána privilegovaná služba.	
Předmět:	
ID zabezpečení:	SYSTEM
Název účtu:	FILANDC1\$
Doména účtu:	FILAN
ID přihlášení:	0x3E7
Služba:	
Server:	NT Local Security Authority / Authentication Service
Název služby:	LsaRegisterLogonProcess()
Proces:	
ID procesu:	0x264
Název procesu:	C:\Windows\System32\lsass.exe
Informace o požadavku na službu:	
Oprávnění:	SeTcbPrivilege

Obr. 10 Úspěšný audit privilegovaného přístupu

Zajímavým faktem je, že v prohlížeči událostí je možné zaznamenat vytvoření více záznamů ve výpisu, po vykonání pouze jedné události. V prostředí Microsoft Windows domény

existuje spousta dalších možností, jaké události a na jaké úrovni je možné sledovat. Jejich vytvoření závisí pouze na zadaných požadavcích.