Univerzita Hradec Králové
Fakulta informatiky a managementu
Katedra informačních technologií

Bezpečnostní dohled OS Windows

(video tutoriály)

Bakalářská práce

Autor: Jan, Loubek
Studijní obor: Aplikovaná Informatika

Vedoucí práce: Ing. Ph.D., Tomáš, Svoboda

Hradec Králové srpen 2024

Prohlášení:

Prohlašuji, že jsem bakalářskou práci zpracoval samostatně a s použitím uvedené literatury.

V Hradci Králové dne 12.8.2024

vlastnoruční podpis

Jan Loubek

Poděkování:

Děkuji vedoucímu bakalářské práce Ing. Ph.D., Tomáš, Svoboda za metodické vedení práce a přínosné konzultace k tématu.

Abstrakt

Bakalářská práce poukazuje na význam logování v Operačním systému Microsoft Windows a jejich význam při vyhledávání škodlivých programů, virů a podezřelých komunikací v síti. Zaměřuje se na využití nástrojů k tomu určených od společnosti Microsoft a jejich představení v praktických ukázkách formou video tutoriálů. Velká pozornost je věnována Sysinternals nástrojům od významného španělského vývojáře Marka Russinoviche. Představí základy auditování. Tutoriály se zaměřují zejména na jejich správné používání a praktické využití v nastaveni logovaní. Na závěr se zaměří na centrální sběr událostí z jednotlivých počítačů na předem určenou stanici.

Abstract

Title: Security Monitoring of Windows OS - Video Tutorials

The bachelor's thesis highlights the importance of logging in the Microsoft Windows Operating System and their significance in detecting malicious programs, viruses, and suspicious network communications. It focuses on the use of tools designed for this purpose by Microsoft and presents them through practical demonstrations in the form of video tutorials. Significant attention is given to the Sysinternals tools by the renowned Spanish developer Mark Russinovich. It introduces the basics of auditing. The tutorials mainly focus on their correct usage and practical application in log setting. Finally, it addresses the centralized collection of events from individual computers to a predetermined station.

Keywords: Event, Sysinternals, video tutorial, log, GPO, basic logging, audit, event collection

Obsah

1 Úvod ... 1
2 Cíl práce ... 2
3 Historie ... 3
3.1 Windows ... 3
3.2 Windows servery ... 5
3.3 Active Directory ... 6
3.3.1 Adresářové služby ... 6
4 Logy ... 7
4.1 Event Viewer ... 7
4.2 Prvky záznamu v událostním protokolu systému Windows ... 8
4.3 Typy protokolů (Logs) ... 9
4.3.1 Protokoly analytické a debug ... 10
4.4 Audit policy ... 11
5 Skupinová politika (Group policy) ... 12
6 Sysinternals ... 15
6.1 Process Explorer ... 16
6.2 Autoruns ... 17
6.2.1 Porovnání Správce úloh a Autoruns ... 17
6.3 Sysmon ... 18
6.4 PsLogList ... 19
6.4.1 Porovnání Event Viewer a PsLogList ... 20
7 Dílčí úlohy bezpečnostního monitoringu ... 21
7.1 První dílčí úloha ... 21
7.2 Druhá dílčí úloha ... 21
7.3 Třetí dílčí úloha ... 22

7.4 Čtvrtá dílčí úloha....23
8 Videotutorialy....24
8.1 Video 1....25
8.2 Video 2....29
8.3 Video 3....37
8.4 Video 4....47
9 Závěry a doporučení....63
10 Seznam použité literatury....64
11 Přílohy....68

1 Úvod

Bezpečnost IT systémů a dat je jedním z největších priorit každé organizace. Potřeba efektivního bezpečnostního monitoringu se tak stává stále důležitější. Tento trend klade nové požadavky na efektivní správu a zabezpečení systémů. Schopnost monitorovat a reagovat na bezpečnostní incidenty je klíčová pro minimalizaci rizik spojených s kybernetickými hrozbami. Systém Windows, jako jeden z nejpoužívanějších operačních systémů na světě, poskytuje různé nástroje a možnosti pro bezpečnostní monitoring, které mohou být využity k ochraně a zabezpečení IT infrastruktury.

V teoretické části budou představeny a podrobně popsány postupy a řešení dílčích úloh bezpečnostního monitoringu v OS Windows s důrazem na využití event logu a nastavení group policy. Tato část bude sloužit jako základ, který umožní pochopit klíčové aspekty a techniky používané při zabezpečení systémů.

Praktická část práce se zaměří na vytvoření konkrétních řešení a návodů ve formě video tutoriálů. Tyto tutoriály budou navrženy tak, aby poskytly praktické ukázky a postupy, které mohou uživatelé snadno následovat a aplikovat ve svých vlastních prostředích. Video formát umožní efektivnější prezentaci postupů a technik, což usnadní jejich pochopení a implementaci.

Výsledkem této práce by měly být ucelené a srozumitelné materiály, které budou sloužit jako užitečný nástroj pro všechny, kteří se chtějí zlepšit v oblasti bezpečnostního monitoringu OS Windows.

2 Cíl práce

Cílem bakalářské práce je vytvořit podpůrné materiály v oblasti bezpečnostního monitoringu s důrazem na konfiguraci a řešení OS Windows v podobě video tutoriálů. V teoretické části budou představeny a podrobně popsány postupy a řešení dílčích úloh bezpečnostního monitoringu v OS Windows s důrazem na využití event logu a nastavení group policy. V praktické části pak budou vytvořena praktická řešení dílčích úloh ve formě video tutoriálů.

3 Historie

3.1 Windows

Historie osobních počítačů se datuje do roku 1977, kdy byl vyvinut mikroprocesor. Počítač se tak stal cenově dostupný i pro soukromé osoby.

V roce 1980 začala IBM (International Business Machines) začala IBM vyrábět osobní počítače a tím vznikla potřeba vytvoření operačního systému. Tohoto úkolu se zhostila firma Microsoft, která se doposud věnovala především vývoji programovacího jazyku BASIC.

Na úplném začátku vývoje operačních systémů vytvořených společností Microsoft pro osobní počítač vytvořený IBM byl předchůdce operačních systémů MS-DOS. Zkratka DOS označuje Diskový Operační Systém. Tento systém umožňoval jednoduchou komunikaci mezi uživatelem a počítačem. Uživatel zadával příkazy počítači pomocí klávesnice, protože myš byla v této době používána jen velmi sporadicky. Komunikace byla zobrazována na jednoduché obrazovce.

Původní verze s názvem MS-DOS 1.0 byla představena v srpnu 1981. Systém běžel v 8KB paměti na procesoru Intel 8086. Disk mohl obsahovat jeden adresář a v něm až 64 souborů, což bylo i v té době nedostačující.

Dále následoval systém DOS 2.0, který byl vydán v roce 1983. Tento systém již fungoval na pevném disku a bylo poprvé možno používat hierarchické adresáře. Poprvé bylo možno použít adresáře a podadresáře a soubory. Obsah paměti byl ji ž 24KB

V roce 1984 vznikl v IBM PC AT s procesorem Intel 80286 a společně s ním Microsoft uvedl na trh DOS 3.0.AT. Tento systém již osahoval rozšířené adresování a primitivní funkce ochran paměti. Paměť se zvýšila na 36KB. Rozvinutější upgrade DOS 3.1. vznikl v roce 1984 a DOS 3.3 v roce 1987. Následně Microsoft vytvořil ještě mnoho dalších verzí MS DOS, které fungovaly zároveň s Windows. Poslední verze MS-DOS 8.0 byla na trh uvedena v roce 2000.

Následovala snaha Microsoftu uživatelsky přívětivější systém. Výsledkem byl nový operační systém s příjemným grafickým rozhraním s názvem Windows. Windows zpočátku nebyl operační systém, ale pouze grafická aplikace, která fungovala nad operačním systémem MS-DOS.

První verze měla název Windows 1.0. a vyšla v roce 1983. Poté následovala verze 2.0. Obě tyto verze nebyly příliš úspěšné, protože pro ně existovalo v té době málo softwaru a nebyly příliš stabilní.

Až verze 3.0 z roku 1990 a následná verze Windows 3.1 z roku 1991 začaly být veřejností široce využívány. V roce 1993 byla vydána verze pod názvem Windows NT 3.1. kde NT označovalo New Technology. Šlo o 32bitový operační systém, který využíval výhod nových microprocesorů a nabízel možnost multitaskingu.

Následně Microsoft vydal v roce 1996 verzi NT 4.0, která má obdobnou architekturu jako 3.x., ale poskytuje již podobné grafické rozhraní jako Windows 95. Tento systém byl primárně určen k použití v domácnostech, ale v praxi byl používán hlavně firmami jako pracovní stanice v místních sítích. Byl stabilní, fexibilní a umožňoval použití více procesorů v jednom počítači.

Následovala verze Windows 95 z roku 1995. Novinkou v této verzi byla možnost multitaskingu a automatické detekce konfigurace zařízení – tzv. Plug and Play.

Verze Windows 98 z roku 1998 byla zaměřena především na implementaci internetu a již obsahovala program Explorer a další programy propojené s internetem.

Další významný uprgrade Microsoft představil v roce 2000 pod názvem Windows Millenium. Základní architektura byla podobná jako u Windows NT 4.0, ale byly přidány nové funkce. Byl zde kladen důraz na podporu distribuovaného zpracování. Základním prvkem byla nová adresářová služba Active Directory. Další důležitou funkcí byla správa napájení, která byla zásadní pro přenosné počítače. Pozornost byla zaměřena na práci s multimédii. Tato verze nebyla primárně určena pro domácí počítače.

V roce 2001 byla vydána desktopová verze Windows XP. Podle počtu prodaných licencí to byl a nejoblíbenější verze Winsows. V roce 2003 byla představena serverová verze Windows Server 2003, která podporuje 32 bitoví i 64bitové procesory.

Další desktopová verze s názvem Windows Vista byla vydána v roce 2006 a podporovala architektury Intel x86 i AMD x64. Hlavní změnou bylo nové grafické rozhraní a výrazné vylepšení zabezpečení. Využívala nové uživatelské rozhraní s Windows Aero. [1]

Verze Windows 7 z roku 2009 kladla důraz na funkčnost a výkon. V podstatě šlo spíš o upgrade Windows Vista. Oproti předchozí verzi měl výrazně vyšší funkčnost a výkon.

Windows 8 z roku 2012 využívaly nové grafické rozhraní Microsoft Metro, které se používá pro tablety, notebooky, stolní počítače a Windows phone.

Následná verze z roku 2015 s názvem Windows 10 přinesla lepší funkčnost mezi různými třídami zařízení. Windows 10 je poslední verze Windows. Verze Windows 11 již nebude. Místo toho budou následovat nové verze Windows 10. Již proběhly 3 takové

aktualizace: verze 1511 v listopadu 2015, verze 1607 v červenci 2016 a verze 1703 v březnu 2017.

Windows 10 je sdílenou platformou známou pod názvem OneCore a funguje na počítačích, telefonech, herní konzoli Xbox, HoloLens a komponentech internetů věcí jako Raspberry Pi2. [2]

3.2 Windows servery

Společnost Microsoft paralelně vyvíjela operační systémy Windows fungující jako síťový server.

První z nich se jmenoval Windows 3.11 – Windows for Workgroups a byl představen veřejnosti v roce 1992.

Zajímavými funkcemi tohoto systému poskytujících síťovou podporu byly síťové karty a kabely, sdílení adresářů, disků a tiskáren, funkce emailů a rychlých zpráv.

Operační systém fungující jako server se začal vyvíjet až s Windows NT. Windows NT 4.0 Server z roku 1996 byl první z této skupiny. Mohl sloužit mnoha uživatelům v síti najednou.

Jeho nástupcem byl systém Windows Server 2000. Hlavní novinkou byl prvek Active Directory fungující jako služba pro správu uživatelů a zdrojů v lokální síti.

V roce 2003 následoval systém Windows Server 2003, který byl postaven na systému Windows XP. Novinkou oproti předchozí verzi byla internetová informační služba pro vytváření serverových webových stránek.

Windows Server 2008 z roku 2008 obsahoval vylepšení služby Active Directory, pravidel pro skupiny, správy disků a zabezpečení.

V roce 2012 následoval systém Windows server 2012. Přinášel novinku ve využití cloudů a podpory virtualizace serverů.

Od roku 2016 systém Windows Server 2016 nabízí uživatelům modernizaci datových center, což umožňuje přesun datových úložišť do veřejného cloudu Azure. Jako novinka byl představen Nano Server, což je malý operační systém účelově určený na provoz cloudových aplikací. Funguje jako platforma pro kontejnery[3]

3.3 Active Directory

Active Directory je rozsáhlý systém spravující správu počítačové struktury a sítě. Je to adresářová struktura v systémech Windows 2000 a Windows Server 2003.
Adresář obsahuje informace o jednotlivých objektech a vztazích mezi nimi. Mezi tyto objekty patří servery, stanice, aplikace, databáze, jednotliví uživatelé... Uživatel potřebuje co nejjednodušeji nalézt tyto komponenty a pracovat s nimi. Správce zas potřebuje řídit, jak jsou tyto objekty používány.

Active Directory obsahuje mnoho služeb. Hlavní rolí je správa účtů a uživatelů, jejich autorizace a autentizace. Dalšími úkoly jsou např. Group Policy (správa povolení v jednotlivých počítačích) nebo hromadné instalace aplikací. Pomáhá Serverům pracujícím s klientskými pracovními stanicemi založenými na Windows 95, Windows 98 a Windows NT 4.0. .

3.3.1 Adresářové služby

Vedle doménové funkce Active Directory Directory Service, jsou zde i vedlejší role např. Active Directory - Federation Services nebo role RODC - Domain Controller pouze pro čtení.
Funkce . Active Directory - Federation Services poskytuje možnost jednotného přihlášení ve více aplikacích. Umožní tak například přístup uživatelům z jiných organizací. Umožňuje tak jednotkám bezpečnou spolupráci napříč doménami Active Directory a snižuje nutnost vytvářet nadbytečné duplicitní účty a hesla. Usnadňuje autentizaci, takže např. webové aplikace mohou vyžadovat ověření pomocí čipové karty.[4]

4 Logy

Služba protokolu událostí se spouští automaticky při spuštění systému Windows. Protokoly aplikací a systému mohou zobrazovat všichni uživatelé, ale protokoly zabezpečení jsou přístupné pouze správcům.

4.1 Event Viewer

Event Viewer (Prohlížeč událostí) je nástroj ve Windows, který zobrazuje podrobné informace o významných událostech v počítači. Příklady těchto událostí zahrnují programy, které se nespustí podle očekávání, nebo automaticky stahované aktualizace. Prohlížeč událostí je obzvláště užitečný při řešení chyb ve Windows a aplikacích.

Prohlížeč událostí zobrazuje tyto typy událostí:

- Chyba: Významný problém, jako je ztráta dat nebo funkcionality. Například pokud služba selže při načítání při startu, bude zaznamenána chyba.
- Varování: Událost, která není nutně významná, ale může naznačovat možný budoucí problém. Například pokud je nízké místo na disku, bude zaznamenáno varování.
- Informace: Událost popisující úspěšný provoz aplikace, ovladače nebo služby. Například když se síťový ovladač úspěšně načte, bude zaznamenána událost informace.
- Úspěšný audit: Auditovaný pokus o zabezpečený přístup, který se podaří. Například úspěšný pokus uživatele o přihlášení do systému bude zaznamenán jako událost úspěšného auditu.
- Neúspěšný audit: Auditovaný pokus o zabezpečený přístup, který selže. Například pokud uživatel zkusí přistoupit k síťovému disku a selže, pokus bude zaznamenán jako událost neúspěšného auditu.[5]

Použitím protokolů událostí v Event Vieweru lze získat informace o hardwaru, softwaru a problémech systému a sledovat události zabezpečení Windows.
Postup pro přístup k Event Vieweru ve Windows 8.1, Windows 10 a Serveru 2012 R2:

1. Kliknout pravým tlačítkem myši na tlačítko *Start* a vybrat *Ovládací panely* > *Systém a zabezpečení* a dvakrát kliknout na *Správa*.
2. Dvakrát kliknout na *Zobrazení událostí*.
3. Vybrat typ protokolů, které se mají zkontrolovat (např. Aplikace, Systém).[5]

4.2 Prvky záznamu v událostním protokolu systému Windows

Událostní protokol systému Windows poskytuje informace o hardwarových a softwarových událostech, které se vyskytují v operačním systému Windows. Pomáhá síťovým administrátorům sledovat potenciální hrozby a problémy, které mohou snížit výkon. Windows ukládá událostní protokoly ve standardním formátu, což umožňuje jasný porozumění informacím. Následující jsou hlavní prvky událostního protokolu:

- Název protokolu

  Název událostního protokolu, do kterého budou zapisovány události z různých komponent protokolování. Události jsou obvykle zaznamenávány pro systém, zabezpečení a aplikace.

- Datum/čas události

  Obsahuje datum a čas, kdy se událost stala.

- Kategorie úkolu

  Identifikuje typ zaznamenaného událostního protokolu. Vývojáři aplikací mohou také definovat kategorie úkolů pro poskytnutí dalších informací o události.

- ID události

  Toto identifikační číslo systému Windows pomáhá síťovým administrátorům jednoznačně identifikovat konkrétní zaznamenanou událost.

- Zdroj

  Název programu nebo softwaru způsobujícího záznam událostního protokolu.

- Úroveň

  Úroveň události představuje závažnost zaznamenaného událostního protokolu. Patří sem informace, chyby, podrobné záznamy, varování a kritické záznamy.

- Uživatel

  Jméno uživatele, který se přihlásil do počítače se systémem Windows, když se událost stala.

- Počítač

  Název počítače, který zaznamenal událost.[6]

4.3 Typy protokolů (Logs)

Windows Server zaznamenává události v následujících protokolech:

- Protokol aplikací

  Protokol aplikací obsahuje události zaznamenané programy. Události, které jsou zapsány do protokolu aplikací, jsou určeny vývojáři softwarového programu.

- Protokol zabezpečení

  Protokol zabezpečení obsahuje události, jako jsou platné a neplatné pokusy o přihlášení. Obsahuje také události související s využitím zdrojů, například při vytváření, otevírání nebo mazání souborů. Pro zapnutí, použití a určení, které události jsou zaznamenávány v protokolu zabezpečení, musíte být přihlášeni jako správce nebo jako člen skupiny Administrátoři.

- Protokol systému

  Protokol systému obsahuje události zaznamenané komponentami systému Windows. Tyto události jsou předem určeny systémem Windows.

- Protokol služby adresářů

  Protokol služby adresářů obsahuje události související s Active Directory. Tento protokol je k dispozici pouze na řadičích domén.

- Protokol serveru DNS

  Protokol serveru DNS obsahuje události související s rozlišováním DNS jmen na nebo z internetových protokolových (IP) adres. Tento protokol je k dispozici pouze na DNS serverech.

- Protokol služby replikace souborů

  Protokol služby replikace souborů obsahuje události, které jsou zaznamenávány během procesu replikace mezi řadiči domén. Tento protokol je k dispozici pouze na řadičích domén.[7]

4.3.1 Protokoly analytické a debug

Analytické a Debug protokoly jsou ve výchozím nastavení vypnuty. Po jejich povolení se mohou rychle zaplnit velkým množstvím protokolů. Z tohoto důvodu je se zapínají na určenou dobu, aby shromáždily nějaká údaje pro ladění a poté se znovu vypnou. Tento postup lze provést pomocí uživatelského rozhraní systému Windows nebo příkazové řádky. [14] Protokoly je třeba nejprve zviditelnit v uživatelském rozhraní [15]

- Protokol analytický

  Analytické události jsou zveřejněny ve velkém množství. Popisují provoz programu a naznačují problémy, které nemohou být řešeny uživatelským zásahem.

- Protokol Debug

  Debug události jsou používány vývojáři při ladění problémů s používanými programy.[16]

4.4 Audit policy

Auditní politika systému Windows určuje, jaké typy informací o systému se bude nalézat v bezpečnostním protokolu. Windows používá devět kategorií auditní politiky a 50 podkategorií auditní politiky, aby uživateli poskytl detailnější kontrolu nad tím, které informace jsou zaznamenávány.

Ve výchozím nastavení, pokud je definována hodnota pro politiku v jedné z hlavních kategorií, buď v místní bezpečnostní politice počítače nebo v příslušné skupinové politice (GPO), pak tato hlavní politika obvykle přepíše jakékoli konfigurace, které jsou provedeny uživatelem na úrovni podkategorií. Podle výchozího chování systému Windows se politiky podkategorií projeví pouze tehdy, když uživatelem je zanechána související hlavní kategorie nedefinovaná v místní bezpečnostní politice a ve všech příslušných GPOs. Pokud je politika kategorie definována, pak budou definovány všechny politiky podkategorií pod touto politikou.

Důležitá jsou slova "obvykle" a "výchozí chování", protože nový Editor objektů skupinové politiky (GPE) Audit: Force audit policy subcategory settings (Windows Vista nebo novější) může toto chování obrátit a nastavit podkategoriální konfigurace nad hlavními politikami, pokud je to povoleno. Pokud je tato možnost povolena, konfigurace podkategorií přepíše způsob, jakým aplikovaná skupinová politika nastavuje hlavní politiku.[8]

5 Skupinová politika (Group policy)

Skupinová politika je soubor nástrojů uvnitř operačních systémů Microsoft Windows Server, který umožňuje IT správcům centrálně spravovat mnoho aspektů jak uživatelských účtů v jejich doméně, tak i účtů počítačů připojených k doméně. Ve skutečnosti ji lze používat i bez domény.

Většinou se skupinová politika používá tehdy, když je potřeba publikovat nebo nastavit nastavení pro širokou (nebo úzkou) základnu uživatelů nebo klientů stolních počítačů v korporátním prostředí. Skupinová politika je pro tyto úkoly velmi užitečná a může ušetřit pracovníkům IT nespočet hodin práce, kterou by jinak strávili ručním nastavováním těchto stejných nastavení na všech počítačích. Zatímco skupinová politika poskytuje správcům stolních počítačů spoustu flexibility, může se stát ještě efektivnější vzhledem k tomu, že účty počítačů v rámci Active Directory zahrnují jak stolní/laptopové počítače, tak i servery. Většina firem má oddělené role pro správce stolních počítačů a serverů, ale celkově mohou z těchto schopností, které jsou uloženy ve skupinové politice, velmi profitovat. V dnešním myšlení zaměřeném na informační bezpečnost, se nejčastěji kladem důraz na uživatele a jejich zařízení, aby se zajistilo, že tyto počítače nejsou negativně ovlivňovány vnějšími silami, přičemž většina zabezpečení sítě je zaměřena na infrastrukturu serverů. Servery v síti jsou zařízení, která poskytují služby a ukládají data. Udržování těchto dat v bezpečí je velkým úkolem. Zabezpečení serverů je v dnešním světě nezbytné a existuje mnoho způsobů, jak skupinovou politikou prosadit toto zabezpečení. [9]

Group Policy (skupinové politiky) slouží k centrální správě počítačů s pomocí Active Directory. Hlavně se tedy využijí pro počítače zařazené do domény. Lze ale využít i lokální politiky (Local Group Policy), které nabízí o něco omezenější funkčnost, ale fungují i na samostatné počítače. [10]

Skupinová politika je infrastruktura, která umožňuje specifikovat spravované konfigurace pro uživatele a počítače prostřednictvím nastavení skupinové politiky a preferencí skupinové politiky. Pro konfiguraci nastavení skupinové politiky, která ovlivňuje pouze místní počítač nebo uživatele, lze použít Editor místní skupinové politiky. Nastavení skupinové politiky a preferencí skupinové politiky lze spravovat v prostředí Active Directory Domain Services (AD DS) pomocí Konzole správy skupinové politiky (GPMC). Nástroje pro správu skupinové politiky jsou také součástí balíčku Nástroje pro vzdálenou správu serveru (Remote Server Administration Tools), který

poskytuje způsob, jak spravovat nastavení skupinové politiky z administrátorova pracovního stolu.

Když je GPMC nainstalován na serverech nebo klientských počítačích, je zde také nainstalován modul Windows PowerShell. GPMC má plnou funkcionalitu Windows PowerShell. Pokud je nainstalován balíček Nástroje pro vzdálenou správu serveru, jsou také nainstalovány nejnovější cmdlety pro skupinovou politiku ve Windows PowerShell.[11]

Lze také centrálně konfigurovat volitelné záznamy a trasování pro Pokročilou správu skupinové politiky (AGPM) pomocí administrativních šablon.

Pro dokončení těchto postupů je vyžadován uživatelský účet s rolí Správce AGPM (plná kontrola), uživatelský účet schvalovatele, který vytvořil GPO nebo uživatelský účet s potřebnými oprávněními v Pokročilé správě skupinové politiky. Kromě toho je vyžadován uživatelský účet s přístupem k serveru AGPM pro spuštění záznamů na serveru AGPM. [12]

Skupinová politika je nejjednodušší způsob, jak dosáhnout a konfigurovat nastavení počítačů a uživatelů v síti založené na službách Active Directory Domain Services (AD DS). Pokud firma nepoužívá skupinovou politiku, ztrácí obrovskou příležitost snížit náklady, ovládat konfigurace, udržovat uživatele produktivní a spokojené a zlepšit zabezpečení. Skupinová politika funguje na principu "dotkněte se jednou, nastavte mnoho".

- Požadavky pro používání skupinové politiky a následování pokynů, které tyto tyto šablony poskytují, jsou jednoduché:
- Síť musí být založena na AD DS (to znamená, že alespoň jeden server musí mít nainstalovanou roli AD DS).
- Počítače, které jsou spravovány, musí být připojeny k doméně, a uživatelé, kteří jsou spravovány, musí používat doménové přihlašovací údaje k přihlášení na své počítače.
- Je nutné mít oprávnění ke změnám skupinové politiky v doméně.

I když se tato šablona zaměřuje na používání skupinové politiky v AD DS, lze také konfigurovat nastavení skupinové politiky lokálně na každém počítači. Tato schopnost je skvělá pro jednorázové použití nebo pro počítače ve workgroupu, ale používání lokální skupinové politiky není doporučeno pro firemní sítě založené na AD DS. Důvod je jednoduchý: Skupinová politika založená na doméně centralizuje správu, takže

můžete ovládat mnoho počítačů z jednoho místa. Lokální skupinová politika vyžaduje, aby se dotkla každého počítače, což není ideální použití v rozsáhlém prostředí.
Operační systém Windows uplatňuje nastavení politiky, která se definuje pomocí skupinové politiky. Většinou je zakázáno uživatelům toto rozhraní nastavovat. Navíc, protože Windows ukládá nastavení skupinové politiky na zabezpečených místech v registru, standardní uživatelské účty nemohou tato nastavení změnit. Takže nastavením na jedné konzoli lze nastavit a uplatnit toto nastavení na mnoha počítačích. Když se nastavení již nevztahuje na počítač nebo uživatele, skupinová politika odstraní nastavení politiky, obnoví původní nastavení a povolí jeho uživatelské rozhraní. [13]

6 Sysinternals

Sysinternals je sada nástrojů, která později byla akvizována společností Microsoft. Tato sada nástrojů nabízí širokou škálu utilit určených pro pokročilou správu, diagnostiku a monitorování operačního systému Windows. Nástroje Sysinternals jsou navrženy tak, aby poskytovaly hlubší úroveň informací a kontrolu než standardní nástroje dodávané s Windows. [20]

Vývoj Windows Sysinternals byl započat společníky Bryce Cogswell a Mark Russinovich v roce 1996. V červenci 2006 Microsoft převzal společnost Winternals a Sysinternals. Jedním z cílů převzetí bylo zajistit, že tyto nástroje zůstanou nadále volně dostupné.[17] Do roku 2013[18] byly stránky Sysinternals na technet.microsoft.com jedním z nejnavštěvovanějších míst na TechNetu, s průměrně 50 000 návštěvníky denně a třemi miliony stažení měsíčně. Uživatelé Sysinternals se stále vraceli pro nejnovější verze nástrojů a nové utility.

První nástroj Sysinternals byl Ctrl2cap pro usnadnění přechodu z UNIXových systémů. Předtím než se začal používat Windows NT v roce 1995, byla klávesa Ctrl umístěna tam, kde je na běžných PC klávesnicích klávesa Caps Lock. Ctrl2cap je dodnes k dispozici na stránkách Sysinternals .

Další nástroj byl NTFSDOS. Jedná se o nástroj, který uživatelům umožnil získat data z oddílu formátovaného jako NTFS pomocí běžné diskety DOS. Další dva nástroje, se jmenovaly Filemon a Regmon. Tyto tři utility - NTFSDOS, Filemon a Regmon - se staly základem Sysinternals. Filemon a Regmon, byly vydány pro Windows 95 a Windows NT, ukazovaly činnost souborového systému a registru. Staly se prvními nástroji svého druhu a nedocenitelnými pomocníky při debug. [17]

Nástroje Sysinternals pokrývají širokou škálu funkcí v mnoha aspektech operačního systému Windows. Zatímco některé sofistikovanější nástroje, jako je Process Explorer a Process Monitor, pokrývají více kategorií operací, jiné lze lépe nebo hůře seskupit do konkrétních kategorií. Mnohé z nich jsou vybaveny grafickým uživatelským rozhraním (GUI), zatímco jiné jsou konzolové nástroje, vybavené mnoha přepínači určenými pro automatizaci nebo běžící v režimu příkazového řádku.[19]

Některé klíčové aspekty a filozofie spojené s Sysinternals zahrnují:

- **Pokročilé diagnostické** nástroje: Sysinternals nabízí nástroje, které umožňují detailní monitorování běžících procesů, služeb, síťové aktivity,

správu ovladačů, sledování změn v registru a další. Tyto nástroje jsou užitečné pro identifikaci a řešení složitých problémů v operačním systému.

- **Transparentnost a kontrola**: Sysinternals umožňuje uživatelům hlubší pohled do toho, co se děje na jejich systému. Umožňuje zobrazovat informace o procesech, souborech, síťové komunikaci a dalších systémových aspektech, což umožňuje lepší pochopení a správu systému.
- **Nástroje pro profesionály a pokročilé uživatele**: Tyto nástroje jsou nejčastěji využívány správci systémů, technickými specialisty, vývojáři a dalšími, kteří potřebují pokročilé nástroje k diagnostice a správě systému.
- **Rozmanitost a specializace**: Sada nástrojů Sysinternals obsahuje různé specializované utility, jako jsou monitorování procesů, správa spouštění, analýza síťového provozu, a mnoho dalšího. Tato rozmanitost pokrývá širokou škálu potřeb a scénářů, kterým čelí správci systému.

Vzhledem k tomu, že Sysinternals byl integrován do produktů a služeb Microsoftu, nástroje této sady jsou často používány v profesionálním prostředí a přispívají k lepšímu řízení a diagnostice prostředí založených na Windows. Díky pravidelným aktualizacím a podpoře ze strany Microsoftu zůstává Sysinternals důležitým zdrojem pro pokročilou správu systému Windows.[20]

6.1 Process Explorer

Process Explorer poskytuje informace o tom, které a procesy byly otevřeny nebo načteny. Zobrazuje seznam procesů, služeb a uživatelů, grafy výkonu systému a využití sítě a abstrakci nazvanou "aplikace".[25] Process Explorer, na rozdíl od Správce úloh, který je uživatelů je oblíben pro rychlou orientaci, proč je systém pomalý a které nežádoucí procesy je vhodné ukončit, dokáže zobrazit klíčová data, která mohou pomoci technickému uživateli identifikovat proces jako hrozbu. [17]

V hlavním okně Process Exploreru se zobrazují aktuálně aktivní soubory a názvy jejich vlastních účtů. V režimu „Zpracování“, se zobrazují popisovače, které proces vybraný v horním okně otevřel. V režimu „Knihovna DLL“ se zobrazí knihovny DLL a soubory mapované do paměti. Další funkcí Process Explorer je vyhledávání, které procesy mají konkrétní popisovače otevřené nebo načtené knihovny DLL. Tento nástroj bohužel nezobrazuje klíčová data, která mohou pomoci technickému uživateli identifikovat proces jako hrozbu. [25]

Tabulka 1 Porovnání Správce úloh a Process Explorer. Zdroj: [26][25]

	Správce úloh	Process Explorer
Přístupnost	integrovaný do Windows přístupný přímo z operačního systému bez potřeby externích nástrojů	musí být stažen a spuštěn jako externí aplikace z webu Sysinternals
Možnosti	zobrazuje pouze seznam běžících aplikací a procesů, včetně jejich využití CPU, paměti, disku a sítě. jednoduché a intuitivní rozhraní, snadno použitelné pro většinu uživatelů	zobrazuje otevřené soubory, registrace DLL, vlákna a jejich výkon. zobrazuje detailní informace o procesech, které mohou být složité pro běžné uživatele.
Scénáře použití	vhodný pro běžné uživatele, kteří potřebují rychlý přehled o výkonu a správu základních funkcí systému. jednoduchý na používání, bez potřeby hlubokého technického porozumění.	určen pro pokročilé uživatele a IT profesionály, kteří potřebují detailní informace a analýzu složitý pro méně zkušené uživatele kvůli množství detailních informací a funkcí.

6.2 Autoruns

Autoruns je nástroj spravující rozsáhlé informace o spouštění všech spouštěcích mechanismů. Zobrazuje, jaké programy jsou nakonfigurovány tak, aby běžely během spouštění systému nebo přihlášení a spouštění různých aplikací systému Windows, například Internet Explorer, Explorer nebo přehrávač médií.[24]

6.2.1 Porovnání Správce úloh a Autoruns

Tabulka 2 Porovnání Správce úloh a Autoruns. Zdroj: [26][24]

	Správce úloh	Autoruns
Přístupnost	integrovaný přímo do systému Windows snadno přístupný přes klávesové zkratky nebo hlavní panel	není integrován do Windows musí být stažen a spuštěn jako externí aplikace

Možnosti	zobrazuje seznam programů spouštěných při startu systému možnost povolit nebo zakázat spouštění jednotlivých aplikací ukazuje vliv každé aplikace na dobu spouštění systému (nízký, střední, vysoký) nemá pokročilé možnosti správy nebo analýzy spouštěcích položek neumožňuje přidávat vlastní položky nebo zobrazit podrobné informace o souborech a jejich cestách	možnost povolit nebo zakázat jednotlivé spouštěcí položky může zobrazit položky, které jsou skryté před běžnými nástroji možnost hledání online informací o konkrétních položkách vyžaduje více znalostí o systému Windows a jeho spouštěcích mechanismech
Scénáře použití	vhodný pro běžné uživatele, kteří potřebují jednoduchý a rychlý přehled a základní správu spouštěcích programů	pro pokročilé uživatele a IT profesionály, kteří potřebují detailní analýzu a plnou kontrolu nad všemi spouštěcími položkami systému

6.3 Sysmon

System Monitor (*Sysmon*) je systémová služba systému Windows a ovladač zařízení, který po instalaci v systému zůstává aktivní i při restartování systému, aby monitoroval a protokoloval systémovou aktivitu do protokolu událostí Systému Windows. Slouží k monitorování a zaznamenávání událostí na úrovni jádra systému Windows. Sysmon poskytuje detailní informace o aktivitách na systému, což je užitečné pro analýzu bezpečnostních incidentů, monitorování chování aplikací a detekci potenciálně škodlivého chování. Dále poskytuje podrobné informace o vytváření procesů, síťových připojeních a změnách času vytvářených souborů.

Shromažďováním událostí generovaných pomocí souborů událostí systému Windows a následnou analýzou událostí lze identifikovat škodlivou nebo neobvyklou aktivitu a porozumět tomu, jak ve síti fungují útočníci a malware. Služba funguje jako chráněný proces, takže nepovoluje širokou škálu interakcí v uživatelském režimu. *Sysmon* neposkytuje analýzu událostí, které generuje, ani se nepokouší se skrýt před útočníky.

Sysmon zahrnuje následující funkce:

- Zaznamenává vytváření procesů pomocí úplného příkazového řádku pro aktuální i nadřazené procesy.
- Zaznamenává hodnotu hash procesních souborů pomocí SHA1 (výchozí), MD5, SHA256 nebo IMPHASH.
- Současně lze použít více hodnot hash.
- Zahrnuje identifikátor GUID procesu v procesu vytváření událostí, které umožňují korelaci událostí i v případě, že Systém Windows znovu používá ID procesů.
- Obsahuje identifikátor GUID relace v každé události, který umožňuje korelaci událostí ve stejné přihlašovací relaci.
- Zaznamenává načítání ovladačů nebo knihoven DLL s jejich podpisy a hodnotami hash.
- Otevírá protokoly pro nezpracovaný přístup ke čtení disků a svazků.
- Volitelně protokoluje síťová připojení, včetně zdrojového procesu každého připojení, IP adres, čísel portů, názvů hostitelů a názvů portů.
- Detekuje změny v době vytvoření souboru, aby bylo jasné, kdy byl soubor skutečně vytvořen. Úprava časových razítek vytvoření souboru je technika, kterou malware běžně používá k pokrytí jeho stop.
- Automaticky znovu načtěte konfiguraci, pokud se změnila v registru.
- Filtruje pravidla pro dynamické zahrnutí nebo vyloučení určitých událostí.
- Generuje události z počátku procesu spouštěné za účelem zachycení aktivity vytvořené sofistikovaným malwarem v režimu jádra.[21]

6.4 PsLogList

Elogdump slouží k prohlížení a zobrazování událostí z protokolu událostí v místním nebo vzdáleném počítači. Tento nástroj umožňuje uživatelům přístup k událostem zalogovaným pomocí Windows Event Logging mechanismu. PsLogList je klon elogdump s tím rozdílem, že PsLogList umožňuje přihlášení ke vzdáleným systémům v situacích, kdy aktuální sada přihlašovacích údajů zabezpečení nepovolí přístup k protokolu událostí, a PsLogList načte řetězce zpráv z počítače, na kterém se nachází protokol událostí, které se zobrazí.

PsLogList zahrnuje následující funkce:

- Získání dat z logů využitím API poskytovaného systémem Windows pro získávání informací z Event Viewer.
- Filtrování a selekce umožňuje uživatelům aplikovat různé filtry a kritéria pro získání specifických událostí z Event Viewer.
- Zobrazení obsahu protokolu událostí systému v místním počítači s vizuálně přívětivým formátováním.
- Umožňuje také exportovat zobrazená data do různých formátů.[22]

6.4.1 Porovnání Event Viewer a PsLogList

Tabulka 3 Porovnání Event Viewer a PsLogList. Zdroj: [22][23]

	Event Viewer	PsLogList
Přístupnost	snadno přístupný a intuitivní pro uživatele preferující GUI	vhodný pro pokročilé uživatele a administrátory, kteří preferují příkazový řádek a skriptování
Možnosti	nabízí jednoduché a uživatelsky přívětivé rozhraní pro základní a středně pokročilou správu událostí	poskytuje větší flexibilitu a možnosti pro automatizaci a vzdálenou správu
Scénáře použití	ideální pro rychlé prohlížení a analýzu událostí na jednom počítači	lepší volba pro správu a monitorování událostí na více počítačích a pro integraci do komplexních skriptů a automatizovaných procesů

7 Dílčí úlohy bezpečnostního monitoringu

7.1 První dílčí úloha

Problematika dílčích úloh bezpečnostního monitoringu v OS Windows je zaměřena na práci s prohlížečem událostí a seznámení s jednotlivým typy událostí.

7.2 Druhá dílčí úloha

Problematika dílčích úloh bezpečnostního monitoringu v OS Windows je zaměřena zejména na využití GPO pro sledování auditu změn uživatelských účtů, audit přístupů k adresářové službě, auditu změny zásad auditování audit samotného přihlášení uživatelů.

Politika „Audit správy účtů uživatelů“ (Audit User Account Management) umožňuje auditovat změny uživatelských účtů, zejména změny hesel, změny SID a změny oprávnění ke správě účtu. Monitoring změn hesel je důležitý zejména z důvodů monitorováním a dokumentováním těchto činností. Lze tak identifikovat neoprávněné nebo podezřelé změny hesel. To umožňuje rychle přijmout opatření, která zabrání potenciálnímu narušení bezpečnosti nebo neoprávněnému přístupu k citlivým informacím.[27]

Politika "Auditování přístupu k objektům" (Audit Object Access) monitoruje přístupy k určeným souborům, složkám a objektům. Identifikuje neoprávněné přístupy nebo pokusy o přístup k důležitým datům. Umožňuje efektivní vyšetřování bezpečnostních incidentů tím, že poskytuje důkazy, kdo měl přístup k objektům a jaké operace provedl. Působí jako prevence, protože přístupy k citlivým datům jsou monitorovány, což může odradit zaměstnance a další uživatele od neoprávněného přístupu nebo manipulace s těmito daty. [28]

Politika "Auditování systémových souborů" (Audit System Files) sleduje změny ve specifických systémových souborech a složkách, které jsou kritické pro správné fungování operačního systému. To zahrnuje soubory systému Windows, konfigurační soubory a další důležité soubory. Pomáhá identifikovat neoprávněné nebo nečekané změny v systémových souborech, které mohou být indikátorem malwarové infekce nebo jiných bezpečnostních hrozeb, rekonstruovat, co se stalo, a identifikovat zodpovědné osoby nebo škodlivé entity. Tím pomáhá při správě změn a zajištění, že všechny změny jsou autorizované a zdokumentované.[29]

Politika "Auditování změn zásad" (Audit Policy Change) je klíčová díky zajištění bezpečnosti a stability IT prostředí a pro správu a sledování změn v bezpečnostních politikách systému. Sleduje změny v nastavení bezpečnostních politik, jako jsou zásady skupinových politik (Group Policy), auditovací politiky a další kritické konfigurace. Pomáhá identifikovat neoprávněné nebo nečekané změny, které mohou ohrozit bezpečnost systému, například změny v politikách hesel nebo v přístupových právech. Poskytuje přehled o tom, jaké změny jsou prováděny v bezpečnostních politikách a kdo je provádí. [30]
Politika "Audit přihlášení" (Audit Logon Events) sleduje všechny pokusy o přihlášení k systému, včetně úspěšných a neúspěšných pokusů. Pomáhá identifikovat, kdy a kdo se pokusil přihlásit k systému, odhalit neobvyklé vzorce přihlášení, které mohou indikovat pokusy o útoky jako brute force nebo použití odcizených přihlašovacích údajů. Rekonstruuje, kdo a kdy měl přístup k systému.[31]

7.3 Třetí dílčí úloha

Problematika dílčích úloh bezpečnostního monitoringu v OS Windows je zaměřena zejména na využití Sysinternals nástrojů, které slouží ke sledování procesu a zaznamenávaní událostí, při čem bude kladen důraz na http komunikaci.
Monitorování procesů je klíčové pro efektivní správu počítačového systému, jeho bezpečnost a výkon. Procesy mohou využívat CPU, paměť, disk nebo síťové prostředky neefektivně, což může zpomalit celý systém. Monitorování proto pomáhá identifikovat a následně optimalizovat nebo zcela ukončit tyto náročné procesy. Na pozadí počítače může běžet škodlivý software a vykonávat zde nebezpečné operace. Monitorování procesů umožňuje detekci a efektivní eliminaci těchto nebezpečných aktivit. Sledování procesů může také pomoci odhalit neautorizované aktivity, jako je snaha o přístup k citlivým datům nebo změny v konfiguraci systému. Procesy mohou mít vzájemné závislosti a interakce, které mohou ovlivnit systémovou stabilitu. Monitorování umožňuje korigování těchto interakcí. [33][34]

Sledování http komunikace může identifikovat problémy s výkonem, například pomalé odezvy serveru nebo chyby v síťovém připojení, které mohou ovlivnit uživatelský komfort. Dále může pomoci identifikovat neautorizované nebo škodlivé aktivity, například pokusy o komunikaci s podezřelými servery, které mohou být příznakem

malware nebo botnetů. Umožňuje analyzovat, jak aplikace komunikují se serverem a optimalizovat jejich chování, aby byly efektivnější a rychlejší.

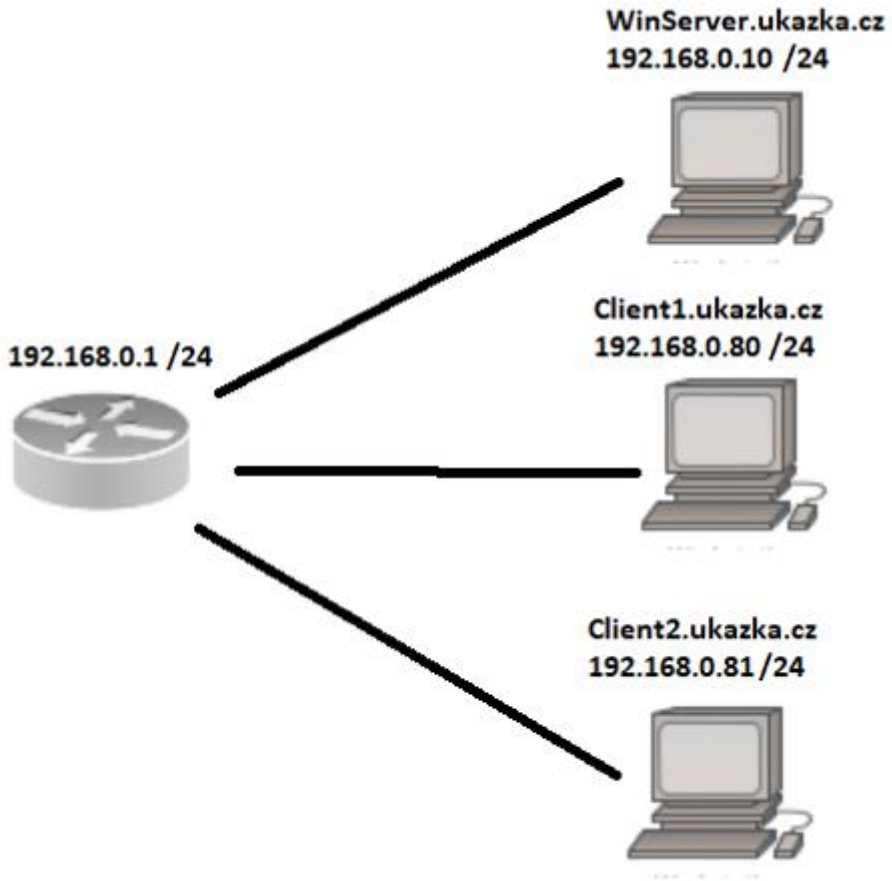
7.4 Čtvrtá dílčí úloha

Problematika dílčích úloh bezpečnostního monitoringu v OS Windows je zaměřena na sběr událostí z uživatelských počítačů.

Centralizace sběru událostí umožňuje rychlý a snadný přístup z jednoho místa k událostem z různých zdrojů, což usnadňuje monitoring a analýzu. Umožňuje konsolidovat data z různých systémů, aplikací a zařízení, což poskytuje ucelený přehled o stavu a aktivitách počítačové infrastruktury.

8 Videotutorialy

V této části byla vytvořena videa, která navazují na předchozí teoretickou část. První video je zaměřeno na základní logování na lokáním počítači. Je zde představen nástroj Event Viewer a jak s ním pracovat v praxi. Druhé video ukáže využití GPO k logování a auditu. Zde je využit Active Directory k vytváření GPO k nastavení auditování. Třetí video se týká využití Sysinternals nástrojů. Jsou tu představeny některé nástroje Sysinternals, které mohou pomoci k identifikaci hrozeb. Závěrečné video vysvětluje využití nástrojů pro sběr logů. Ukazuje možnosti sběru událostí. Ve videotutoriálech byl použit buď samostatný počítač nebo domovská topologie Ukazka.cz, ve které byl simulován jeden server a dva klientské počítače viz Obrázek1. V následujících 4 podkapitolách jsou přespány texty a otisky obrazovky vytvořených videí.

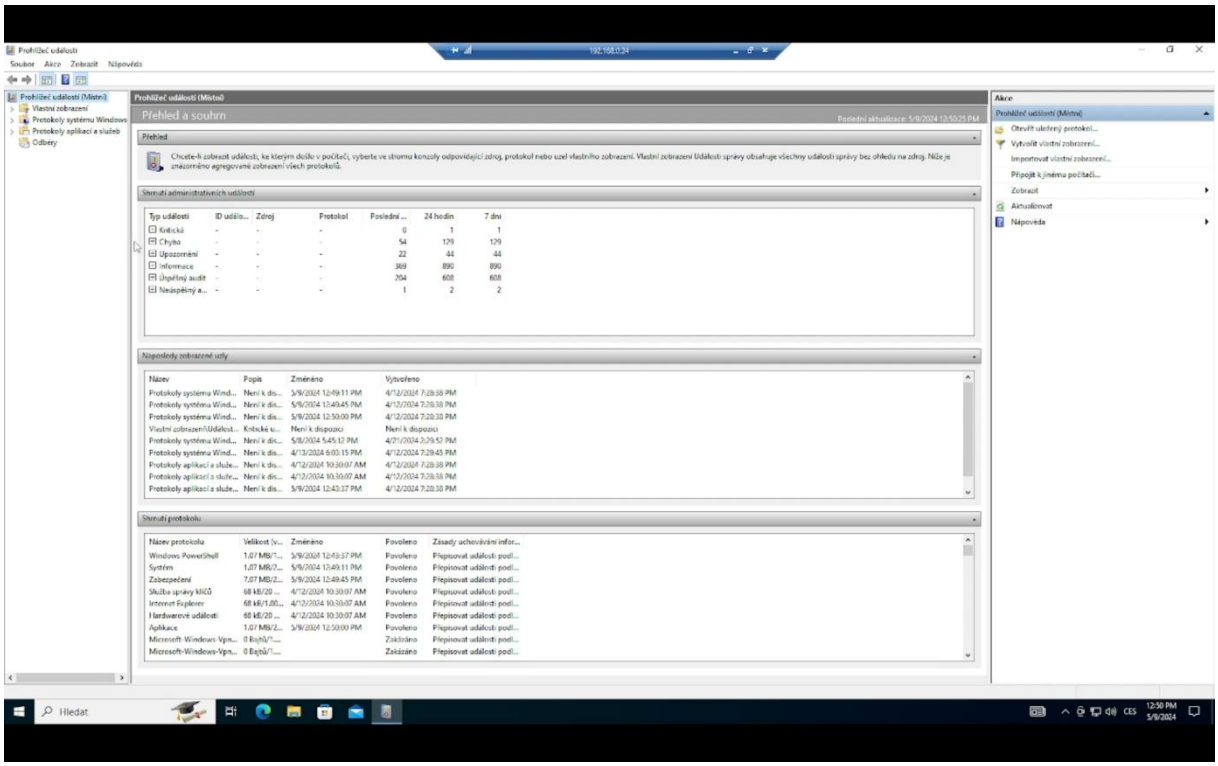


Obr. 1 Topologie sítě. Zdroj: vlastní zpracování

8.1 Video 1

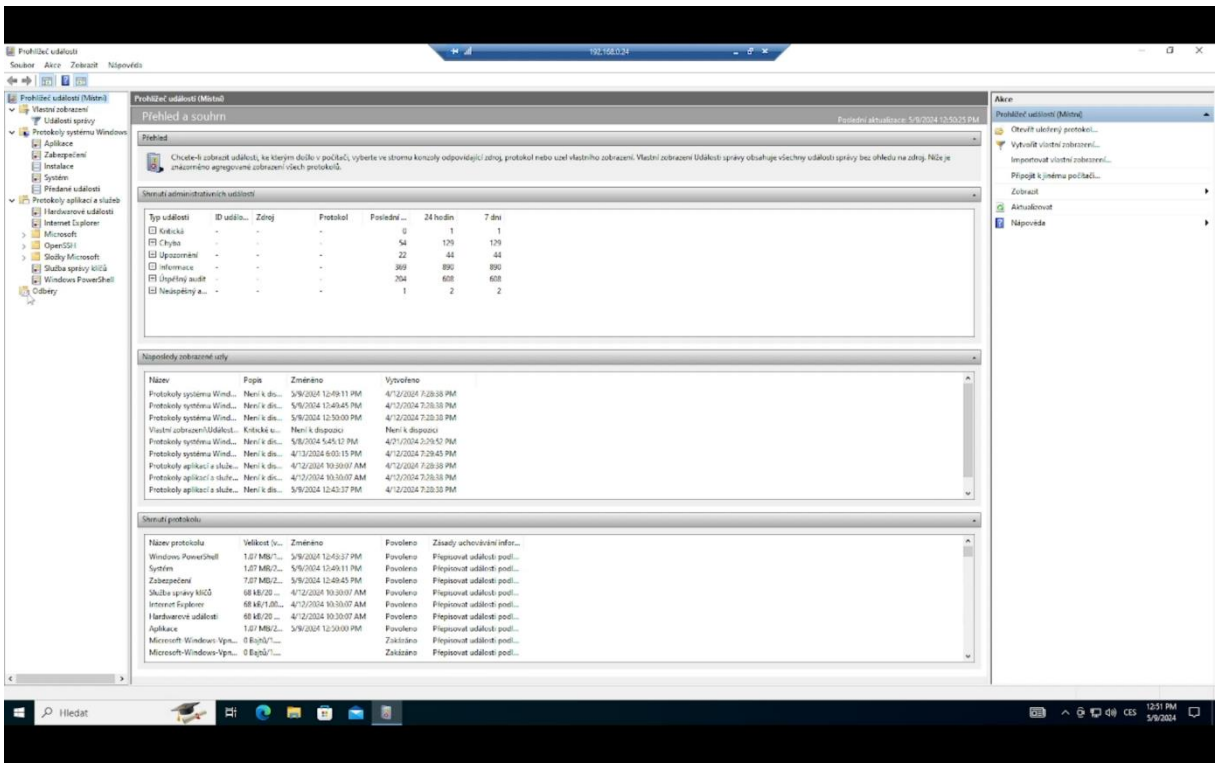
Základní práci s Event Viewer neboli Prohlížečem událostí. Do tohoto prohlížeče se lze dostat několika způsoby. Jedním z nich je zapsat do vyhledávání „eventvwr.msc“. Při zapnutí prohlížeče událostí se zobrazí tabulky „Shrnutí administrativních událostí“, „Naposledy zobrazené uzly“ a „Shrnutí protokolu“.

V tabulce „Shrnutí administrativních událostí“ jsou zobrazeny všechny typy událostí, o kterých se zmíním později. V tabulce „Naposledy zobrazené uzly“ vidíme v poslední době zobrazené události a v tabulce „Shrnutí protokolu“ se nachází jednotlivé protokoly, které nám poskytují události viz Obrázek 2.



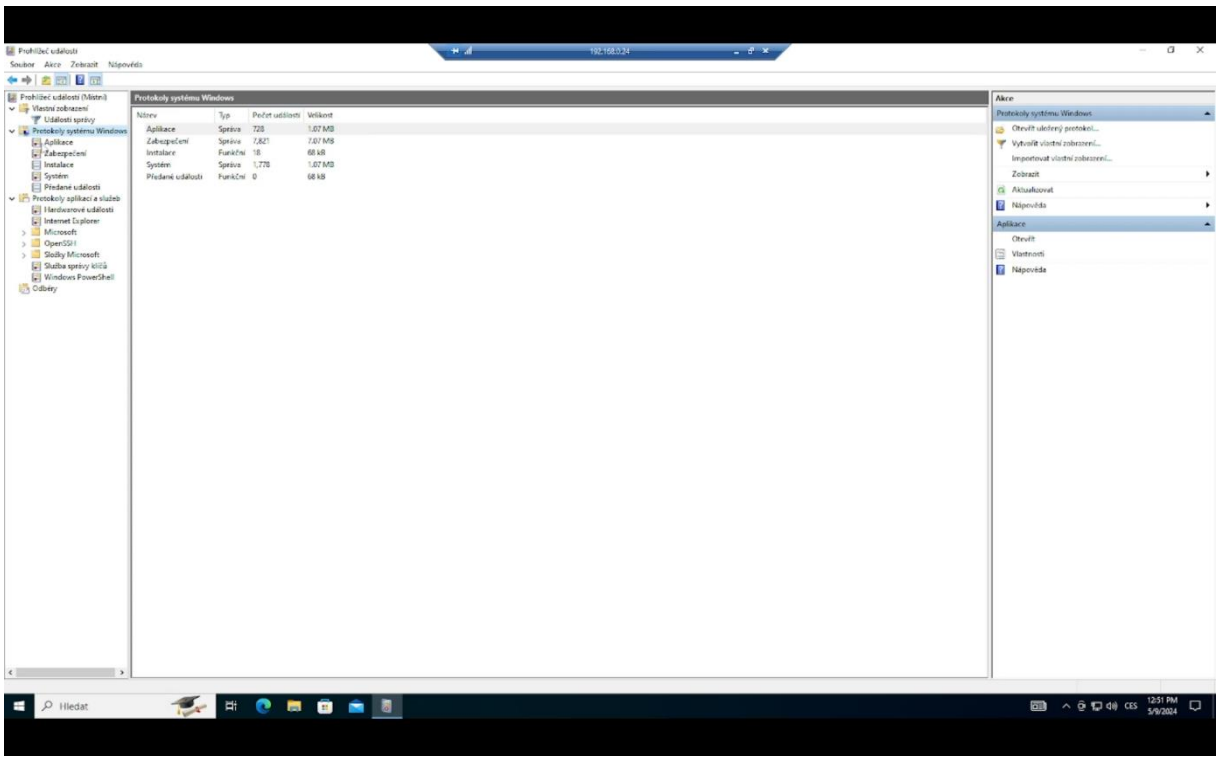
Obr. 2 Úvodní obrazovka Prohlížeče událostí. Zdroj: vlastní zpracování

Nejdůležitější částí obrazovky je nalevo umístěný panel, ve kterém lze zobrazit jednotlivé události, které jsou rozděleny do několika kategorií: Vlastní zobrazení, Protokoly systému Windows, Protokoly aplikací a služeb, a Odběry viz Obrázek 3.



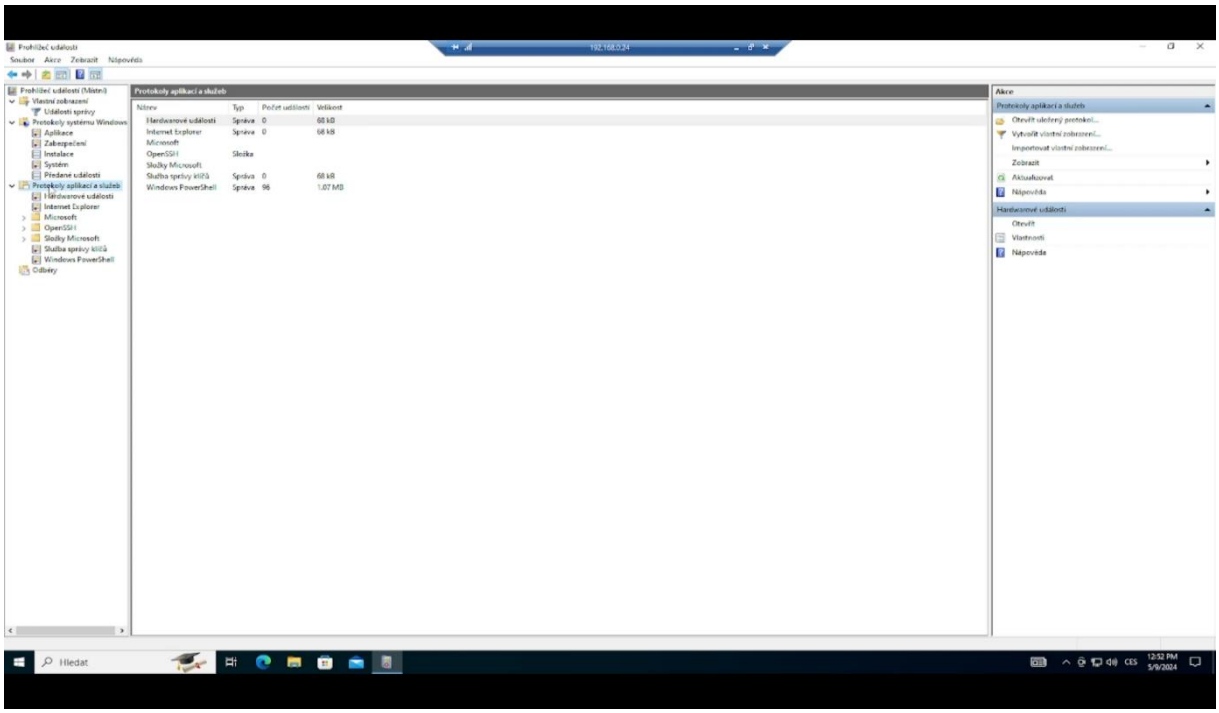
Obr. 3 Prohlížeč událostí s rozbaleným levým panelem. Zdroj: vlastní zpracování

Ve Vlastním zobrazení jsou v základu odfiltrovány upozornění, chyby a kritické události. Dále se zde dají definovat vlastní filtry. V záložce „Protokoly systému Windows“ se nachází 5 položek, z nichž pro nás důležité jsou tyto tři: „Aplikace“, „Zabezpečení“ a „Systém“. Položka „Aplikace“ obsahuje seznam událostí aplikací ukončených i aktuálně probíhajících na této stanici. V položce „Zabezpečení“ jsou uložené události související s bezpečností systému. Do položky „Systém“ se ukládají události spojené s operačním systémem viz Obrázek 4.



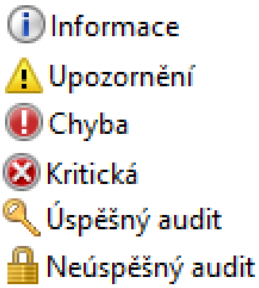
Obr. 4 Prohlížeč událostí s otevřeným Protokoly systému Windows. Zdroj: vlastní zpracování

Dále se podíváme na záložku „Protokoly aplikace a služeb“. Jsou zde zobrazeny speciální typy událostí, které poskytují podrobnější informace o provozu aplikací a služeb. Mohou se zde nacházet například protokoly aplikací, aplikací třetích stran, služeb nebo detaily diagnostiky viz Obrázek 5.



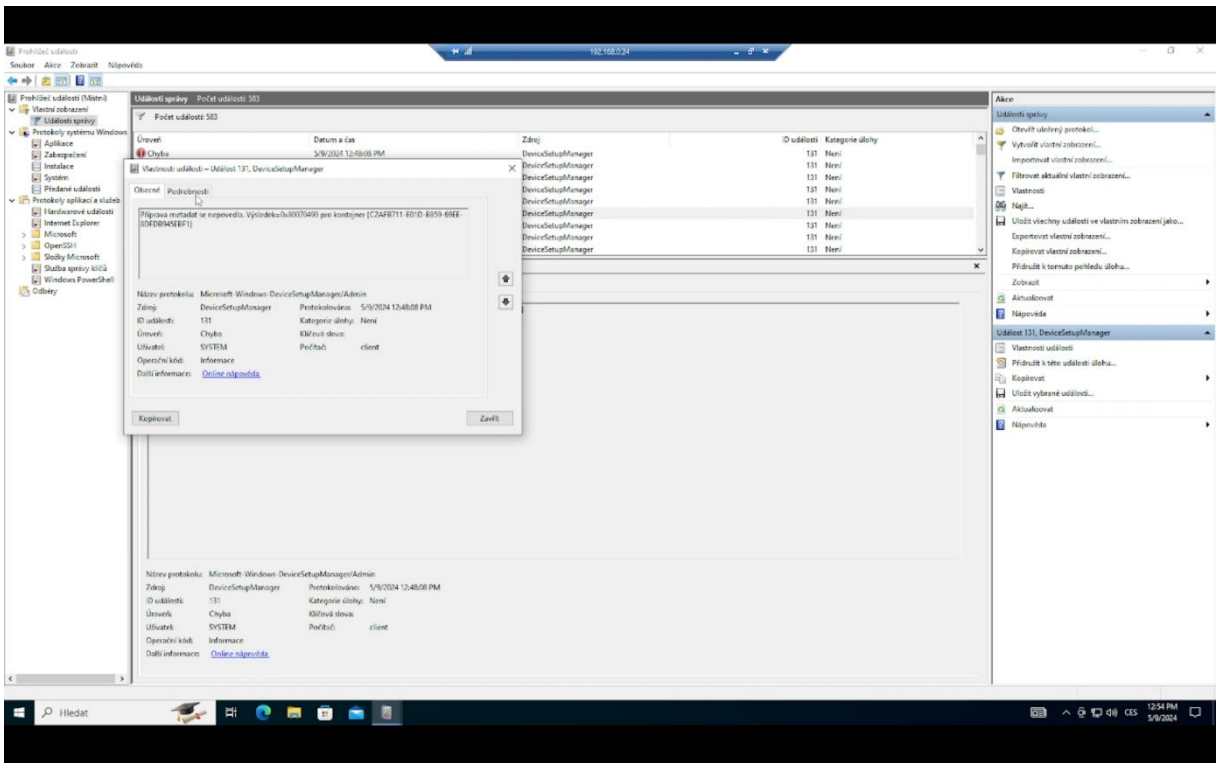
Obr. 5 Prohlížeč událostí s otevřeným Protokoly aplikací a služeb. Zdroj: vlastní zpracování

V záložce „Odběry“ se mohou ukládat události z jiných stanic, pokud je nastavena na sběr událostí. Tímto jsme si vysvětlili rozdělení kategorií protokolů v levém okně a dále si podrobněji ukážeme jednotlivé události a práci s nimi. Události jsou rozděleny do 5 kategorií: Informační, Upozornění, Chyby, Kritické a Audit viz Obrázek 6. Události informačního typu slouží k zaznamenávání běžných informací o provozu aplikací nebo systému. Tento typ události poskytuje obecné informace o běhu aplikace nebo úspěšně dokončených operacích. Události varování naznačují potenciální problémy nebo situace, které by mohly vyžadovat pozornost. Tyto události nejsou kritické, ale mohou naznačovat možný vývoj nebo nesprávnou konfiguraci. Události chybového typu označují skutečné chyby nebo selhání operace. Tento typ události je důležitý pro diagnostiku a opravu problémů v aplikacích nebo systému. Kritické události označují závažné chyby, které mohou mít významný dopad na provoz systému nebo aplikace. Tyto události vyžadují okamžitou pozornost a řešení. Události auditování jsou zaměřeny na sledování činnosti a událostí pro účely bezpečnosti a monitorování. Tento typ události může zahrnovat záznamy o přihlášení, pokusech o přístup nebo dalších akcích uživatelů.



Obr. 6 Typy událostí. Zdroj: vlastní zpracování

Ukážeme si teď jeden příklad, jak zobrazit podrobnosti konkrétní události. Vybereme konkrétní událost, která nás zajímá. Po rozkliknutí se otevře tabulka. Vidíme zde stručný Popis události, Zdroj, ID události, Typ události a Čas vzniku události. Pokud chceme o této události zjistit více, můžeme kliknout na online nápovědu nebo do internetového prohlížeče zkopírovat Zdroj události a ID události viz Obrázek 7.

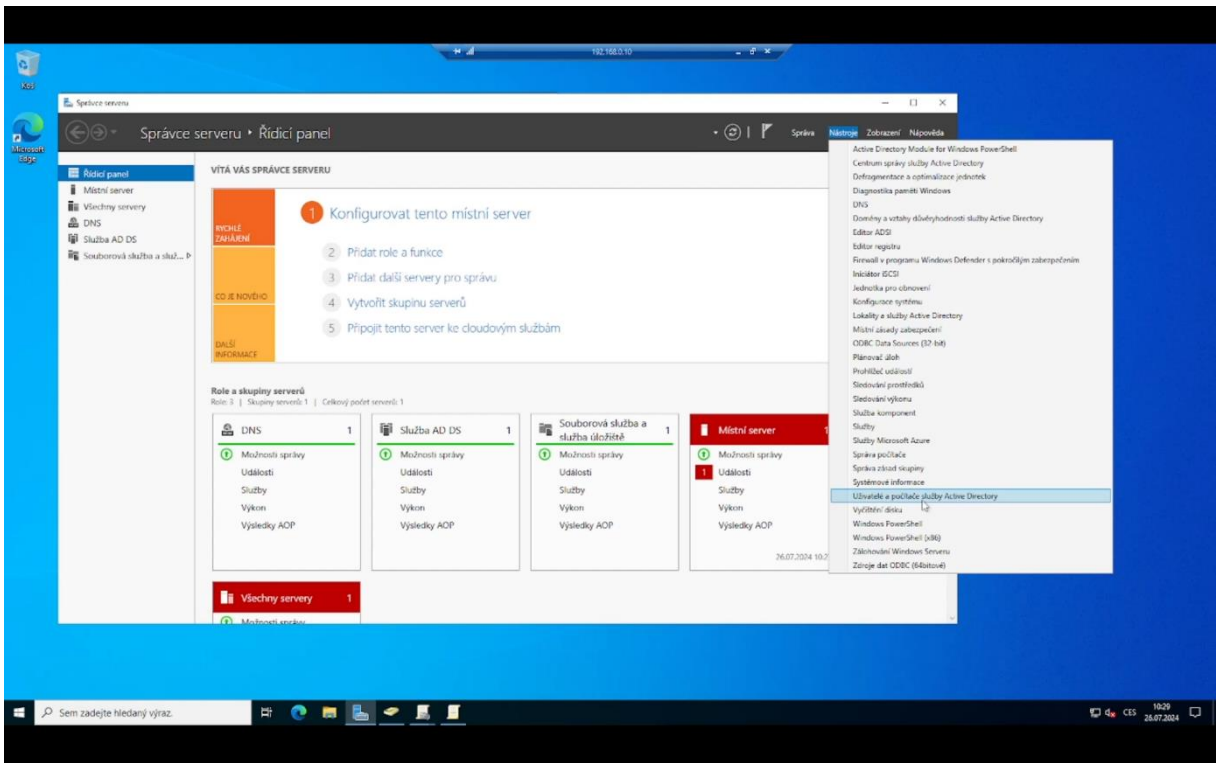


Obr. 7 Prohlížeč událost s otevřenou konkrétní událostí. Zdroj: vlastní zpracování

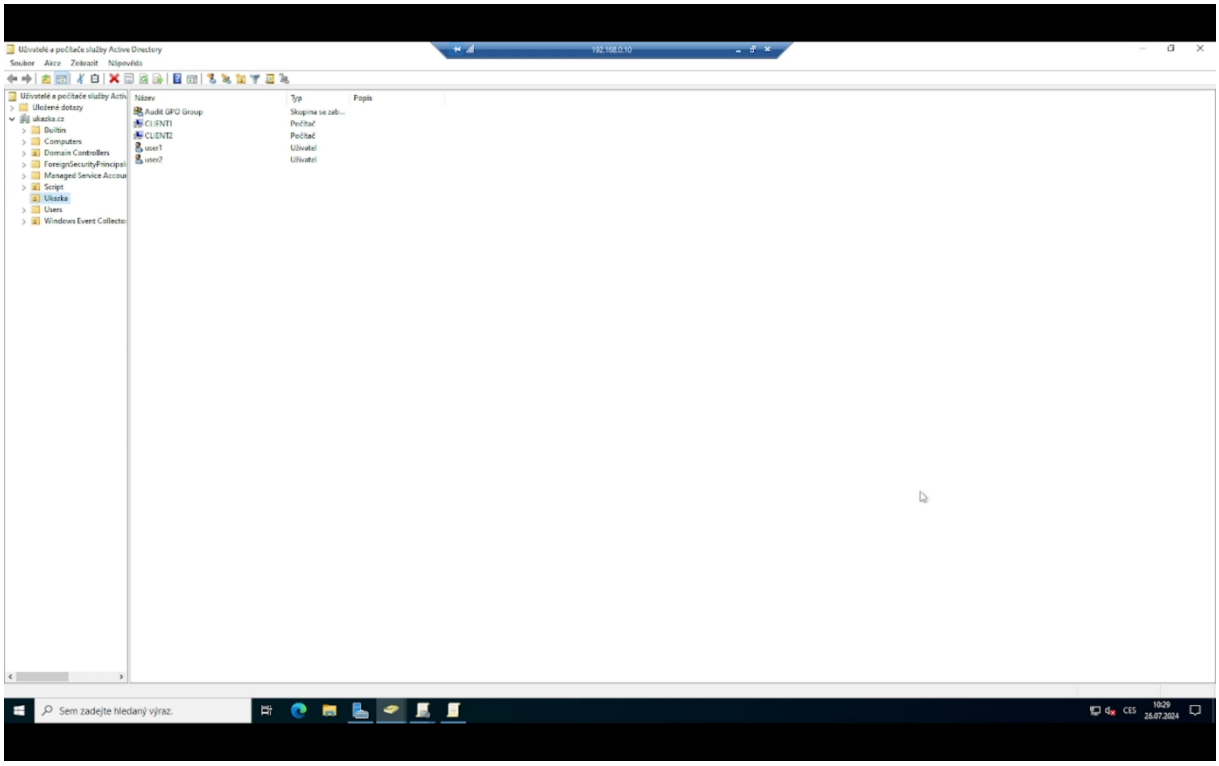
8.2 Video 2

Nastavení auditovací politiky ve Windows Active Directory je důležitým krokem k zabezpečení a správě našeho IT prostředí. Správně nastavená auditovací politika nám pomůže sledovat a zaznamenávat klíčové akce, což může být užitečné při detekci a reakci na bezpečnostní incidenty. Ukážeme si kroky a doporučení pro nastavení auditovací politiky ve Windows Active Directory.

Máme připraven server, na které běží Active Directory a další dva uživatelské počítače, které jsou do této domény připojeny. První, na co se podíváme, je v okně Správce serveru nástroj „Uživatelé a počítače služby Active Directory“ viz Obrázek 8. Vidíme zde organizační jednotku „Ukázka“, která obsahuje uživatelské počítače, uživatelské účty a uživatelskou skupinu viz Obrázek 9.



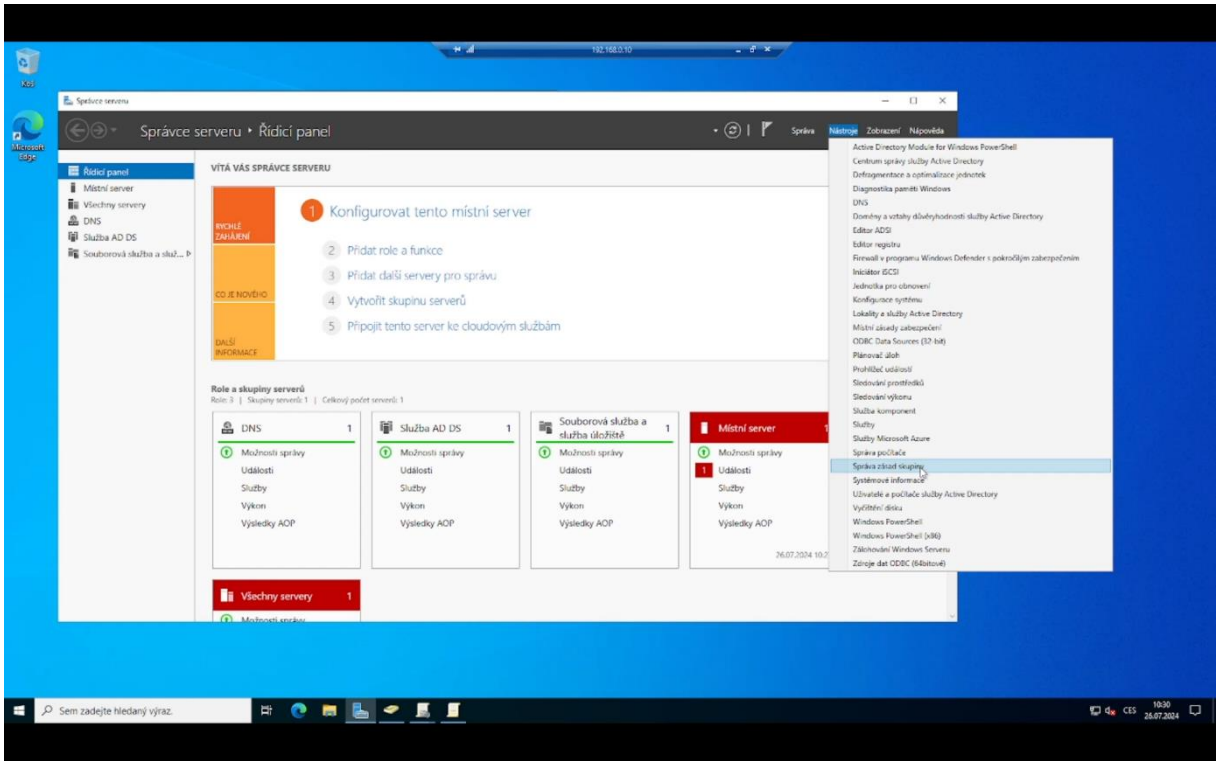
Obr. 8 Správce serveru – výběr Uživatelé a počítače služby Active Directory . Zdroj: vlastní zpracování



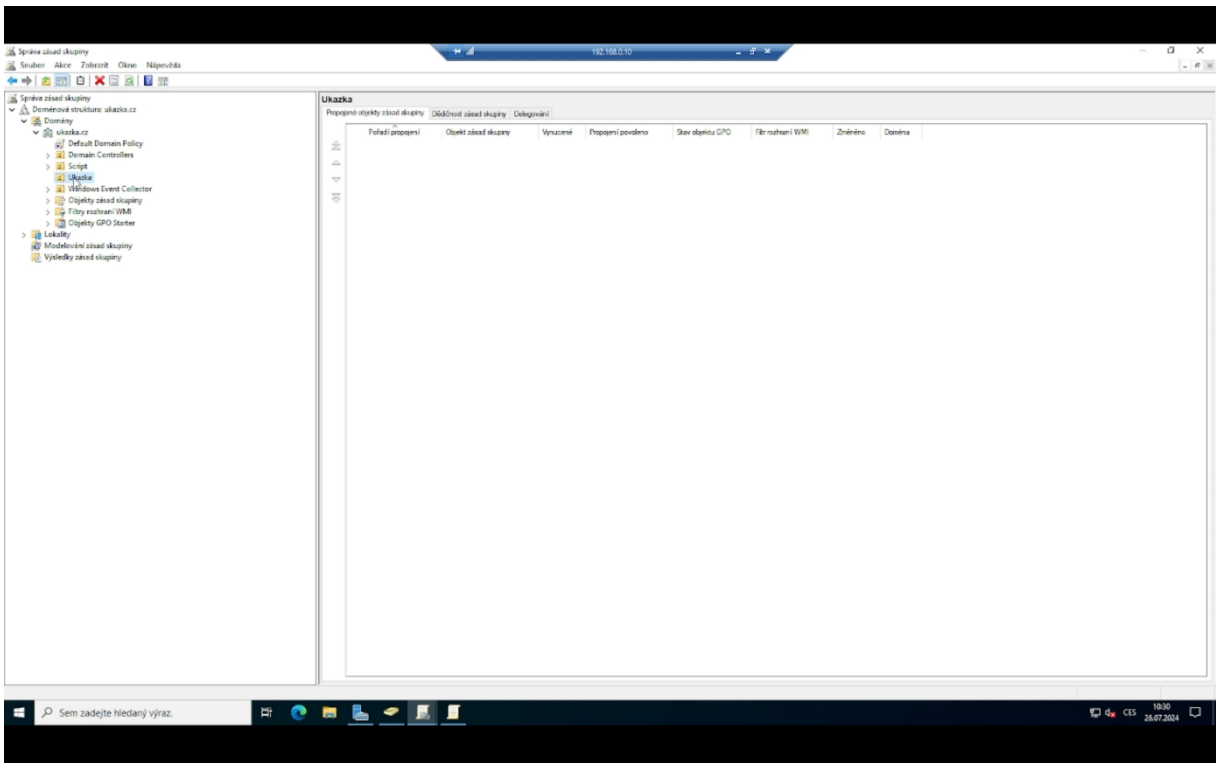
Obr. 9 Organizační jednotka - Ukazka. Zdroj: vlastní zpracování

Vrátíme se do „Správce serveru“, kde otevřeme nástroj „Správa zásad skupiny“ viz Obrázek 10. V záložce „Domény“ rozklikneme položku „Ukázka.cz“. V ní se nachází

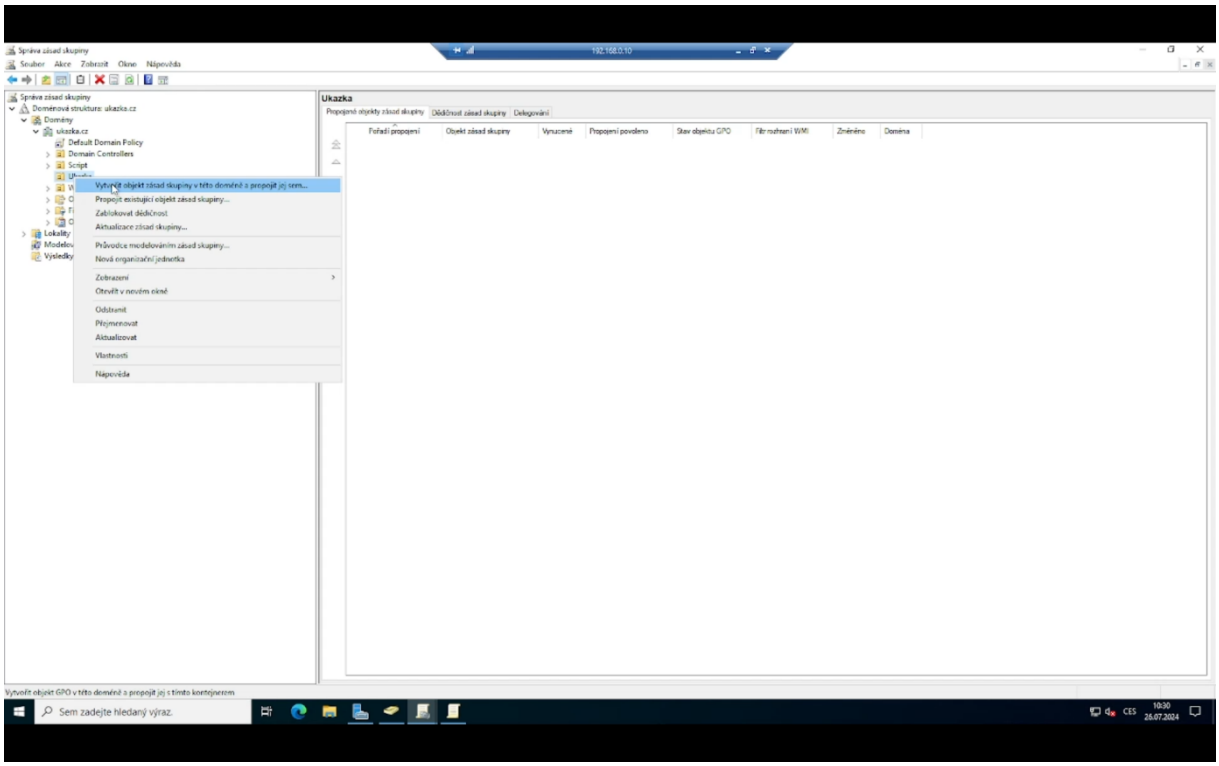
organizační jednotka „Ukázka“ viz Obrázek 11, kterou jsme si před chvílí ukázali. V této organizační jednotce vytvoříme nové GPO viz Obrázek 12 s názvem „Audit GPO“ viz Obrázek 13 a budeme jej následně editovat. To provedeme tak, že na položku „Audit GPO“ klikneme pravým tlačítkem myši a zvolíme „Upravit“ viz Obrázek 14. Otevře se nové okno, ve kterém můžeme editovat politiku. V záložce „Konfigurace počítače“ zvolíme „Zásady“, „Nastavení systému windows“, „Nastavení zabezpečení“, „Upřesnit konfiguraci zásad auditování“, „Zásady auditování“.



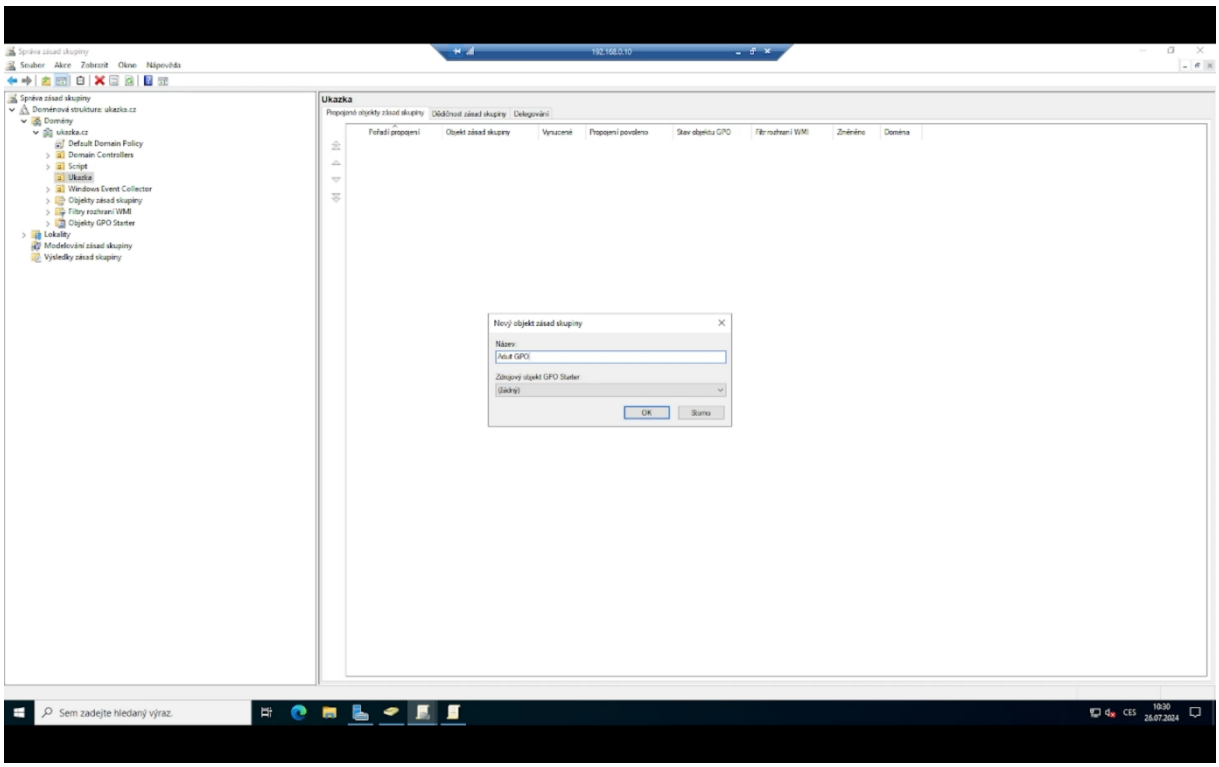
Obr. 20 Správce serveru – Správa zásad skupiny. Zdroj: vlastní zpracování



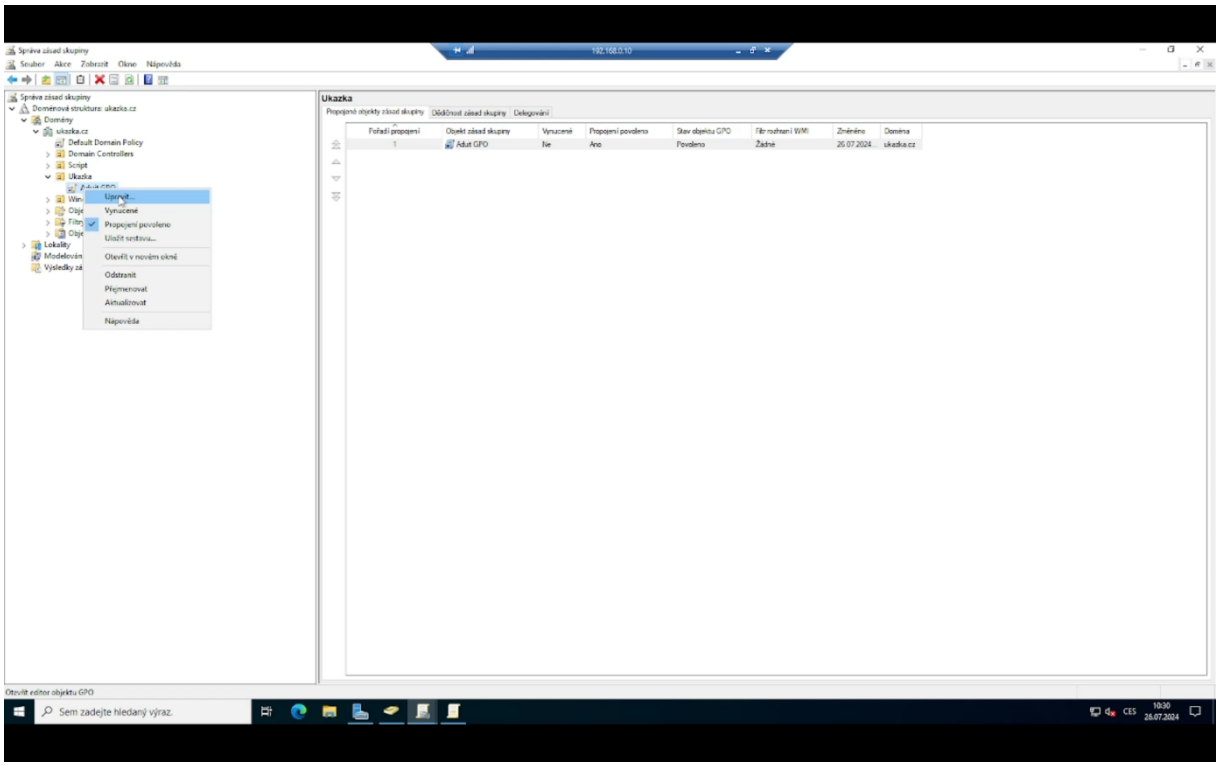
Obr. 31 Výběr organizační jednotky Ukazka. Zdroj: vlastní zpracování



Obr. 42 Vytváření GPO v organizační jednotce Ukazka. Zdroj: vlastní zpracování

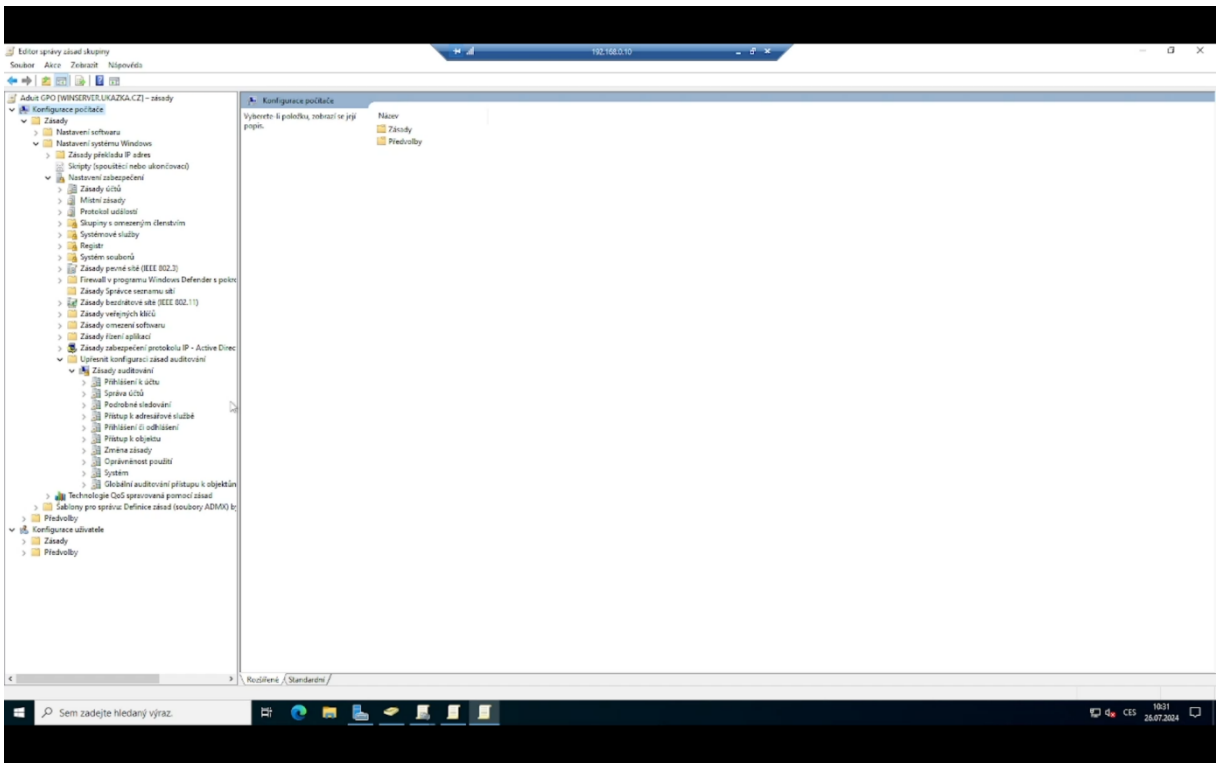


Obr. 53 Pojmenování GPO, Audit GPO. Zdroj: vlastní zpracování



Obr. 64 Upravování GPO – Audit GPO. Zdroj: vlastní zpracování

Ukážeme si několik nejdůležitějších politik viz Obrázek 15. První z nich je významná pro sledování změn v přístupech a oprávněních. Jmenuje se „Auditovat správu účtů uživatelů“ a nachází se ve skupině „Správa účtů“.



Obr. 75 Rozbalené zásady auditování. Zdroj: vlastní zpracování

V politice „Auditovat správu účtů uživatelů“ nastavujeme možnosti auditovat změny uživatelských účtů. Například změny v nastavení uživatelského účtu, nastavení hesel, změny SID, změny oprávnění ke správě účtu. Při auditování úspěšných operací se zaznamenávají úspěšné pokusy a při auditování neúspěšných operací se zaznamenávají neúspěšné pokusy.

Další významnou politikou je „Auditovat přistup k adresářové službě“ ze skupiny „Přístup k adresářové službě“. Toto nastavení zásad umožňuje auditovat události generované při přístupu k objektu služby AD DS.

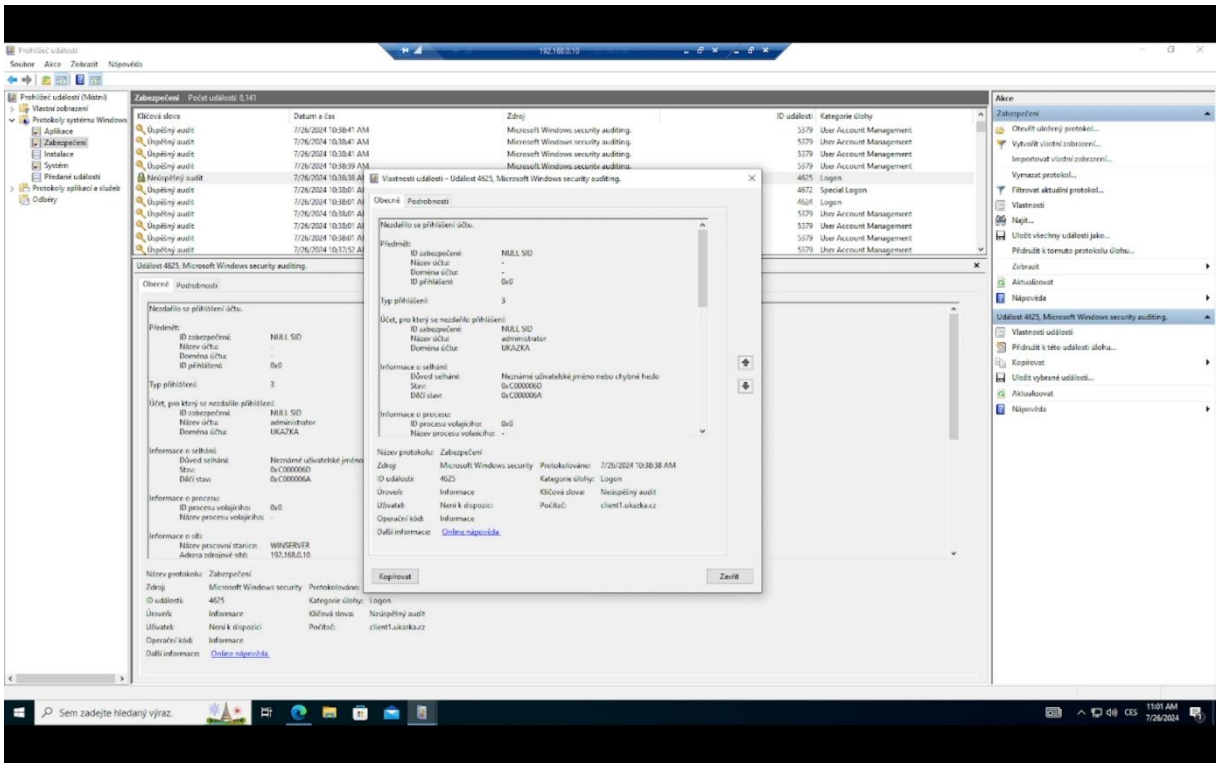
Další důležitou politikou je „Auditovat systém souborů“ ve skupině „Přistup k objektu“. Umožňuje nám sledovat přístupy k citlivým datům. Při konfiguraci těchto zásad, bude generována událost auditu pokaždé, když účet získá přístup k objektu systému souborů s odpovídajícím nastavením seznamu SACL. Při auditování úspěšných operací se zaznamenávají úspěšné pokusy a při auditování neúspěšných operací se zaznamenávají neúspěšné pokusy.

Další příklad významné politiky je „Auditovat změny zásad auditování“ v záložce „Změna zásady“. Sleduje změny, které mohou ovlivnit bezpečnost celého systému. Audituje změny v nastavení zásad auditování zabezpečení, jako například: nastavení auditování v objektu Zásady auditu, změny zásad auditování systému, registrace zdrojů událostí zabezpečení a změny v nastavení auditování pro jednotlivé uživatele.

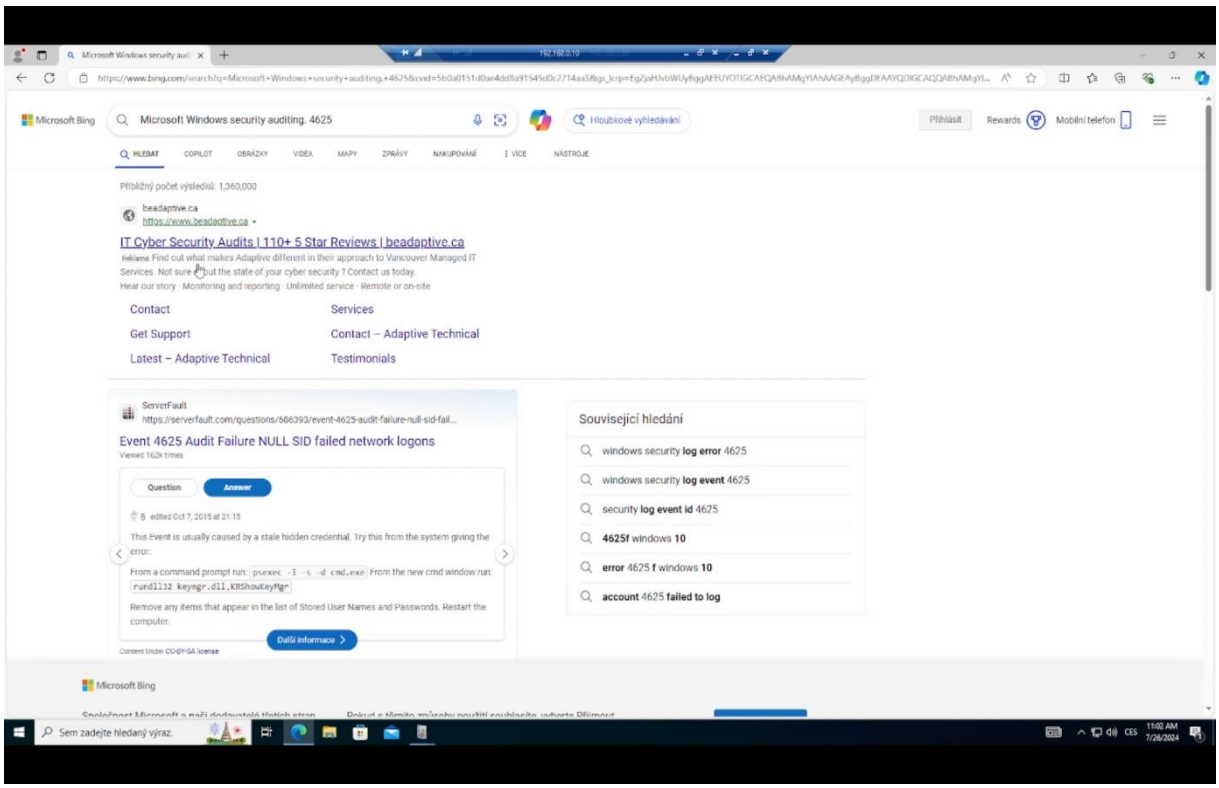
Poslední příklad politiky, který si ukážeme, je „Audit přihlášení“ v záložce „Přihlášení či odhlášení“. Sleduje úspěšné a neúspěšné pokusy o přihlášení. Tato zásada umožňuje auditovat události generované pokusy o přihlášení k uživatelským účtům v počítači. Mezi události patří „Úspěšné pokusy o přihlášení“ nebo „Neúspěšné pokusy o přihlášení“.

Po nastavení potřebných politik okno můžeme zavřít.

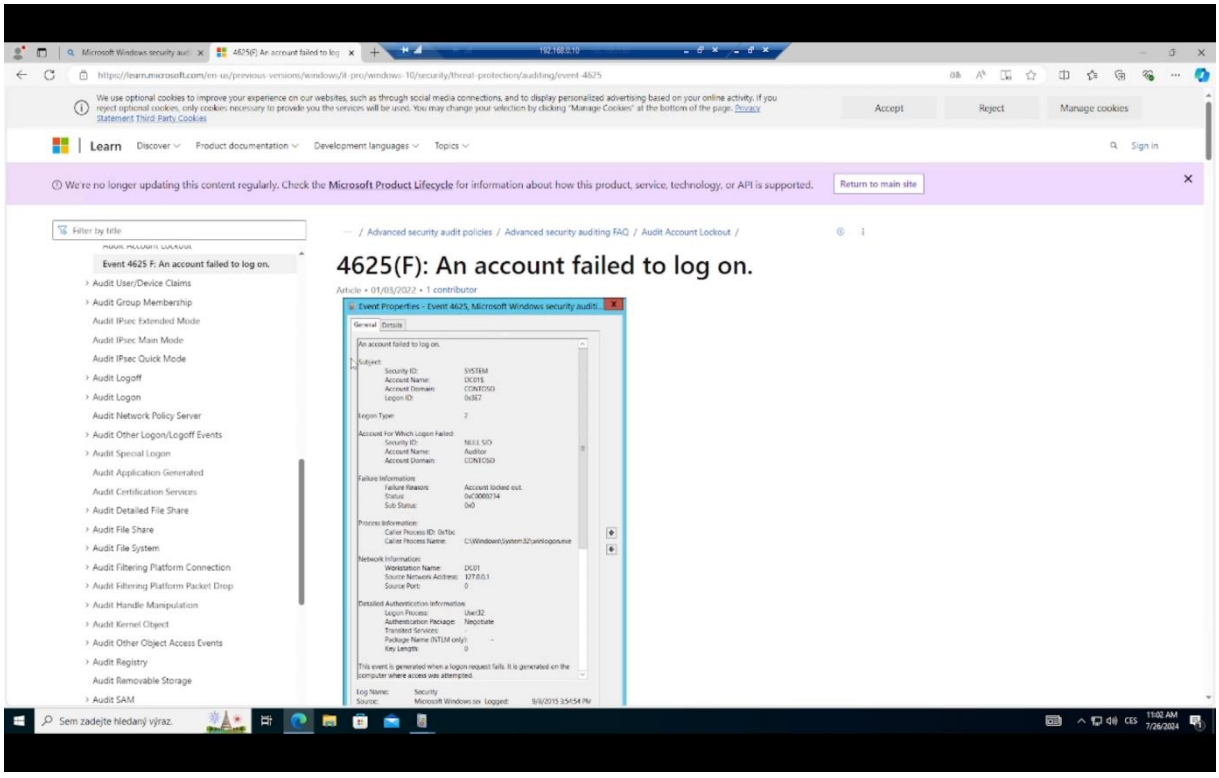
Dále se podíváme na jeden z uživatelských počítačů. Při přihlašování se párkrát přihlásím chybně. Po správném přihlášení otevřeme Prohlížeč událostí. Dále půjdeme do záložky „Protokoly systému Windows“. Zde uvidíme úspěšné a neúspěšné Audity. Na ukázku si vybereme neúspěšný audit o pokus o přihlášení. Rozklikneme „událost“. V popisu události je vidět, že jsem se pokoušel přihlásit účtem „administrátor“ a zadal jsem špatné jméno nebo heslo. Dále vidíme, že jsem se přihlašoval z počítače s touto IP adresou viz Obrázek 16. Pokud by se jednalo o nějakou pro nás neznámou událost, otevřeme internetový prohlížeč a do vyhledávacího řádku zkopírujeme zdroj a ID události. Internetový prohlížeč najde dokumentaci, kde najdeme vysvětlující popis události viz Obrázek 17 a 18.



Obr. 86 Rozbalený Prohlížeč událostí – konkrétní událost podrobněji. Zdroj: vlastní zpracování



Obr. 97 Vyhledávání konkrétní události 1. Zdroj: vlastní zpracování



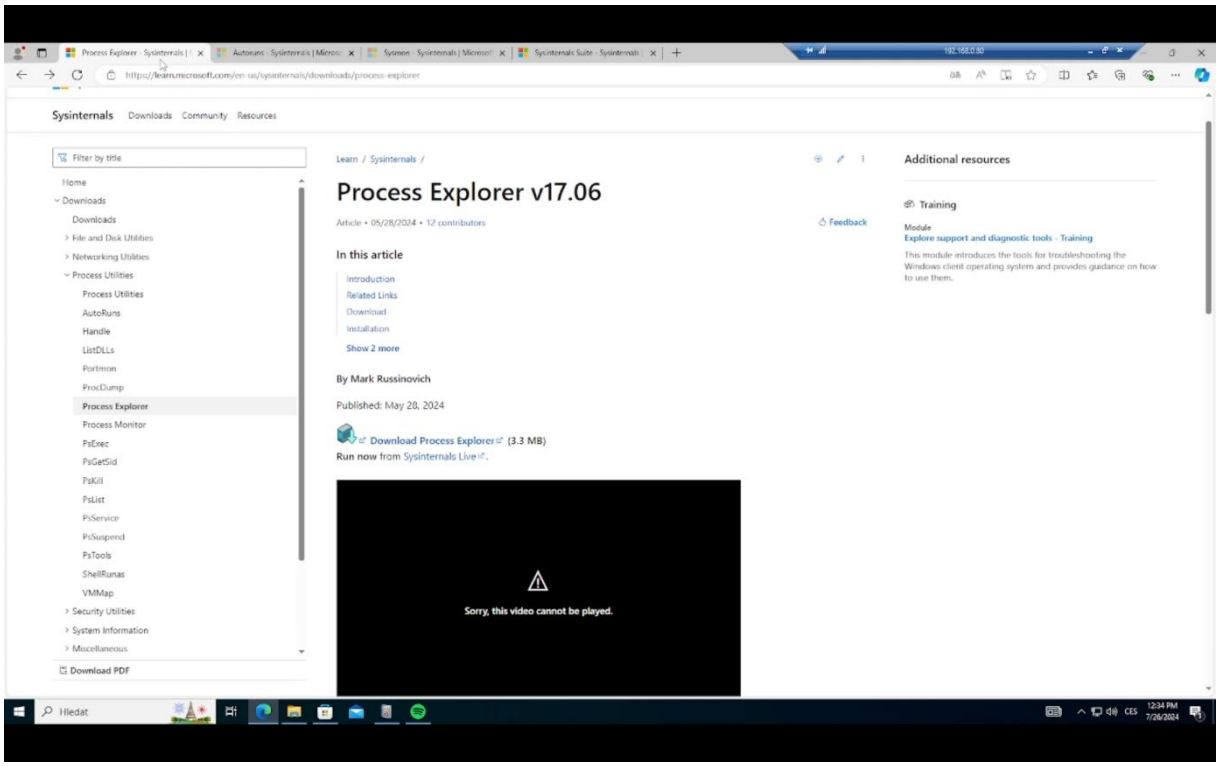
Obr. 108 Vyhledávání konkrétní události 2. Zdroj: vlastní zpracování

8.3 Video 3

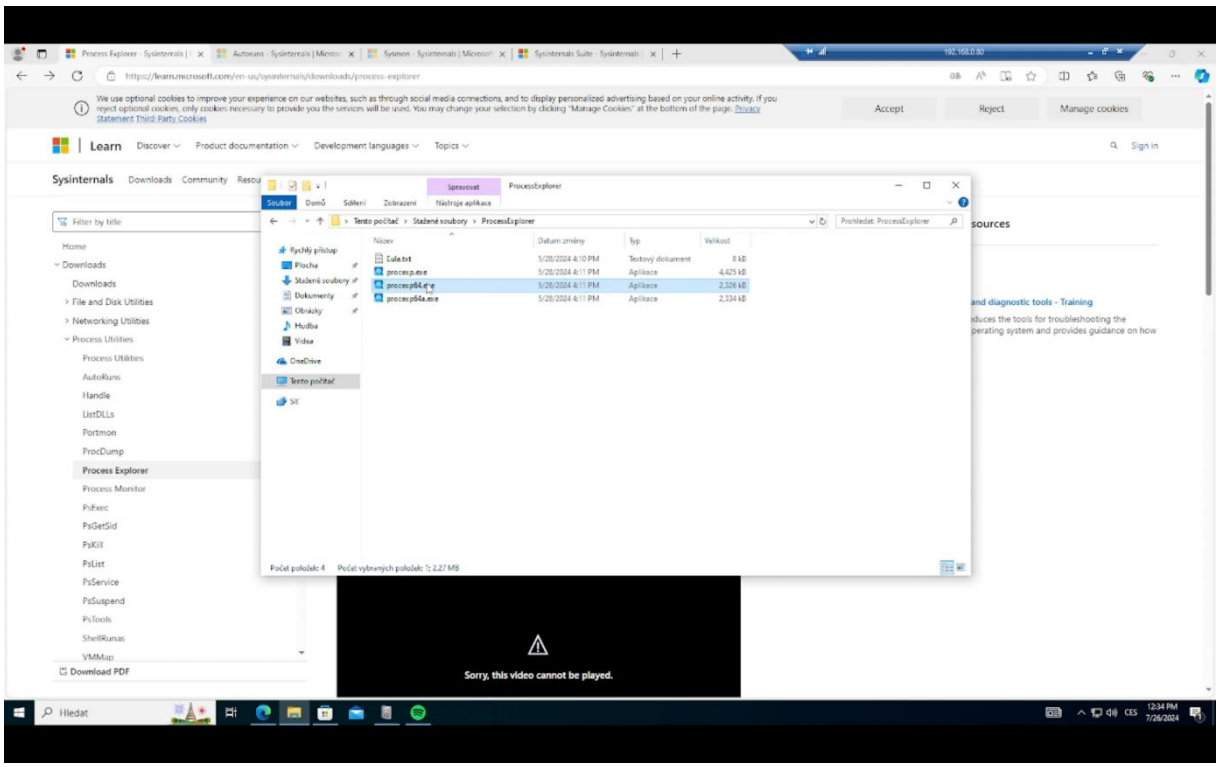
Využití Sysinternals nástrojů.

První nástroj, který nás bude zajímat, je Process Explorer. Poskytuje detailní pohled na všechny běžící procesy a jejich související zdroje v systému.

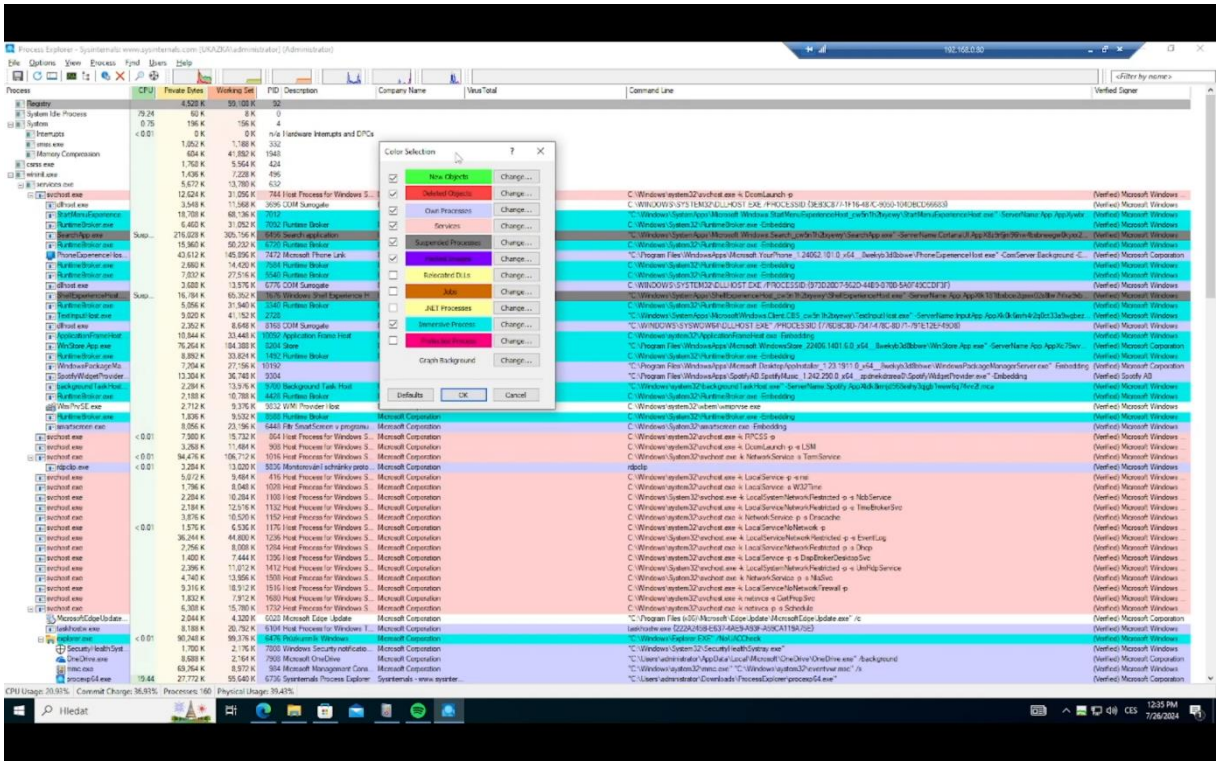
Tento nástroj stáhneme na oficiálních stránkách Microsoftu a rozbalíme viz Obrázek 19. Spustíme program procexp64 s administátorskými viz Obrázek 20. První, co nás zaujme v programu, je pestrost barev. Pro porozumění, co jednotlivé barvy znamenají, klikneme na Options a Configure colors viz Obrázek 21. Zobrazí se tabulka s vysvětlením významu jednotlivých barev. Ukážeme si nejčastějších z nich.



Obr. 119 Oficiální webová stránka Process Explorer. Zdroj: vlastní zpracování



Obr. 20 Rozbalený Process Expoler - spouštění aplikace procexp64.exe. Zdroj: vlastní zpracování

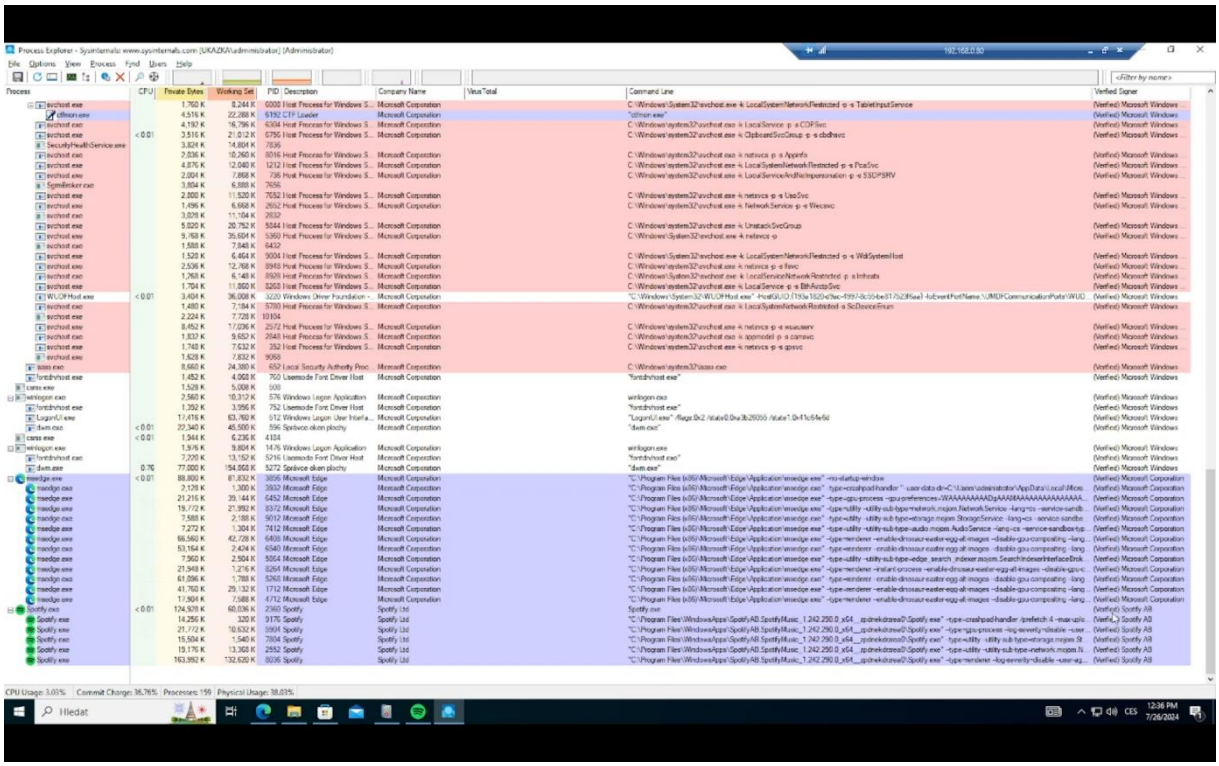


Obr. 21 Process Expoler – tabulka rozdělení barev. Zdroj: vlastní zpracování

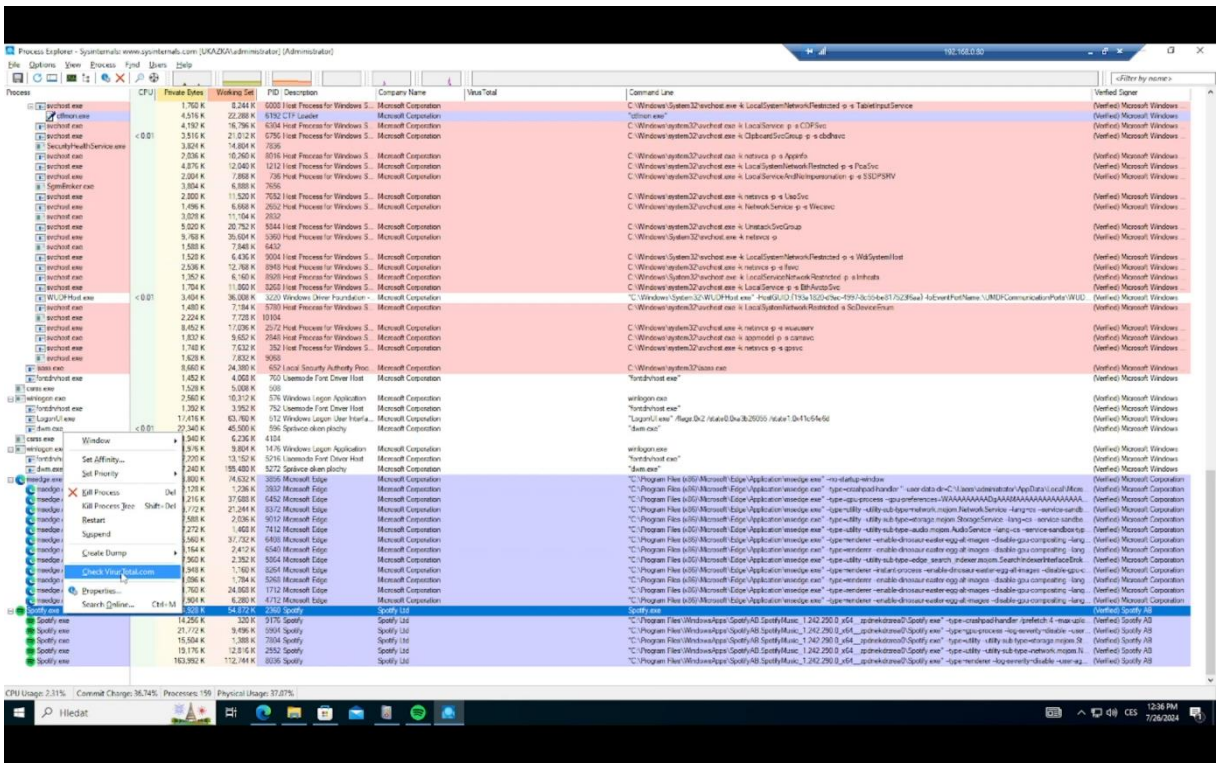
Zelená barva označuje nový proces a pomáhá tak identifikovat, které procesy byly právě zahájeny. Červeně je naopak označen proces, který se uzavírá, a ukazuje tak,

které procesy právě končí. Světle modrá ukazuje procesy, které jsou spuštěny přímo uživatelem nebo aplikacemi, které uživatel používá. Oranžová označuje procesy, které jsou spuštěny jako služba systému Windows a běží na pozadí, obvykle bez přímé interakce s uživatelem. Šedá značí procesy dočasně pozastavené, které nevyužívají systémové prostředky, dokud nejsou znovu aktivovány.

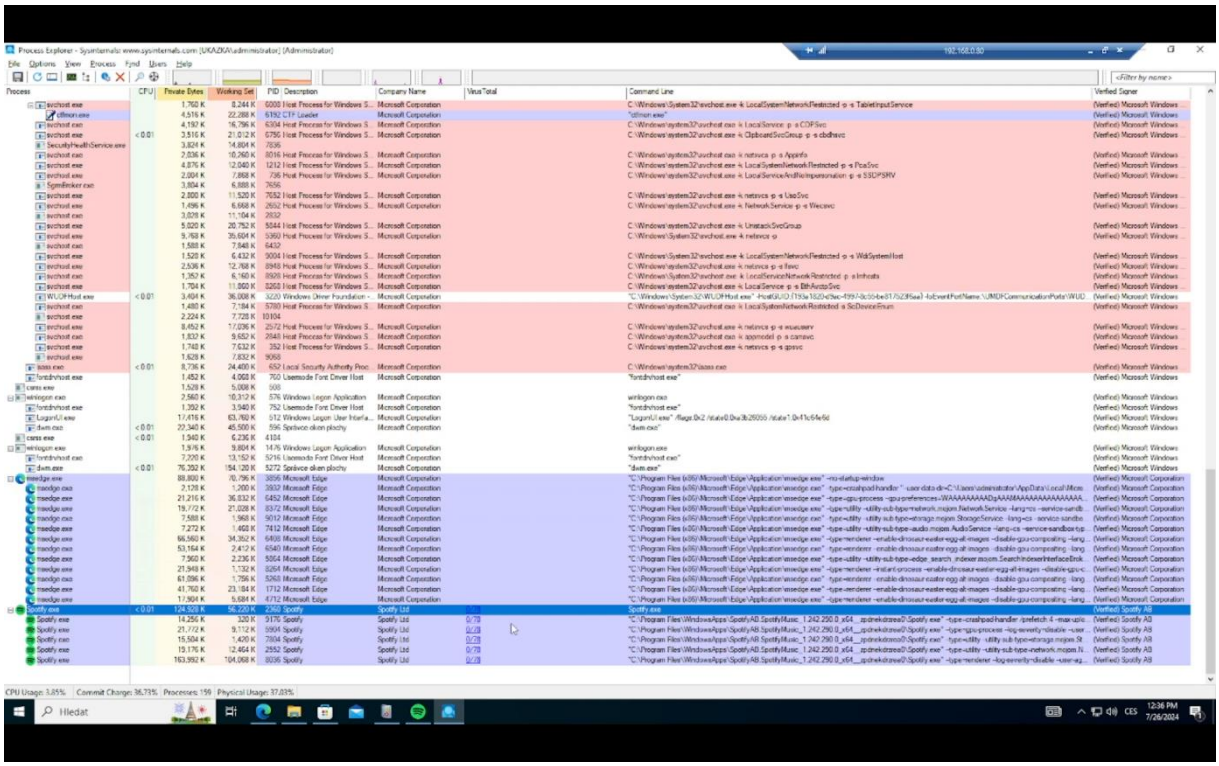
Další užitečnou vlastností Process Exploreru je, že obsahuje informace, zda procesy mají ověřené podpisy viz Obrázek 22. Což je dobrý první krok při zjišťování škodlivého programu nebo viru v počítači. Dalším důležitým krokem při hledání virů, který tento program umožňuje, je odesílání informací na VirusTotal. Ten nám odpoví, zda je zkoumaný proces potenciálně škodlivý viz Obrázek 23 a 24.



Obr. 22 Process Expoler - Ukázka ověřeného podpisu. Zdroj: vlastní zpracování



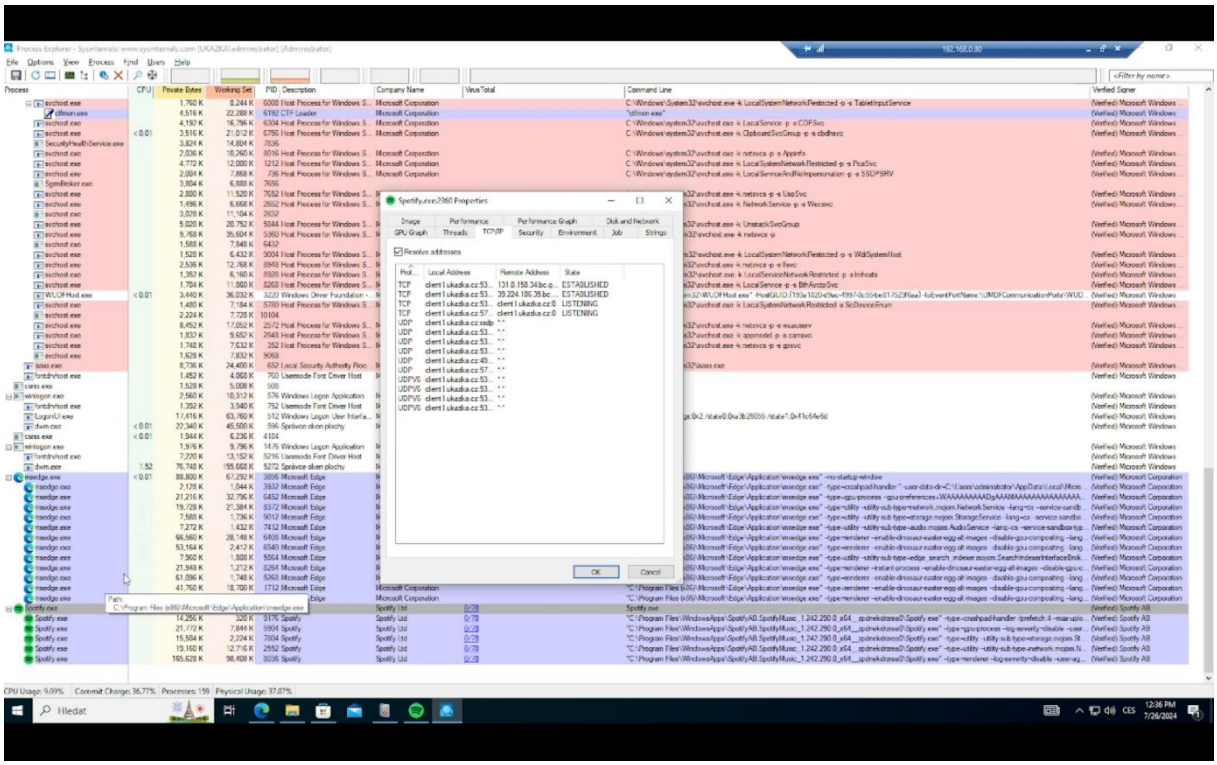
Obr. 23 Process Expoler -zasílání na VirusTotal.com. Zdroj: vlastní zpracování



Obr. 24 Process Expoler – odpověď z ViruTotal.com. Zdroj: vlastní zpracování

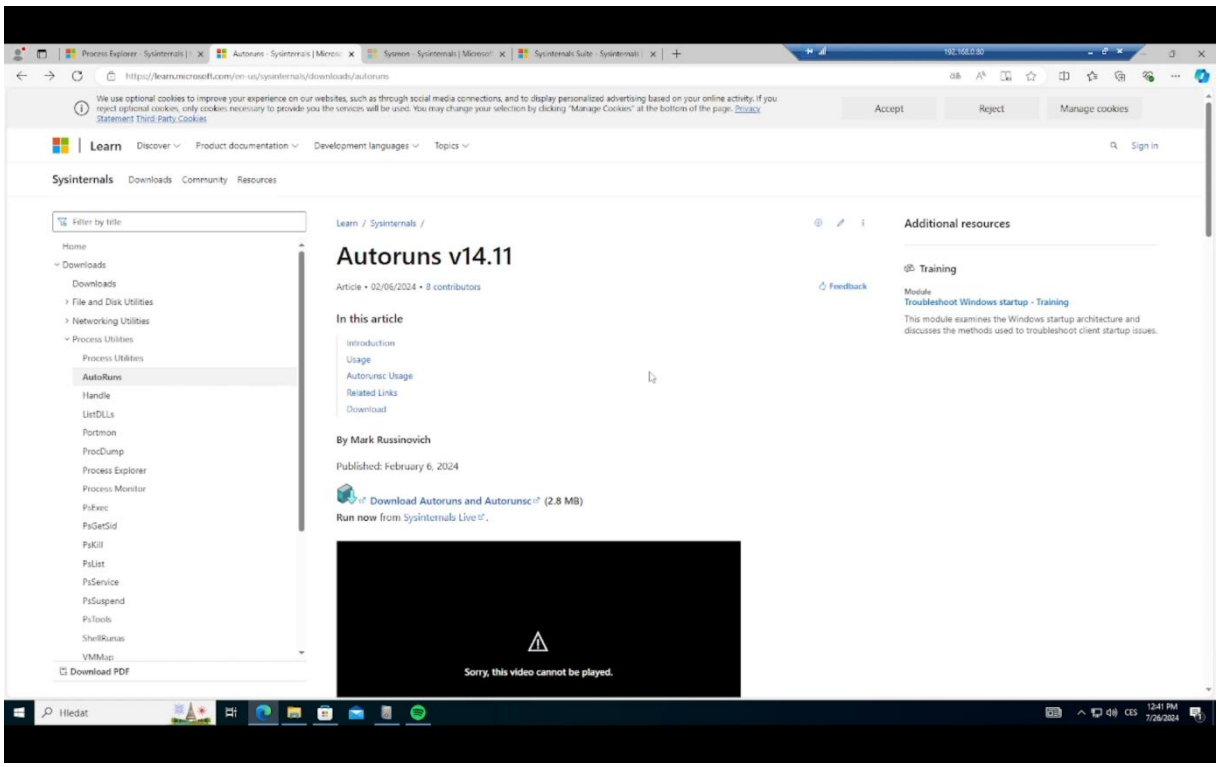
Další zajímavá funkce je zobrazení příkazového řádku, což nám umožní zjistit, s jakými parametry byl proces spuštěn. Poslední důležitá funkce tohoto nástroje, na kterou se

podíváme, je v konkrétním procesu záložka TCP/IP. Můžeme zde vidět s čím konkrétní proces komunikuje viz Obrázek 25.

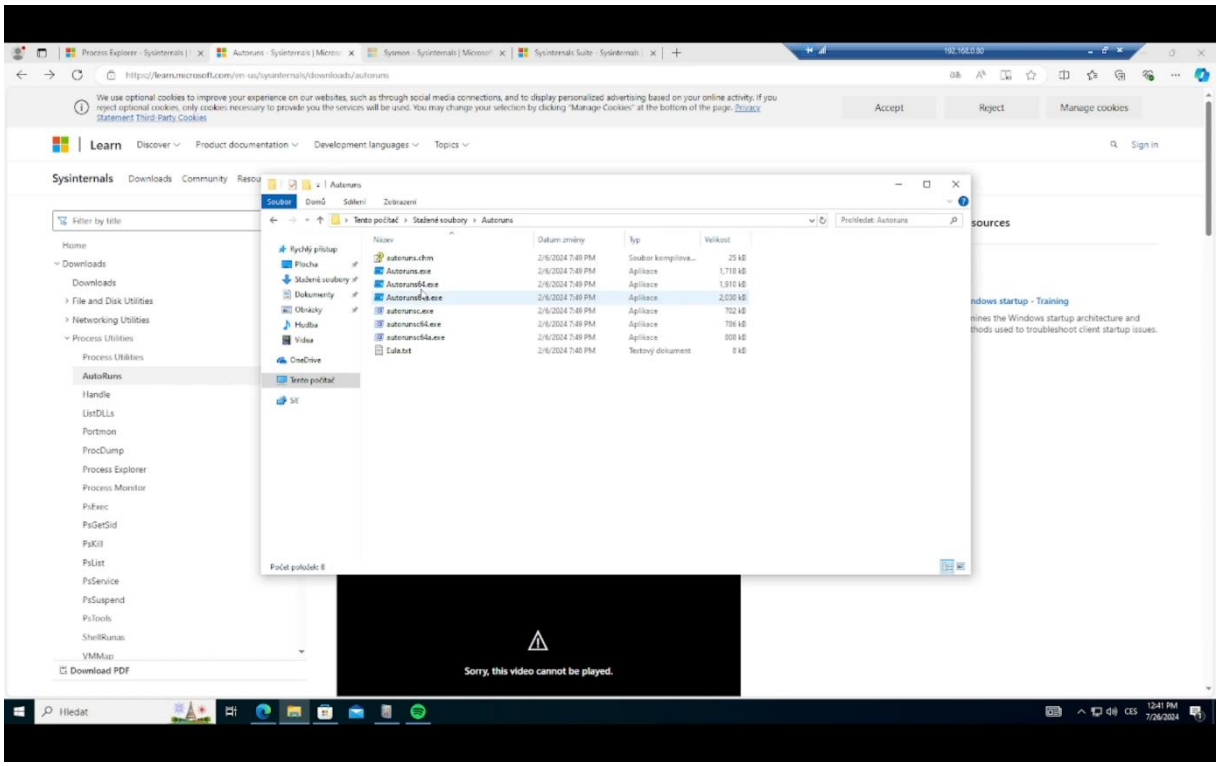


Obr. 25 Process Expoler – TCP/IP komunikace. Zdroj: vlastní zpracování

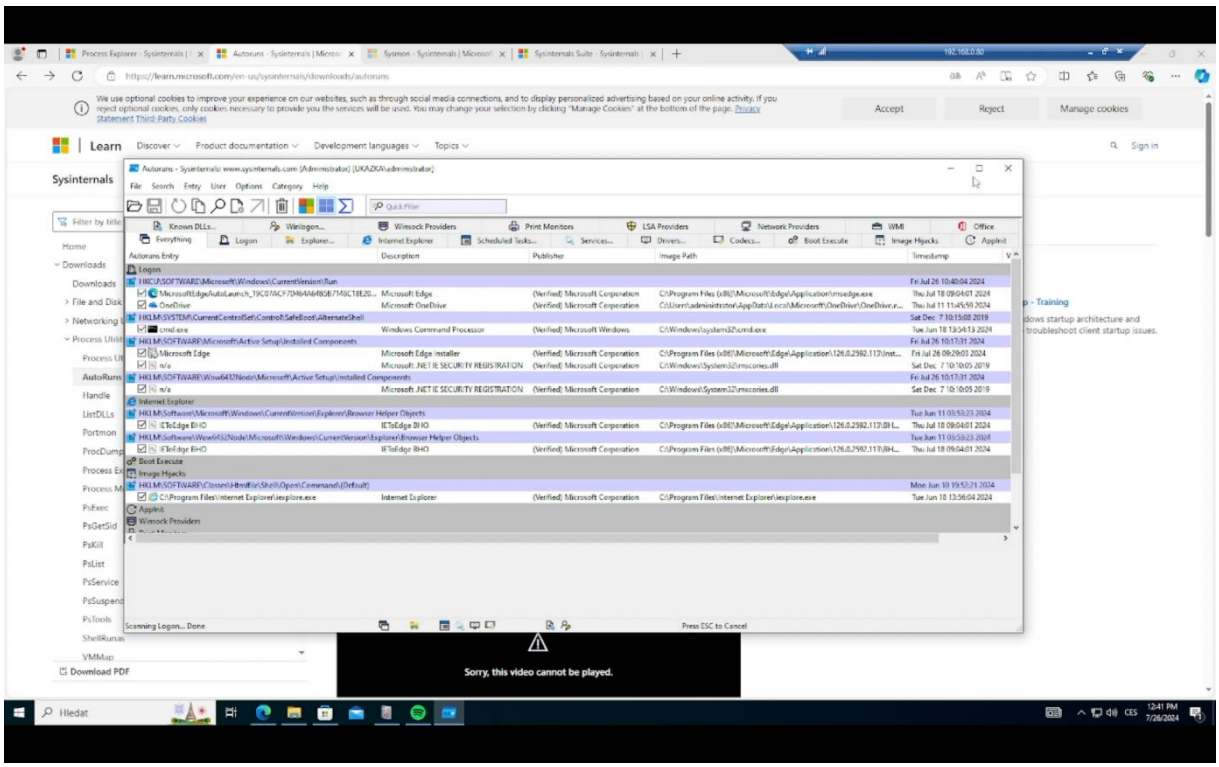
Další nástroj, který si představíme, je Autoruns. Umožňuje spravovat a zobrazovat programy, služby a další komponenty, které se automaticky spouštějí při startu systému nebo při přihlášení uživatele. Také tento nástroj stáhneme z oficiálních stránek Microsoftu, rozbalíme a spustíme s administrátorskými právy viz Obrázek 26 a 27. Zobrazí se zde jednotlivé procesy, které se spustí při jednotlivých úkonech, například při přihlášení do počítače nebo při používání internetového prohlížeče. Jednotlivé procesy zde můžeme zapínat, vypínat, kontrolovat přítomnost virů a podívat se do registrů. Také zde můžeme kontrolovat jednotlivé services a drivers viz Obrázek 28.



Obr. 26 Oficiální webová stránka Autoruns. Zdroj: vlastní zpracování

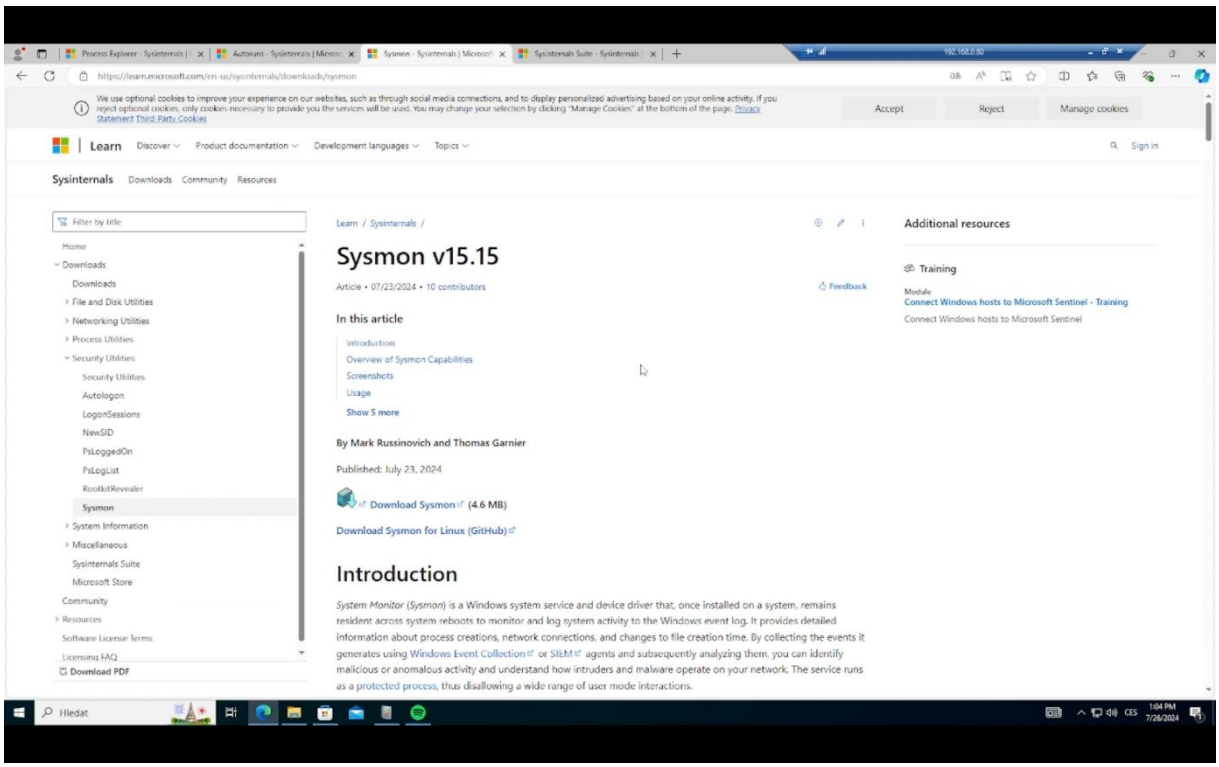


Obr. 27 Rozbalený Autoruns – spouštění Autoruns64.exe. Zdroj: vlastní zpracování

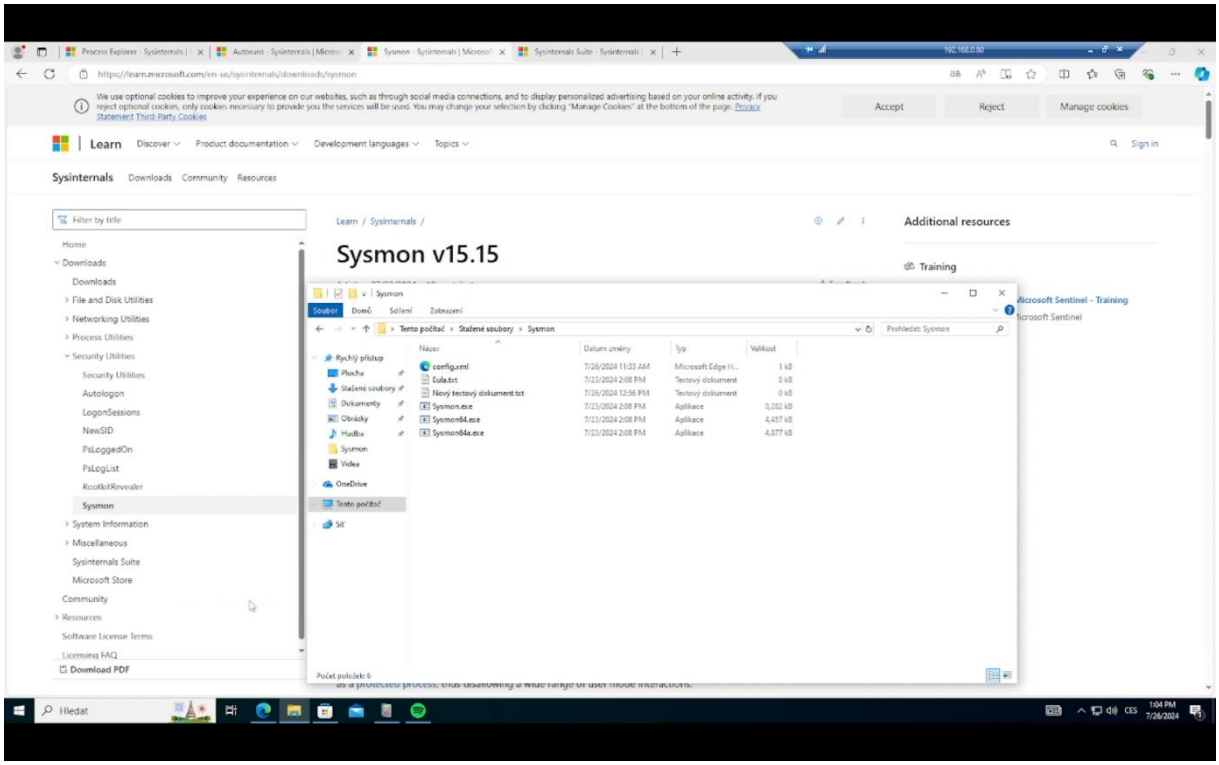


Obr. 28 Aktivní Autoruns. Zdroj: vlastní zpracování

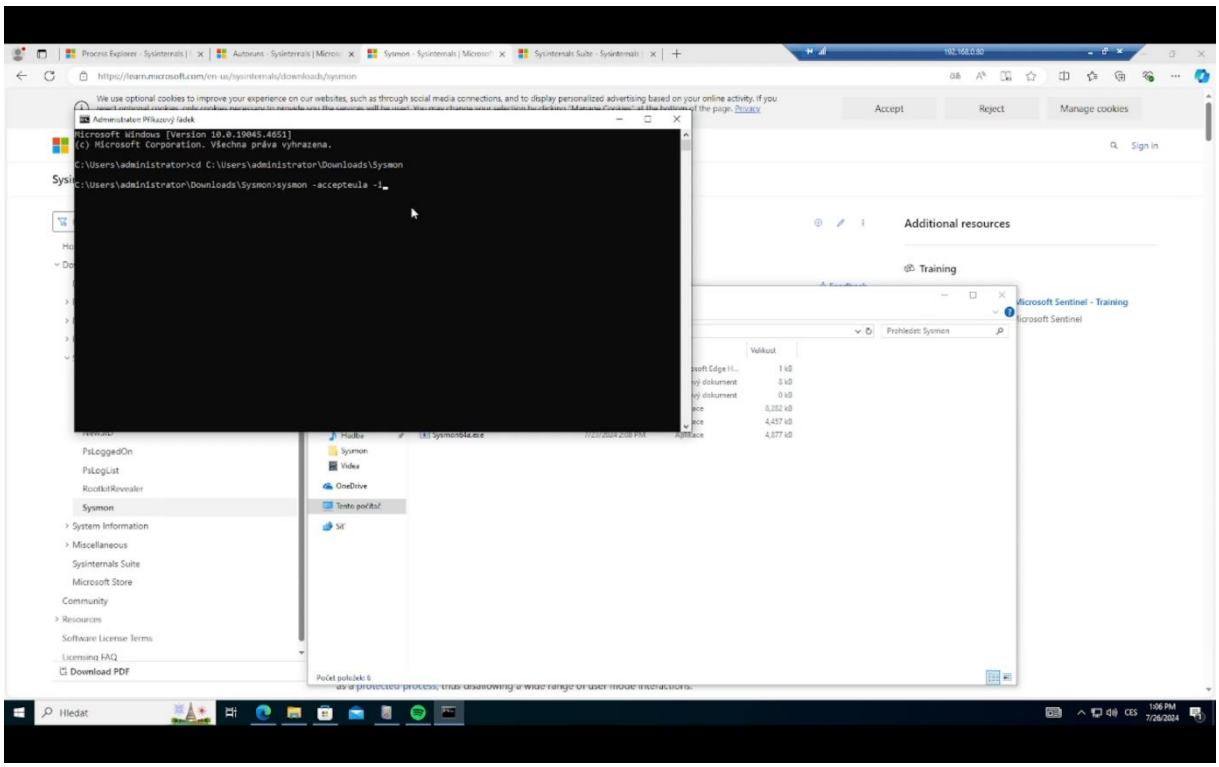
Poslední nástroj, na který se podíváme, je Sysmon. System Monitor, zkráceně Sysmon, je další z řady nástrojů vytvořený společností Microsoft pro pokročilé sledování systému. Poskytuje detailní informace o systémových událostech, což je užitečné pro detekci a diagnostiku bezpečnostních incidentů. Sysmon opět stáhneme na oficiálních stránkách Microsoftu viz Obrázek 29. Stažený soubor rozbalíme. Otevřeme příkazový řádek s administrátorskými právy. Přejdeme do adresáře, kde máme rozbalený Sysmon viz Obrázek 30. Pomocí příkazu „sysmon -accepteula -i“ viz Obrázek 31. Tímto příkazem potvrdíme eulu a nainstalujeme Sysmon. Dále vytvoříme konfigurační xml soubor pomocí jakéhokoliv textového editoru. Tento soubor bude sloužit k určení, co chceme zaznamenávat za informace.



Obr. 29 Oficiální webová stránka Sysmon. Zdroj: vlastní zpracování

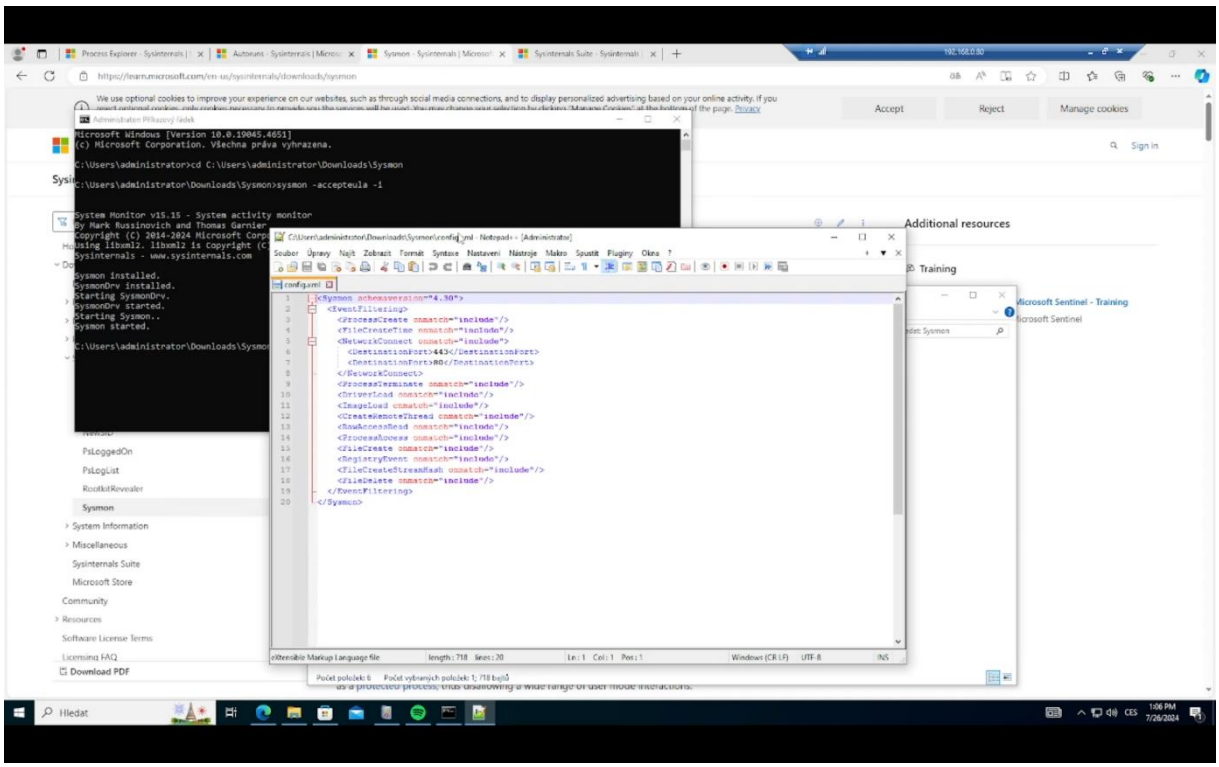


Obr. 30 Rozbalený Sysmon. Zdroj: vlastní zpracování

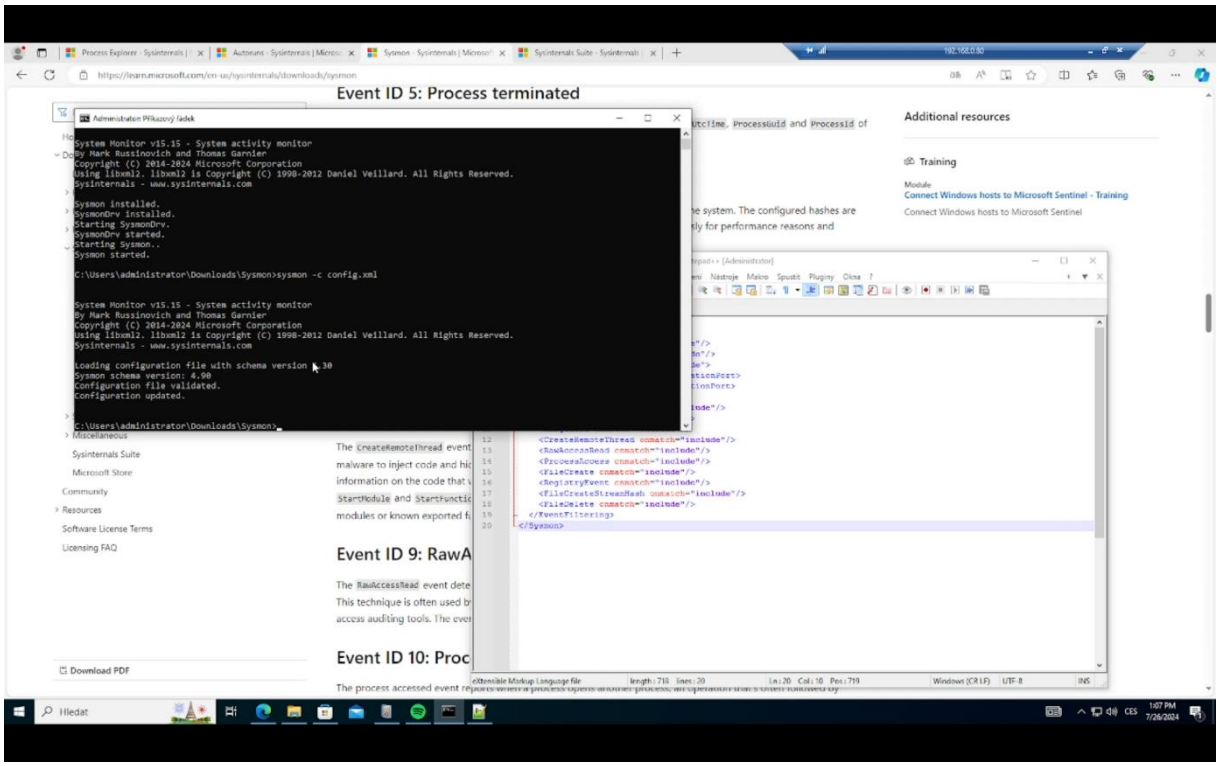


Obr. 31 Spouštění Sysmon přes příkazový řádek. Zdroj: vlastní zpracování

Na prvním řádku určíme, jakou verzi Sysmonu budeme používat. Na dalším řádku uvedeme, jaké Události chceme filtrovat. Dále pomocí dokumentace z webových stránek určíme, jaké přesné eventy chceme zaznamenávat. Můžeme nastavit, aby byly zahrnuty nebo vyloučeny ze zpracovávání. Například u NetworkConnect nastavíme, aby zaznamenávány byly pouze http a https komunikace viz Obrázek 32. Vytvořenou konfiguraci uložíme a opět v příkazovém řádku zadáme příkaz „Sysmon – c“ a náš konfigurační soubor viz Obrázek 33.



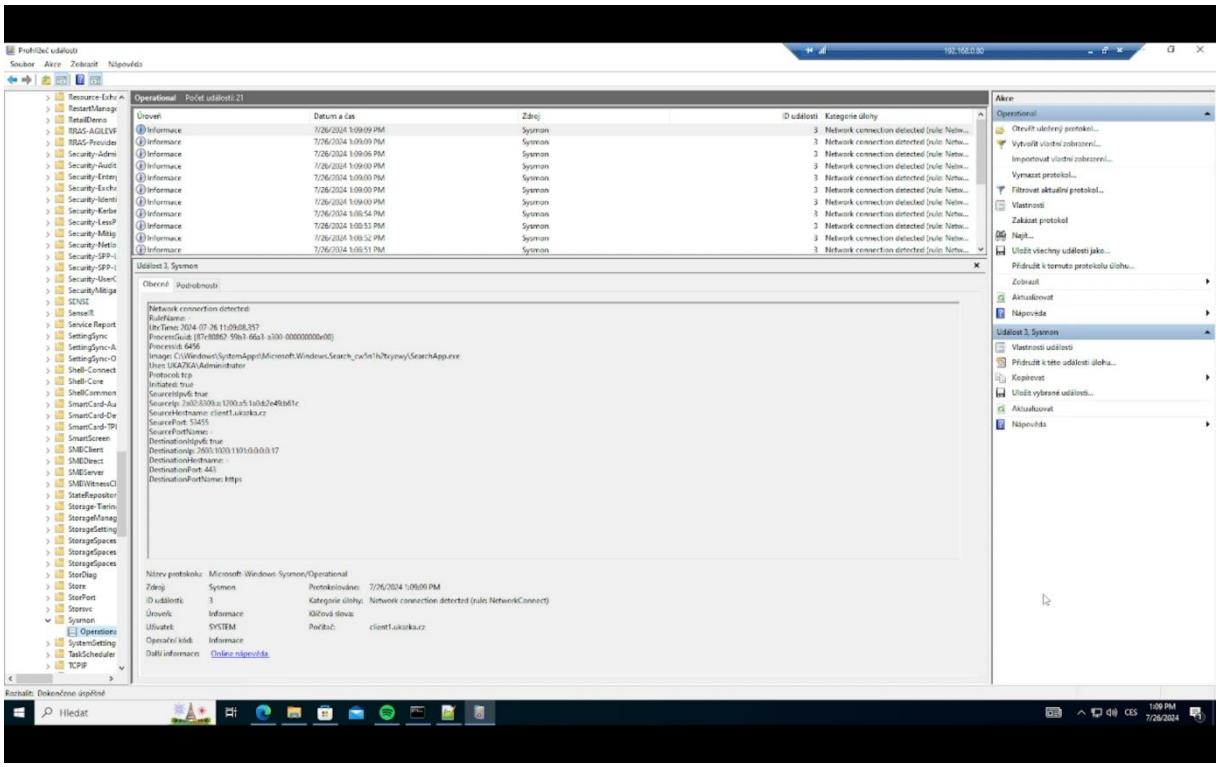
Obr. 32 XML konfigurační soubor pro Sysmon. Zdroj: vlastní zpracování



Obr. 33 Aplikování konfiguračního souboru přes Sysmon. Zdroj: vlastní zpracování

Přepneme se do prohlížeče událostí. Zde jdeme do Protokoly aplikací a služeb, Microsoft, Windows, Sysmon. Pokud se program Sysmon nainstaloval správně, tak zde

uvidíme složku Sysmon. V této složce jsou zaznamenány všechny události, které jsme v předchozím kroku nastavili v konfiguračním souboru viz Obrázek 34.

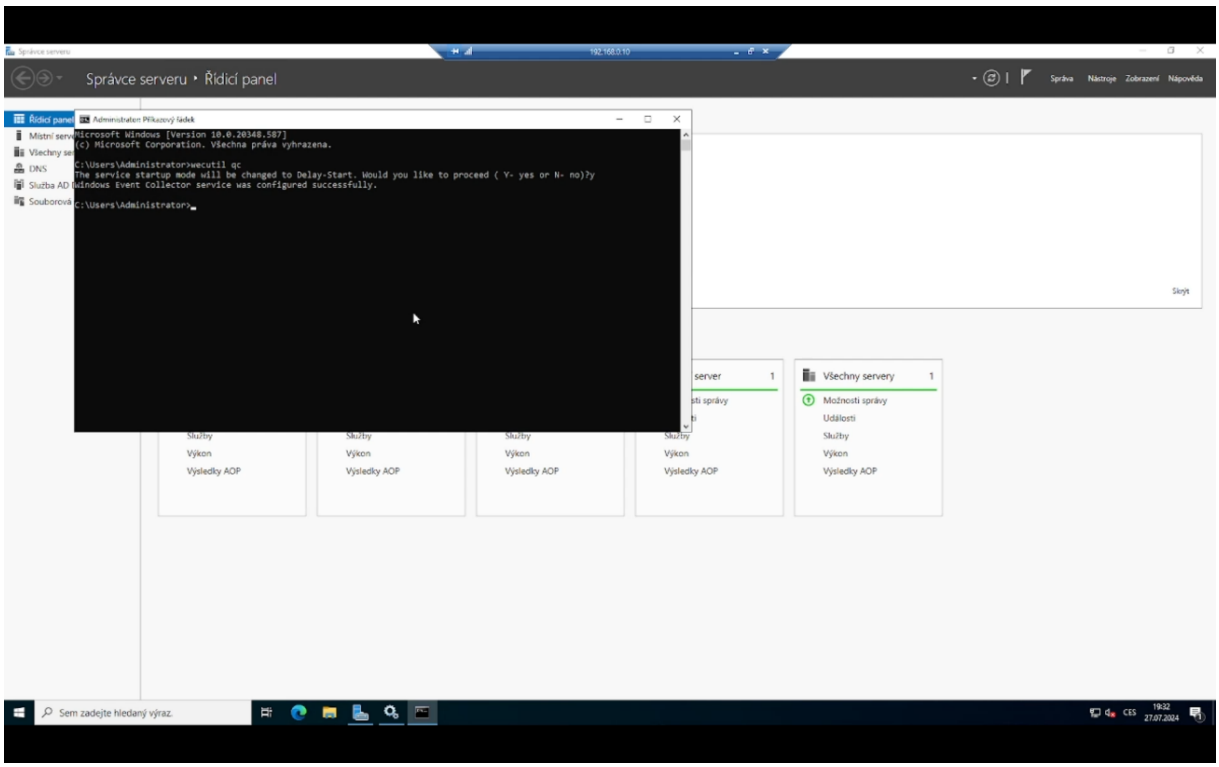


Obr. 34 Prohlížeč událostí s událostí ze Sysmon. Zdroj: vlastní zpracování

Protože neexistuje "univerzální" řešení, které by vyhovovalo všem, a každá infrastruktura je odlišná, je možné, že se po povolení Sysmonu začne produkovat nadměrné množství určitých typů událostí. Pokud dospějete k závěru, že se jedná o falešně pozitivní události, můžete tyto události v Sysmonu odfiltrovat.

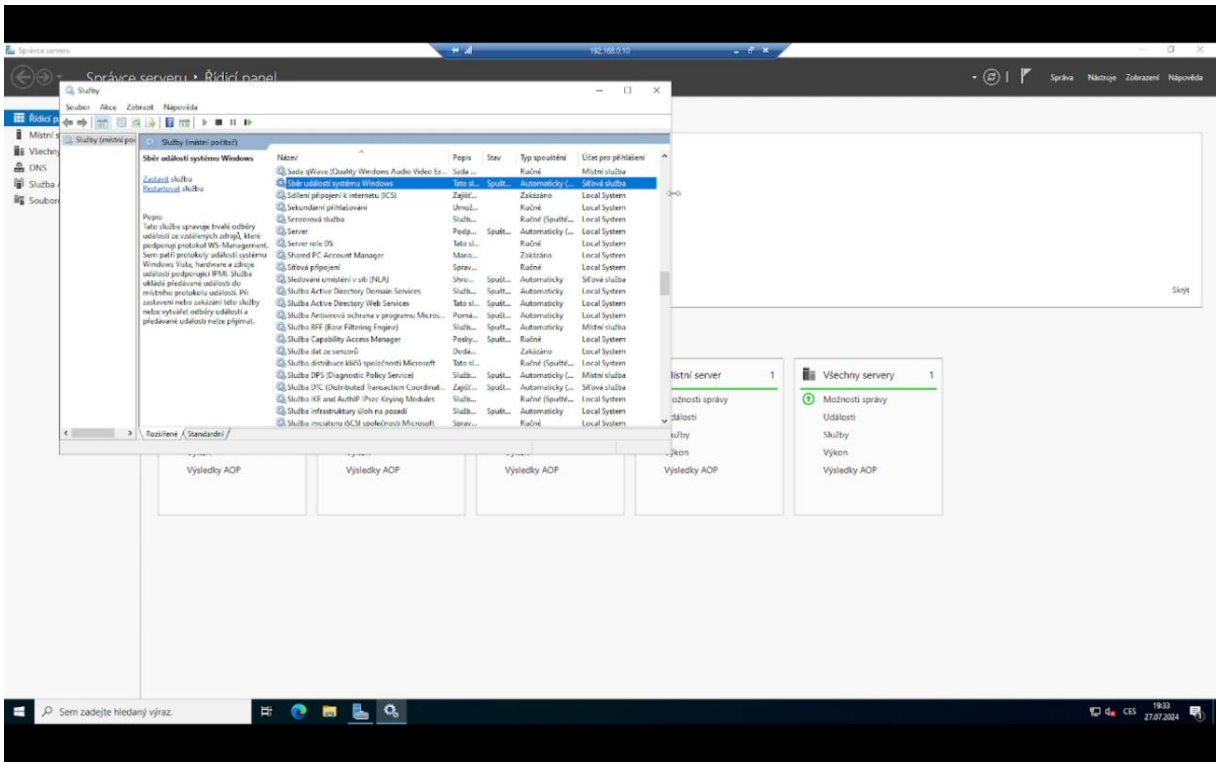
8.4 Video 4

Dvě metody ke sběru Událostí z uživatelských počítačů. Vycházíme z toho, že použijeme jeden server, na který se budou Události zasílat a dva uživatelské počítače, které budou Události odesílat, při čemž na každém z nich použijeme jiný způsob sběru. První způsob, který si ukážeme, je s použitím Windows Event Collector, jehož český název je „Sběr událostí systému Windows". Otevřeme si příkazový řádek s administrátorskými právy a napíšeme „wecutil qc" viz Obrázek 35. Tímto příkazem jsme server nastavili na přijímání Událostí.



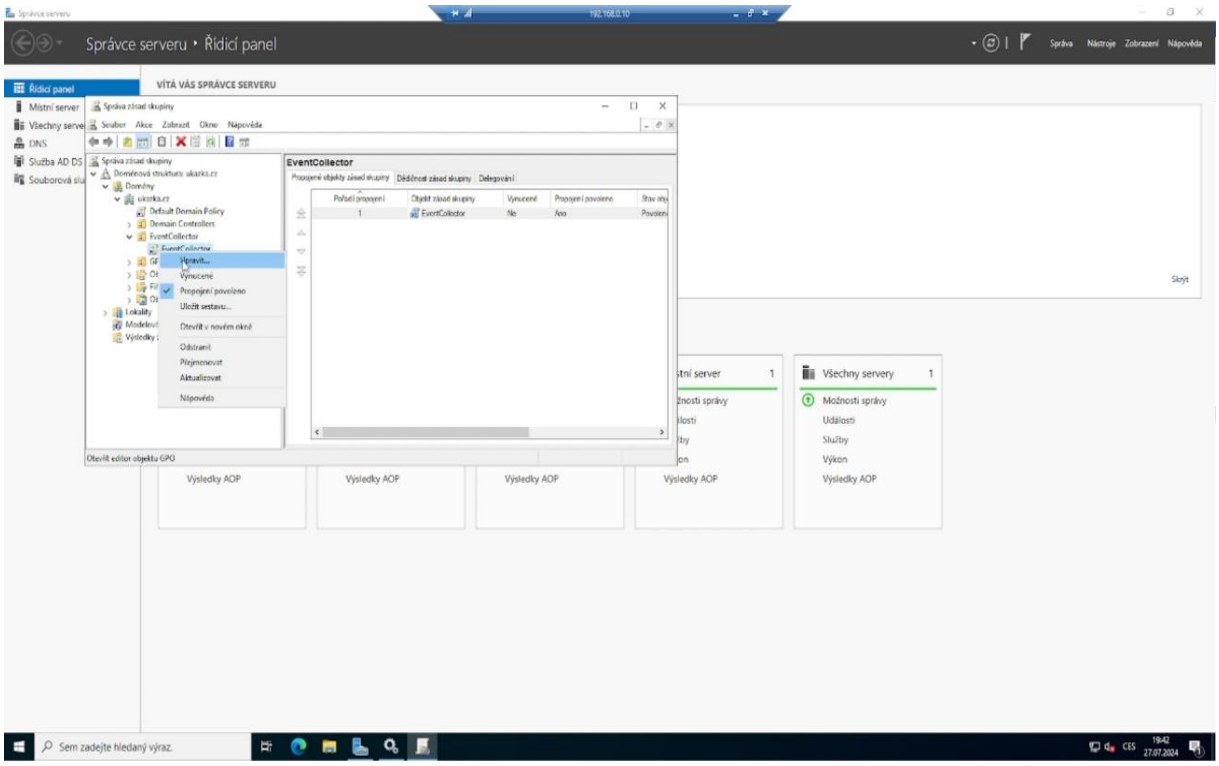
Obr. 35 Spouštění Windows Event Collector přes cmd. Zdroj: vlastní zpracování

Na serveru zkontrolujeme ve Službách, jestli služba „Sběr událostí systému Windows“ je aktivní a automaticky se spouští viz Obrázek 36.

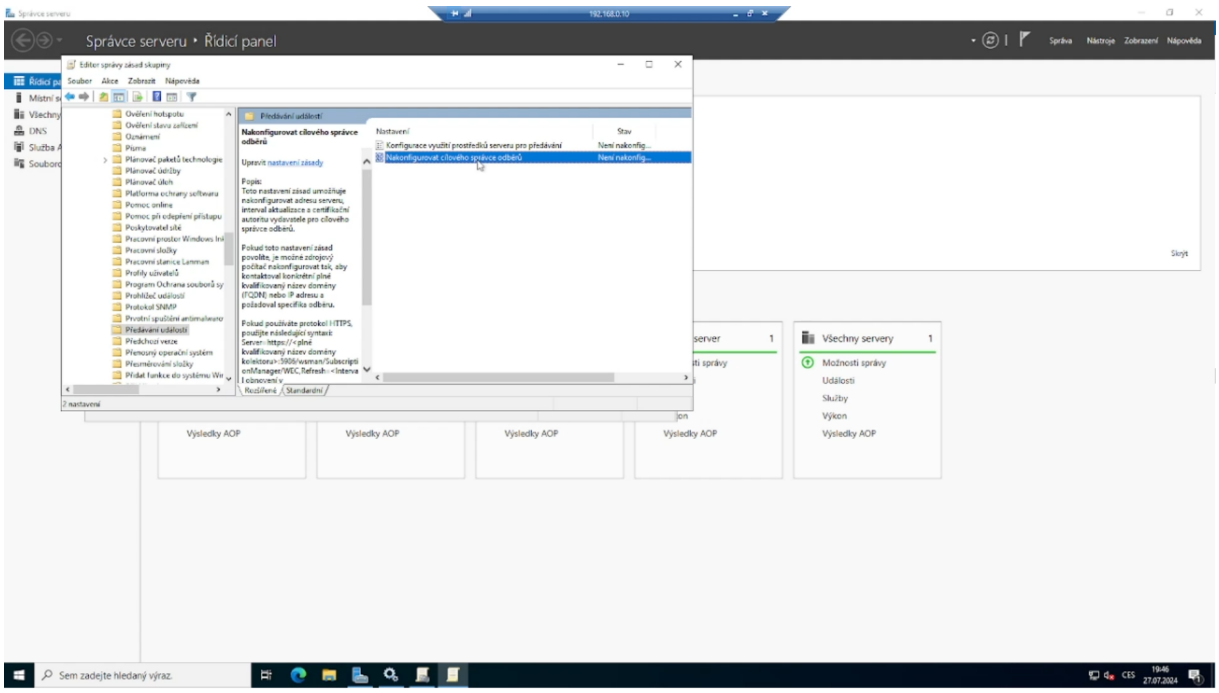


Obr. 36 Kontrola nastartované služby Sběr událostí systému Windows. Zdroj: vlastní zpracování

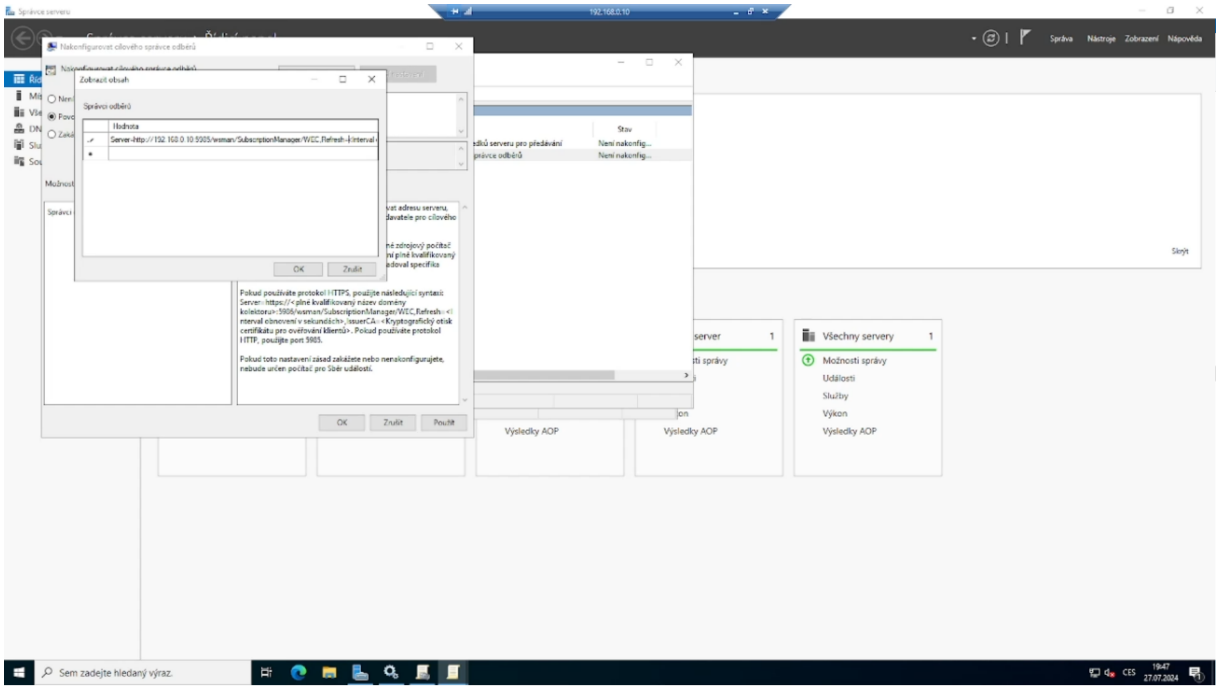
Ve „Správci serveru“ si otevřeme „Správa zásad skupiny“ a následně přejdeme do „Organizační jednotky“, kde je počítač, ze kterého chceme sbírat Události. Zde vytvoříme GPO a upravíme ho viz Obrázek 37. Otevřeme „Konfigurace počítače“, „Zásady“, „Šablony pro správu“, „Předávání událostí“. Zde upravíme položku „Konfigurovat cílového správce odběrů“ viz Obrázek 38. Klikneme na „Povolit“. V okně Nápovědy vidíme, jak má přibližně vypadat parametr, který budeme zadávat. Tento parametr zkopírujeme. V levé části klikneme na záložku „Zobrazit“. Sem vložíme zkopírovaný parametr, přepíšeme na „http“, zadáme IP adresu serveru, na který budeme Události odesílat. Změníme port na 5985 a nakonec přidáme čas, jak často chceme, aby se Události odesílaly viz Obrázek 39. Vše potvrdíme a vrátíme se do editoru. Následně přejdeme do „Konfigurace počítače“, „Zásady“, „Šablony pro správu“, „Vzdálená správa systém „Windows (WinRM)“, „Služba WinRM“ viz Obrázek 40. Zde upravíme „Povolit vzdálenou správu serveru prostřednictvím služby WinRM“. Dále klikeme na „Povolit“. A v možnostech zadáme do filtru protokolu IPv4 „*“ viz Obrázek 41.



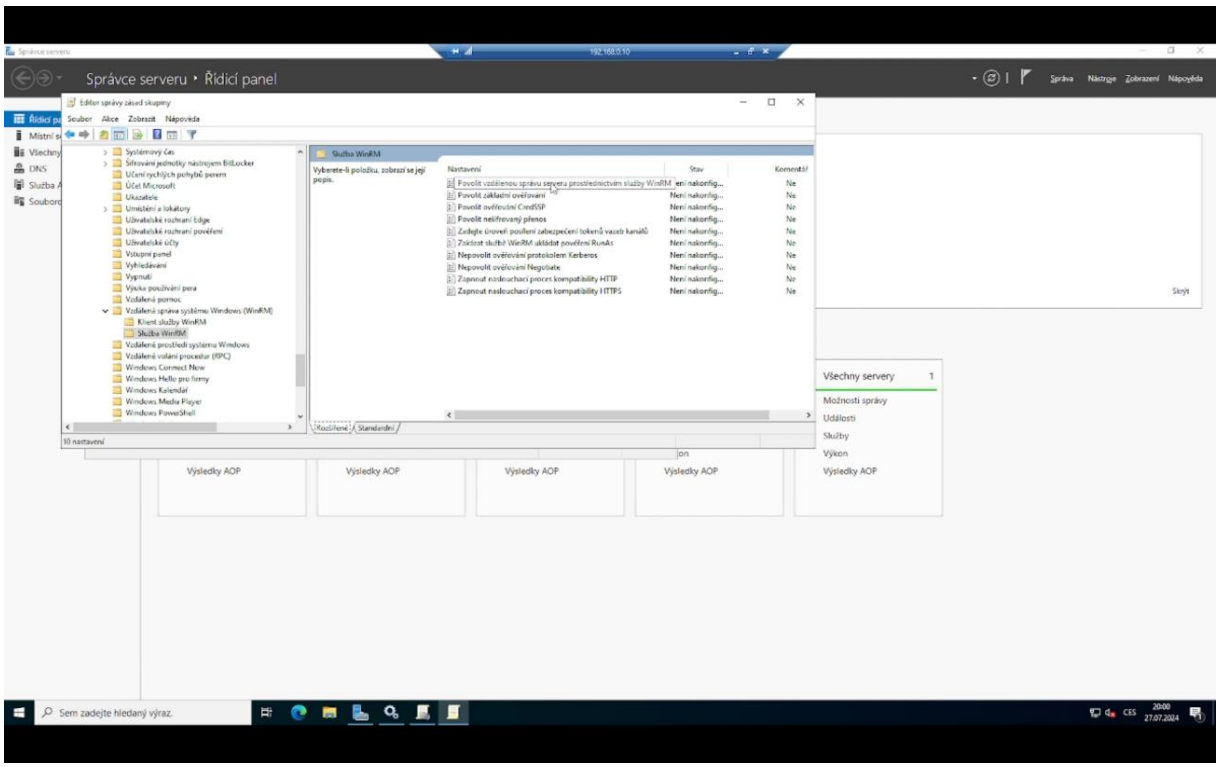
Obr. 37 Úprava organizační jednotky pro Windows Event Collector . Zdroj: vlastní zpracování



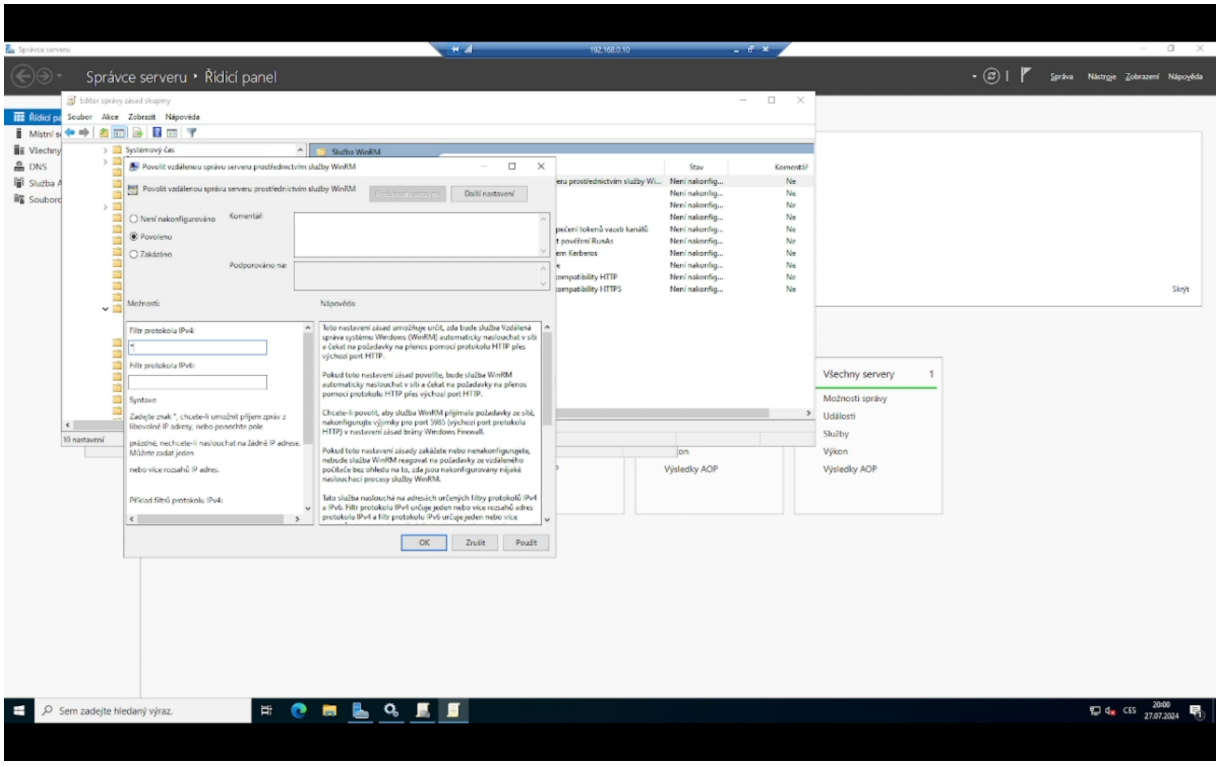
Obr. 38 Úprava položky Konfigurovat cílového správce odběrů. Zdroj: vlastní zpracování



Obr. 39 Úprava parametru v Konfigurovat cílového správce odběrů. Zdroj: vlastní zpracování

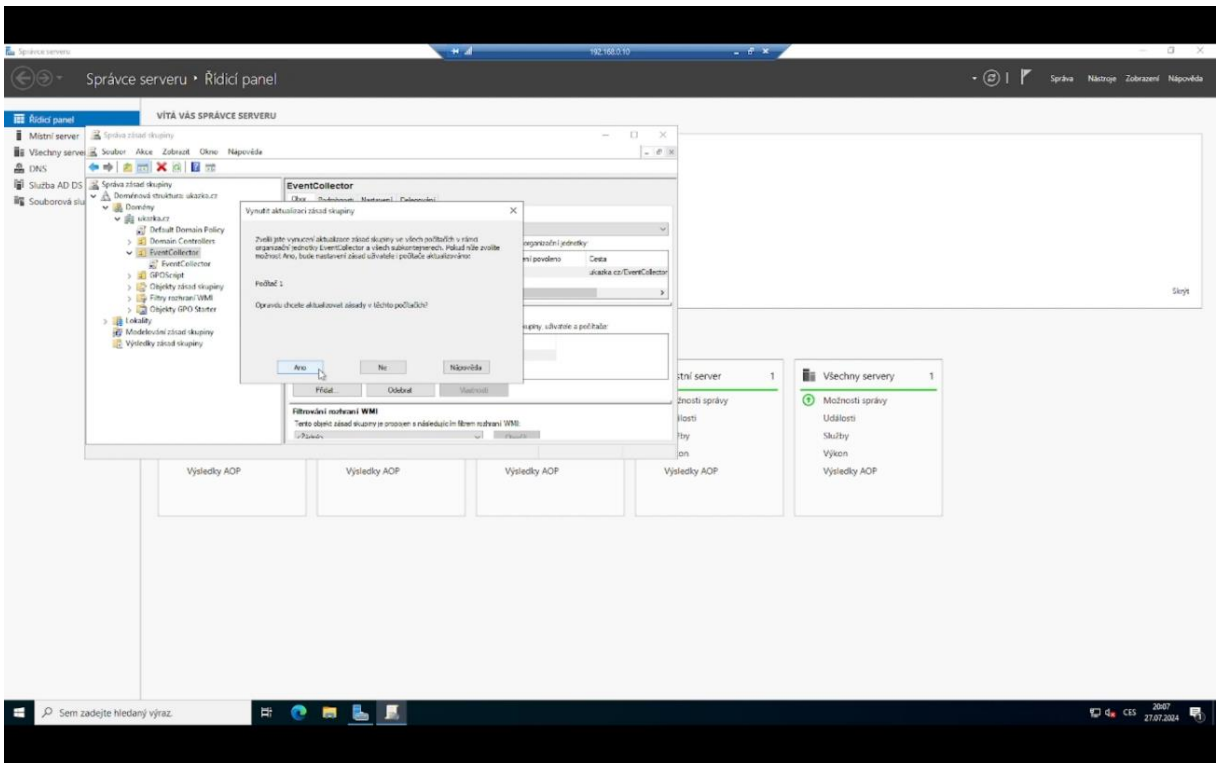


Obr. 40 Úprava položky Povolit vzdálenou správu serveru prostřednictvím služby WinRM. Zdroj: vlastní zpracování

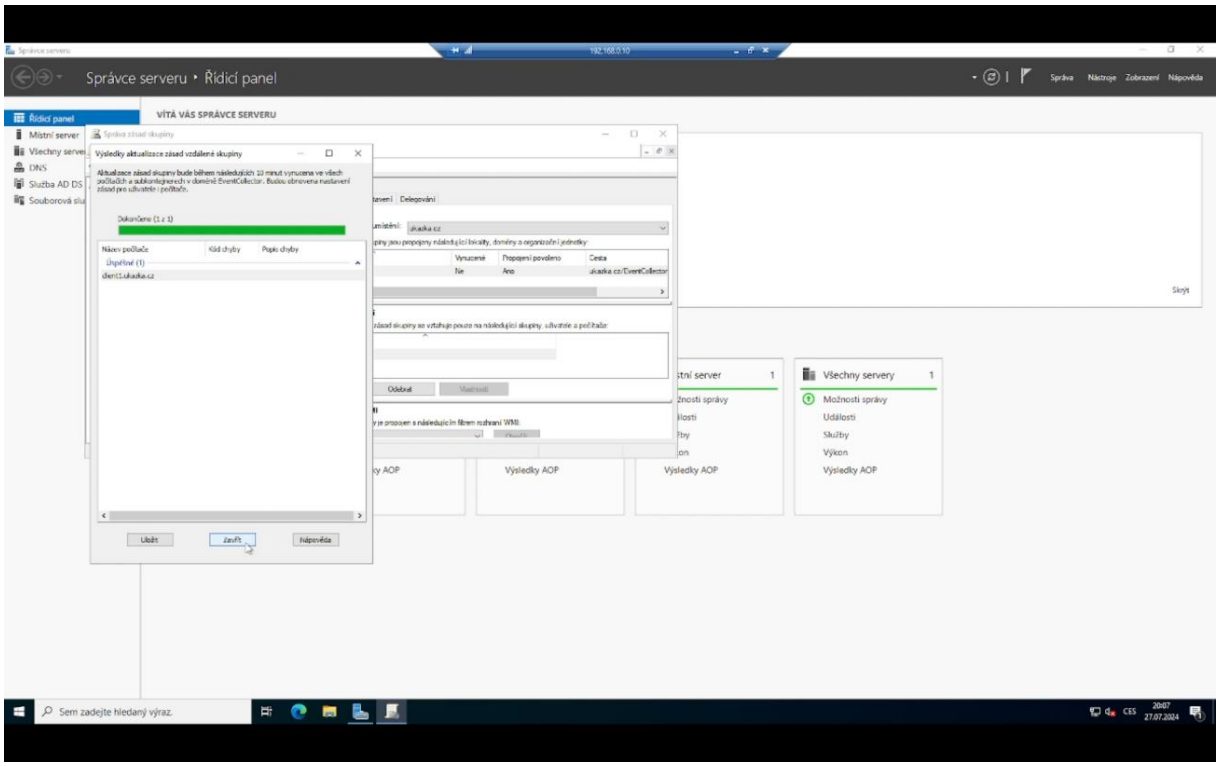


Obr. 41 Úprava parametrů Filtr protokolu IPv4. Zdroj: vlastní zpracování

Práci uložíme, zavřeme a aplikujeme GPO viz Obrázek 42 a 43.

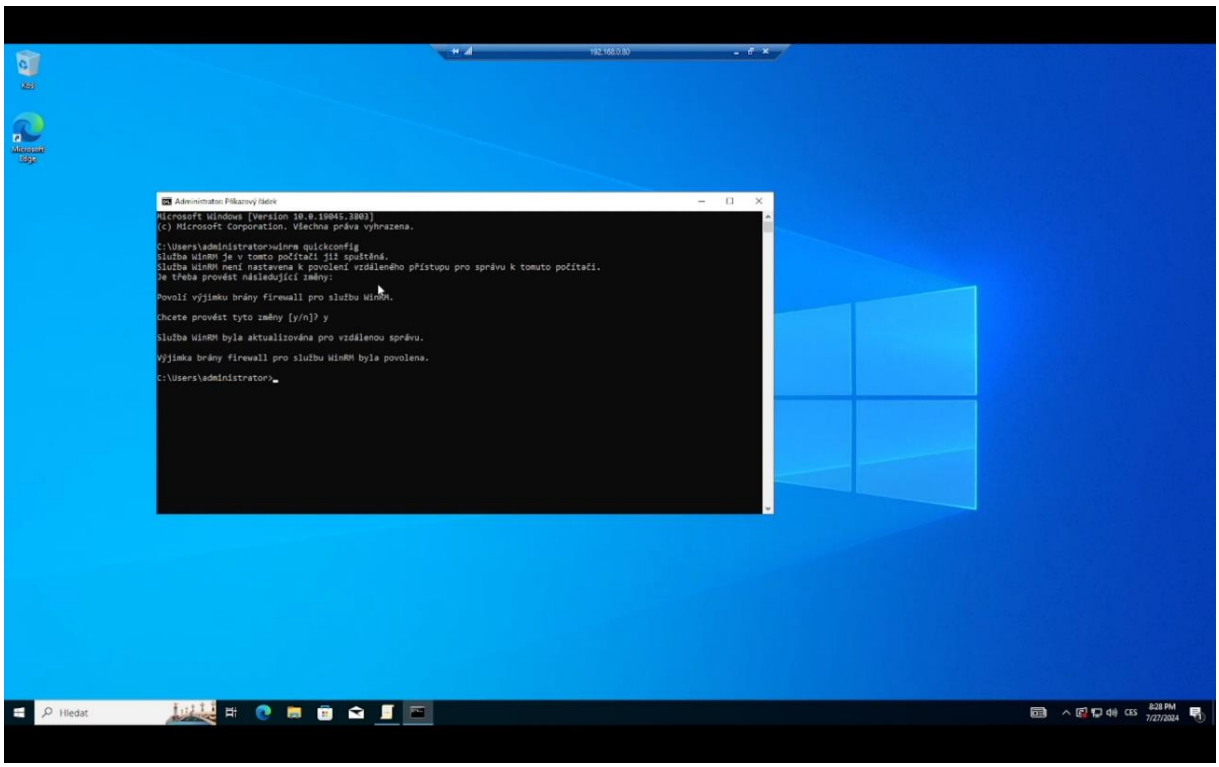


Obr. 42 Aplikování GPO EventCollector 1 . Zdroj: vlastní zpracování



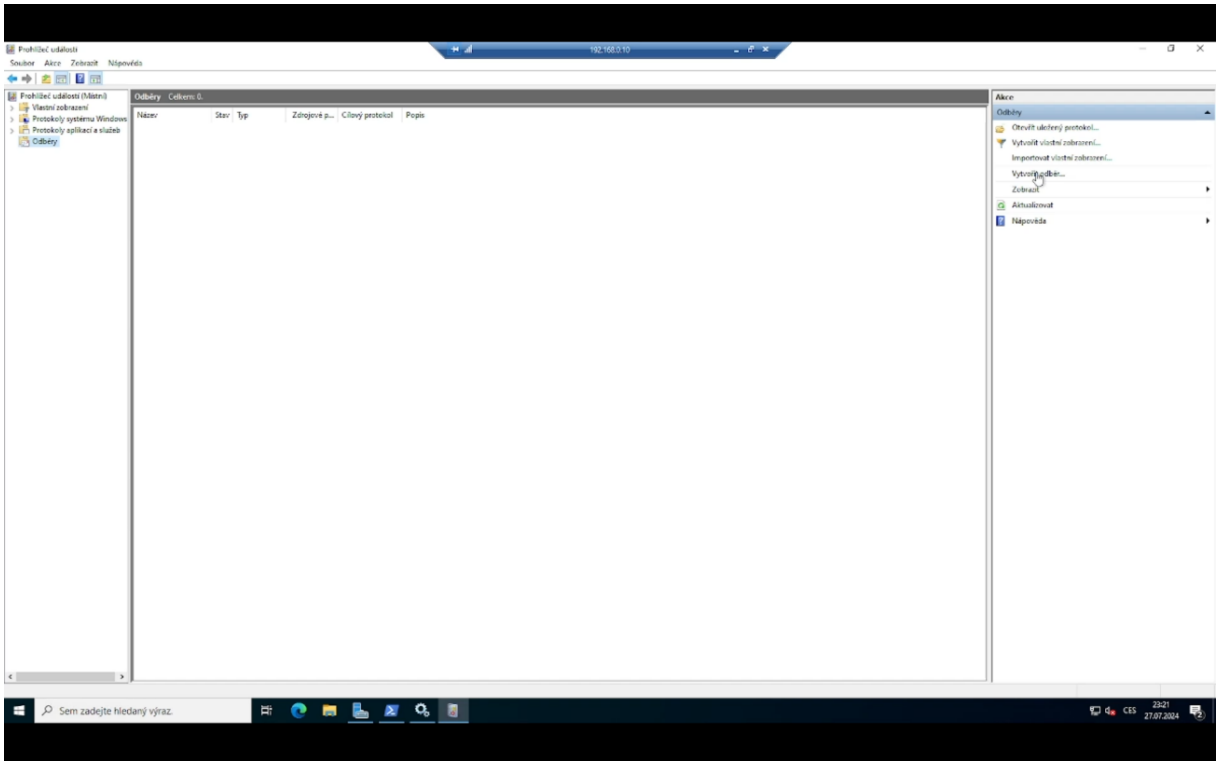
Obr. 43 Aplikování GPO EventCollector 1. Zdroj: vlastní zpracování

Dále přejdeme na uživatelský počítač a do cmd zadáme: winrm quickconfig a potvrdíme a potvrdíme viz Obrázek 44. Vrátíme se zpět na server.

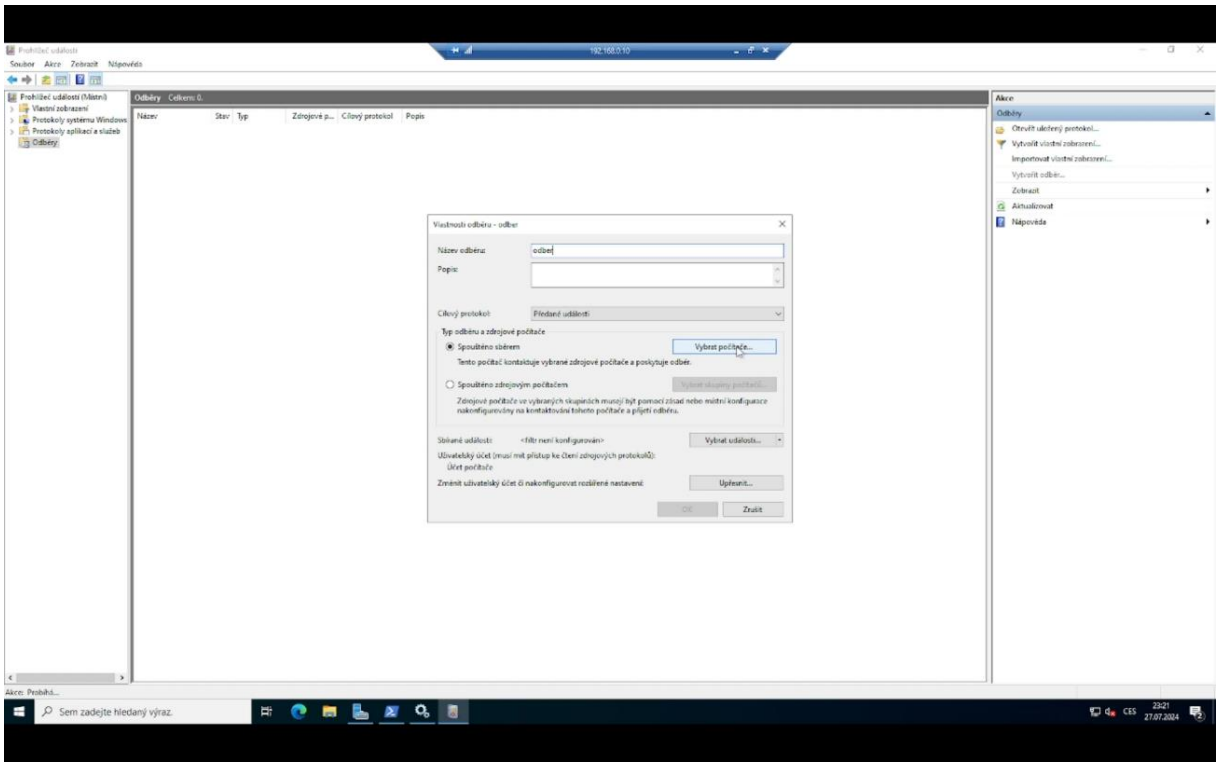


Obr. 44 Uživatelský počítač – zapínání Event Collector. Zdroj: vlastní zpracování

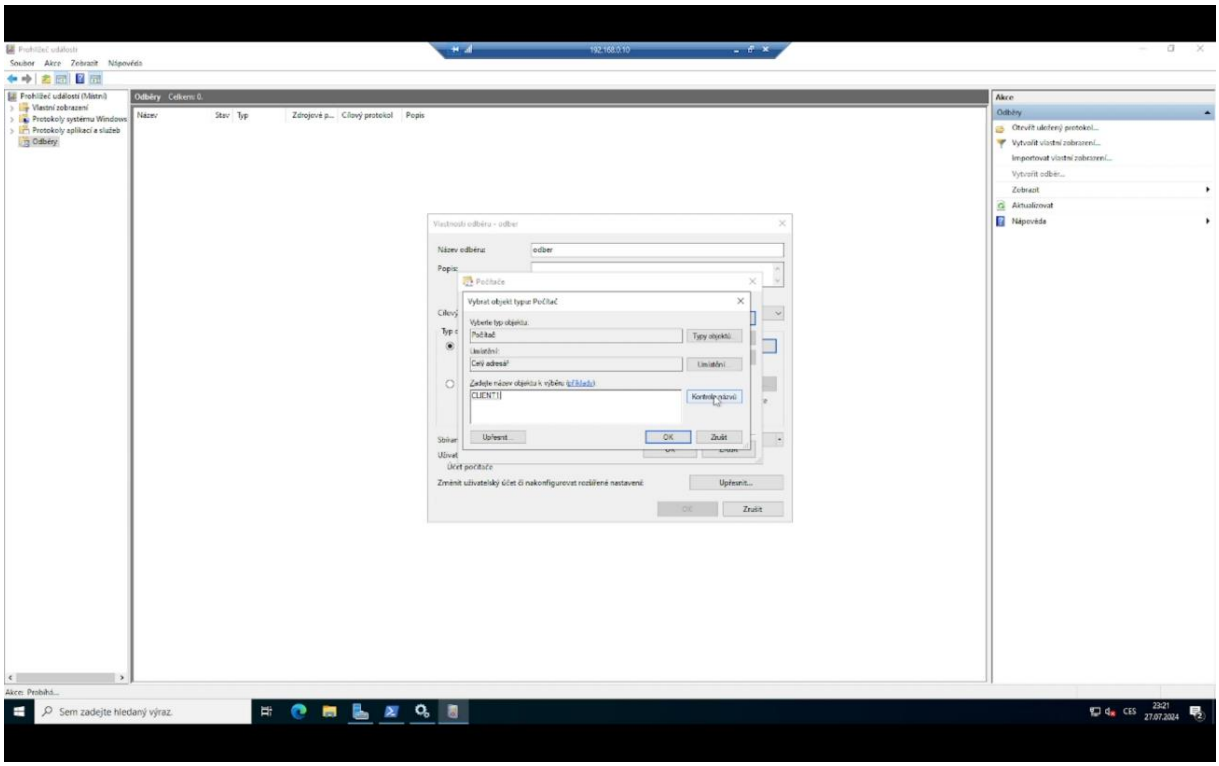
Otevřeme Prohlížeč událostí a přejdeme do záložky „Odběry“. Potvrdíme „ano“. V pravé části obrazovky klikneme na „Vytvořit odběr“ viz Obrázek 45. Tento odběr pojmenujeme. Dále klikneme „Vybrat počítače“, „Přidat doménový počítač“ a zadáme jméno počítače, ze kterého chceme sbírat Události viz Obrázek 46 a 47. Potvrdíme, potvrdíme „OK“ a tím okno zavřeme.



Obr. 45 Prohlížeč událostí – Vytváření odběru. Zdroj: vlastní zpracování

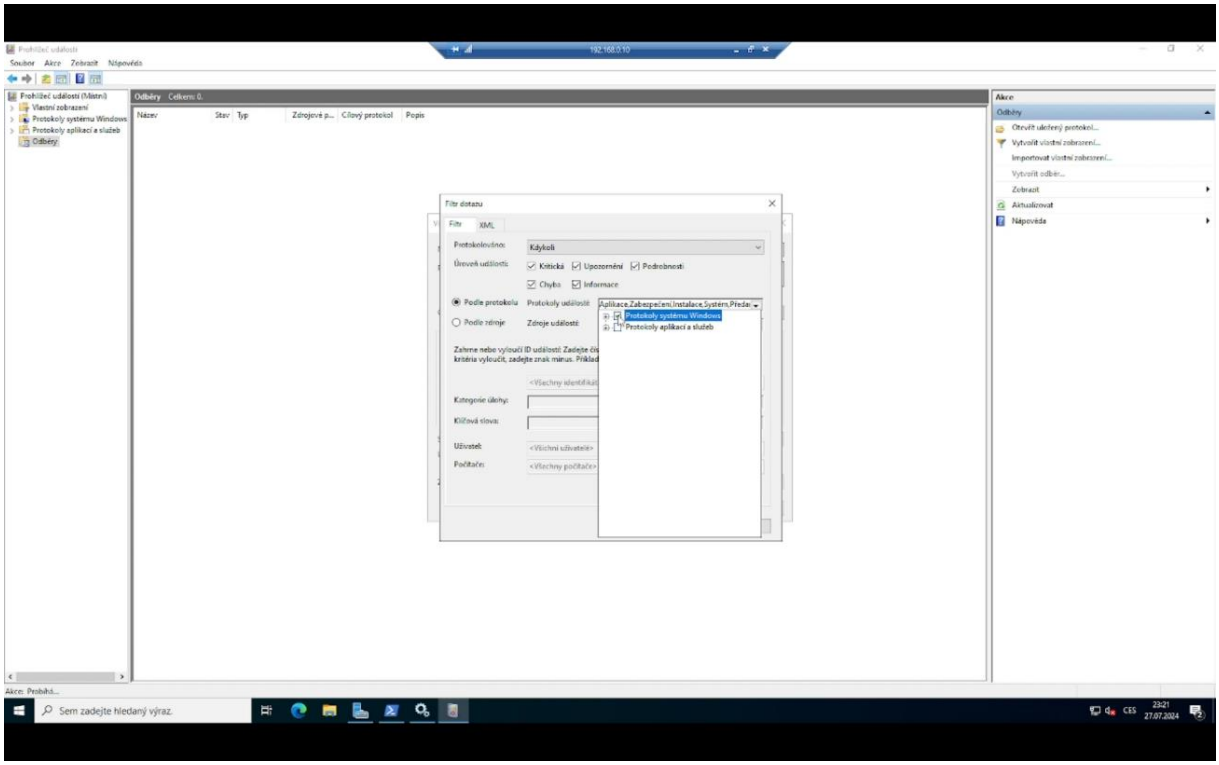


Obr. 46 Pojmenování odběru. Zdroj: vlastní zpracování



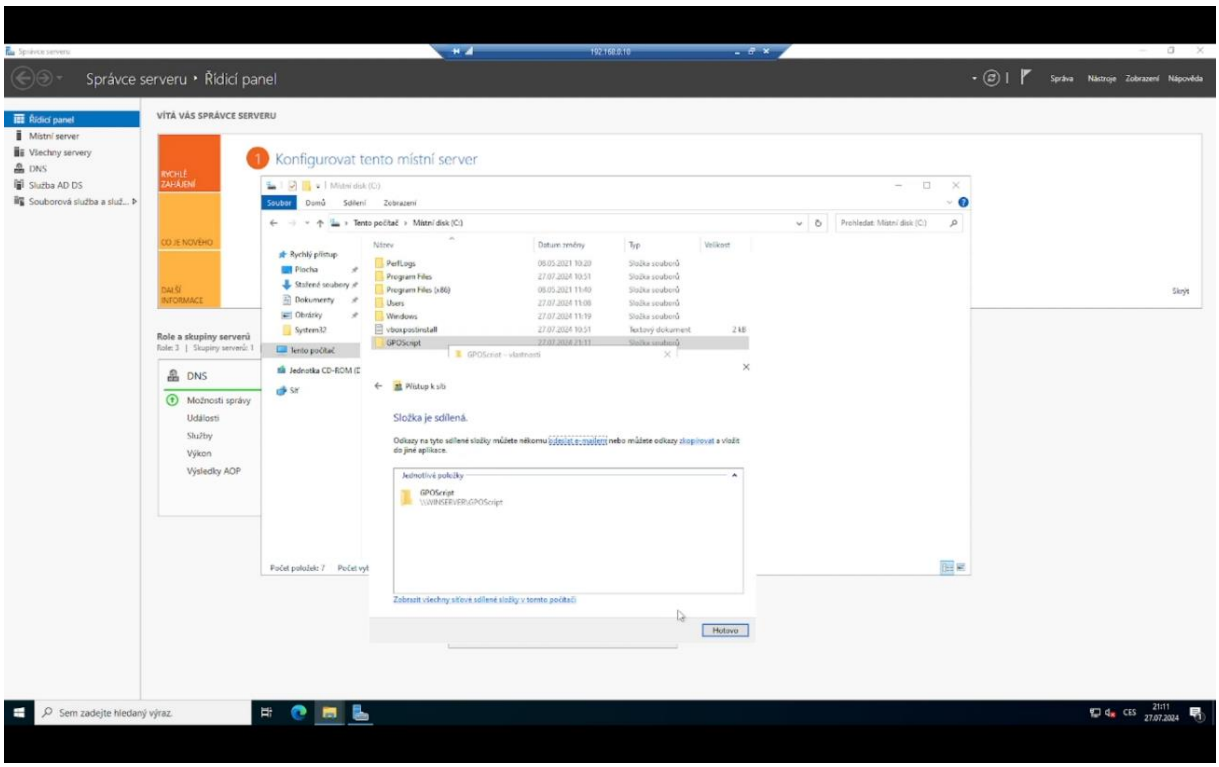
Obr. 47 Přidávání klientského počítače do odběru. Zdroj: vlastní zpracování

Dále si nastavíme, jaké Události chceme odebírat. Klikneme na „Výběr událostí“ a zde zaškrtneme všech pět úrovní Událostí. Následně vybereme, jaké protokoly chceme zasílat. Vybereme všechny „Protokoly systému Windows“ viz Obrázek 48. Potvrdíme dvakrát „OK“, a tím je nastavení dokončeno.



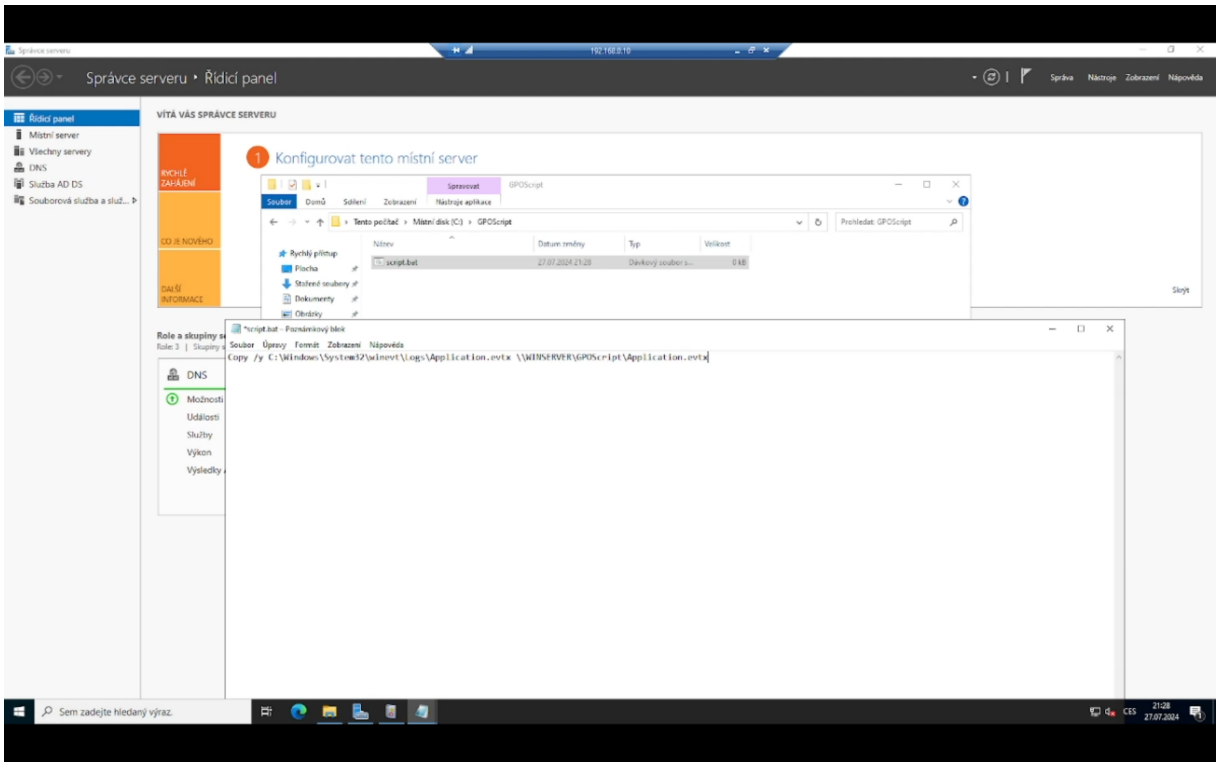
Obr. 48 Výběr filtru odběru. Zdroj: vlastní zpracování

Další metoda sběru, na kterou se podíváme, je Script za pomoci GPO.Nejdříve na serveru vytvoříme složku, do které se budou ukládat Události. Tuto složku nasdílíme a povolíme oprávnění do ní zapisovat viz Obrázek 49.



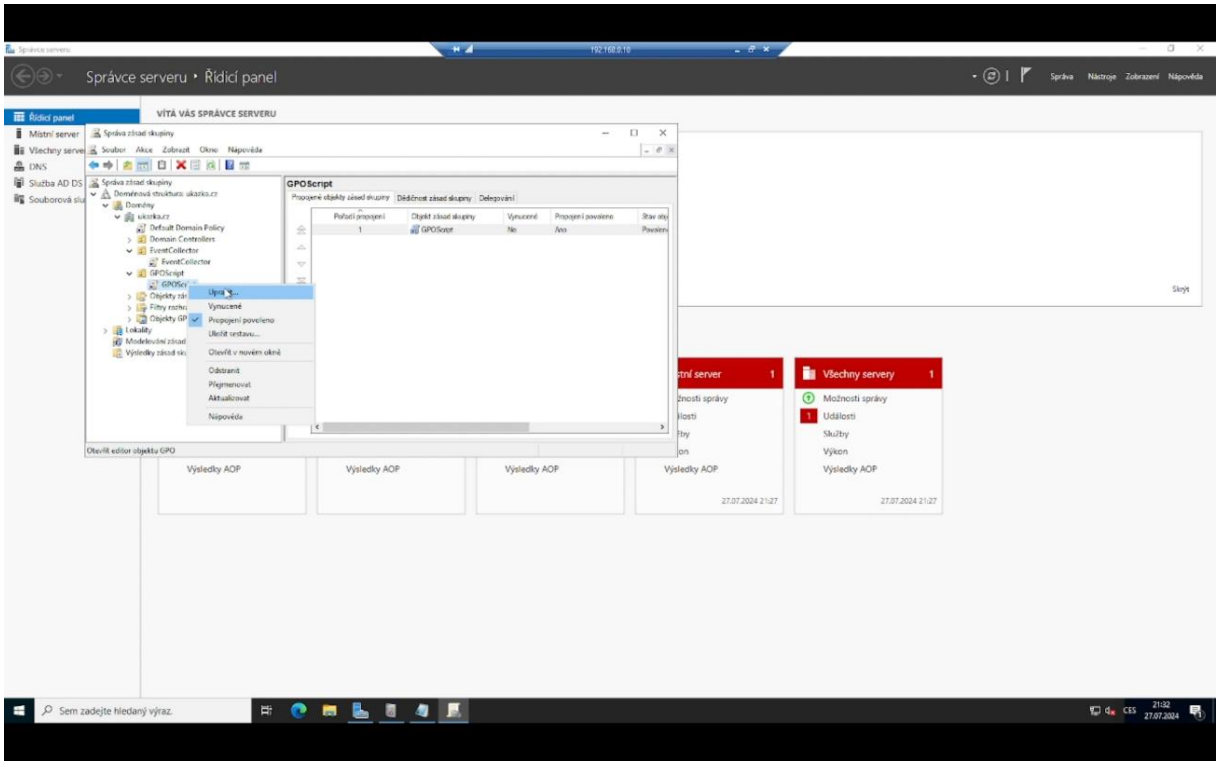
Obr. 49 Nasdílení složky. Zdroj: vlastní zpracování

Napíšeme jednoduchý script a uložíme jej nejlépe do sdílené složky, kterou jsme vytvořili v předchozím kroku viz Obrázek 50.



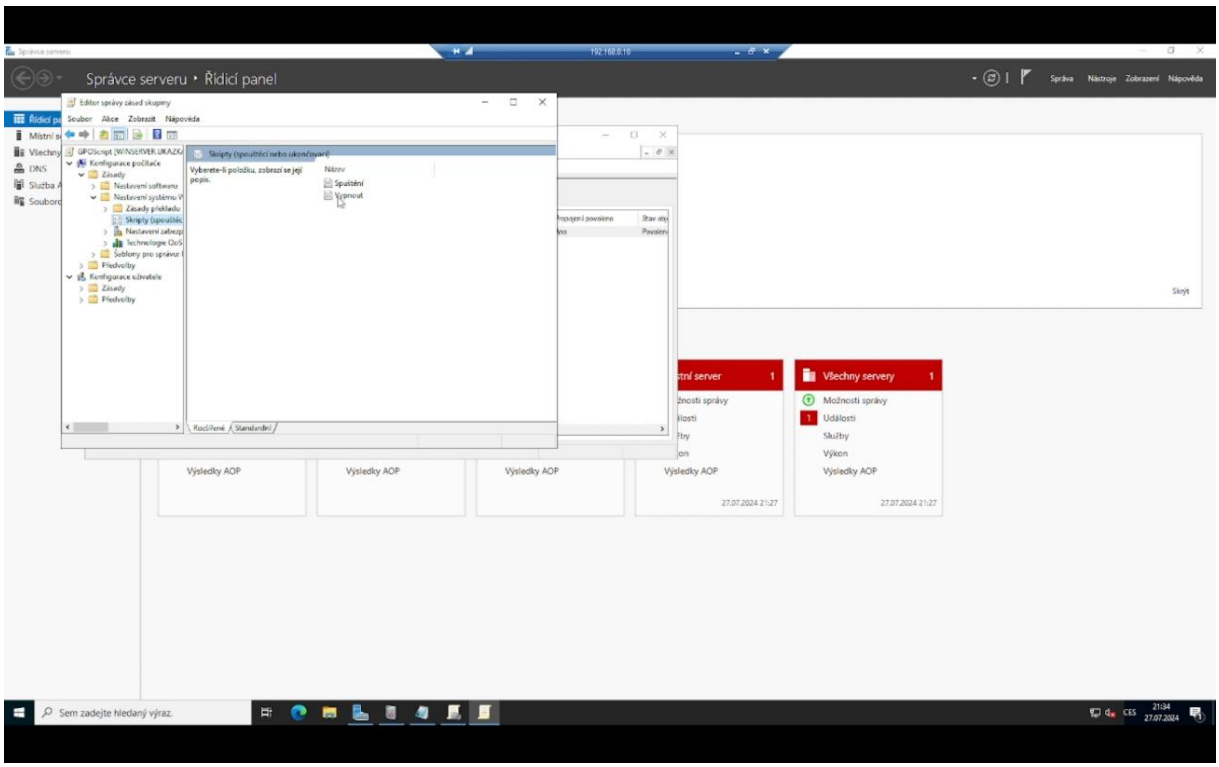
Obr. 50 Vytvoření skriptu pro sběr událostí. Zdroj: vlastní zpracování

Ve „Správci serveru“ si opět otevřeme „Správa zásad skupiny“ a následně přejdeme do „Organizační jednotky“, kde je počítač, ze kterého chceme sbírat Události viz Obrázek 51.

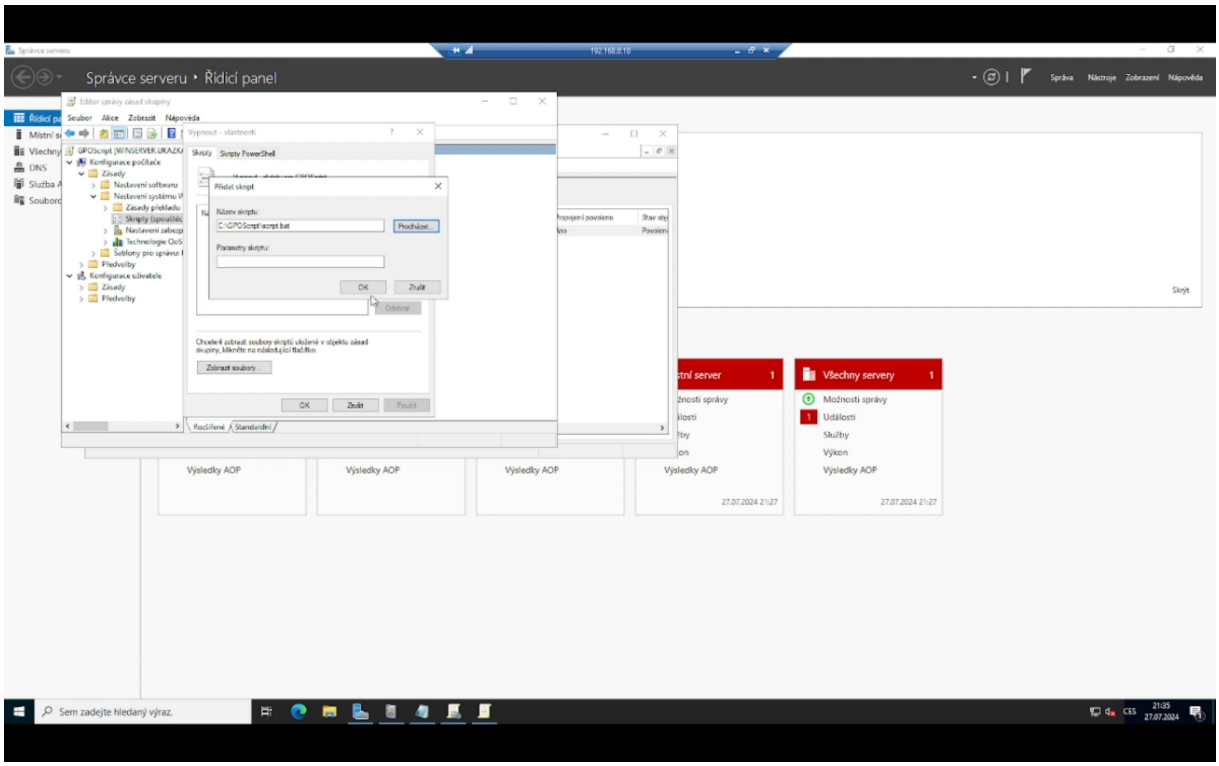


Obr. 51 Úprava organizační jednotky pro script. Zdroj: vlastní zpracování

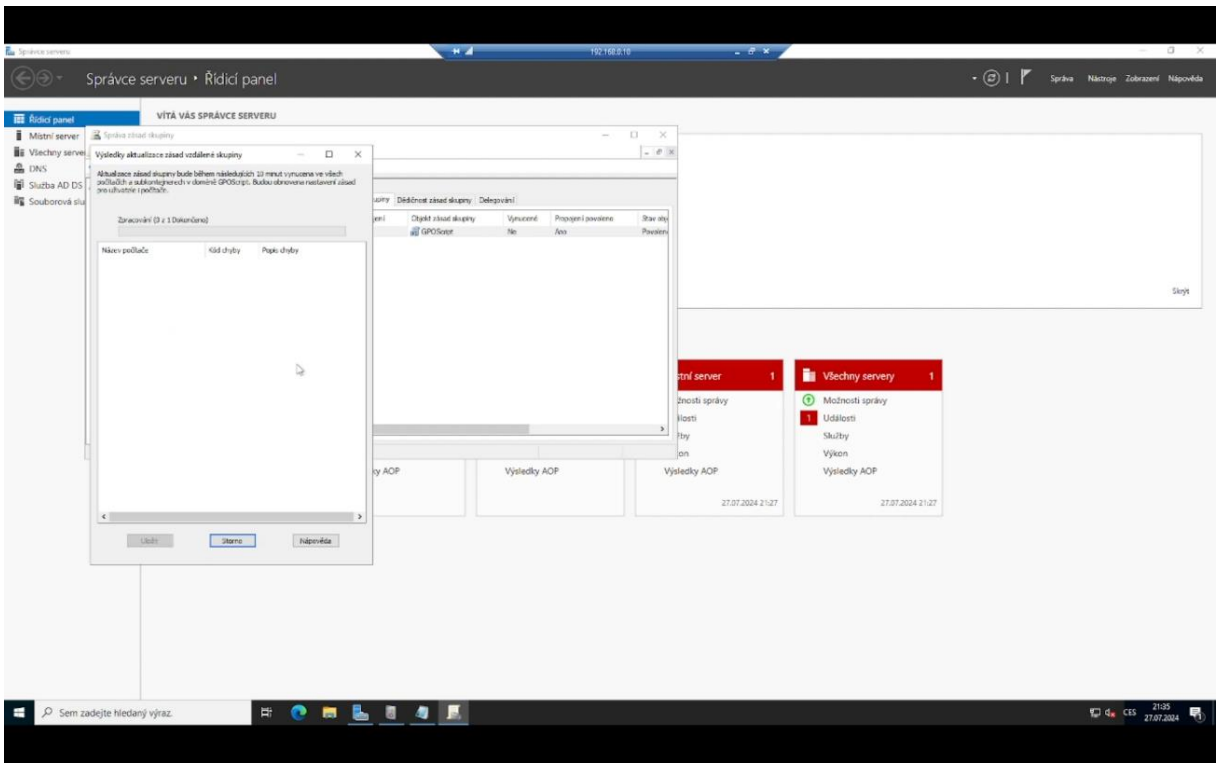
Otevřeme „Konfigurace počítače“, „Zásady“, „Nastavení systému Windows“, „Skripty spuštění nebo ukončení“. Zde upravíme položku „Vypnout“, klikneme na „Přidat“, „Procházet“ a vybereme script, který jsme vytvořili. Výsledek uložíme a aplikujeme viz Obrázek 52, 53 a 54.



Obr. 52 Úprava položky Vypnout. Zdroj: vlastní zpracování



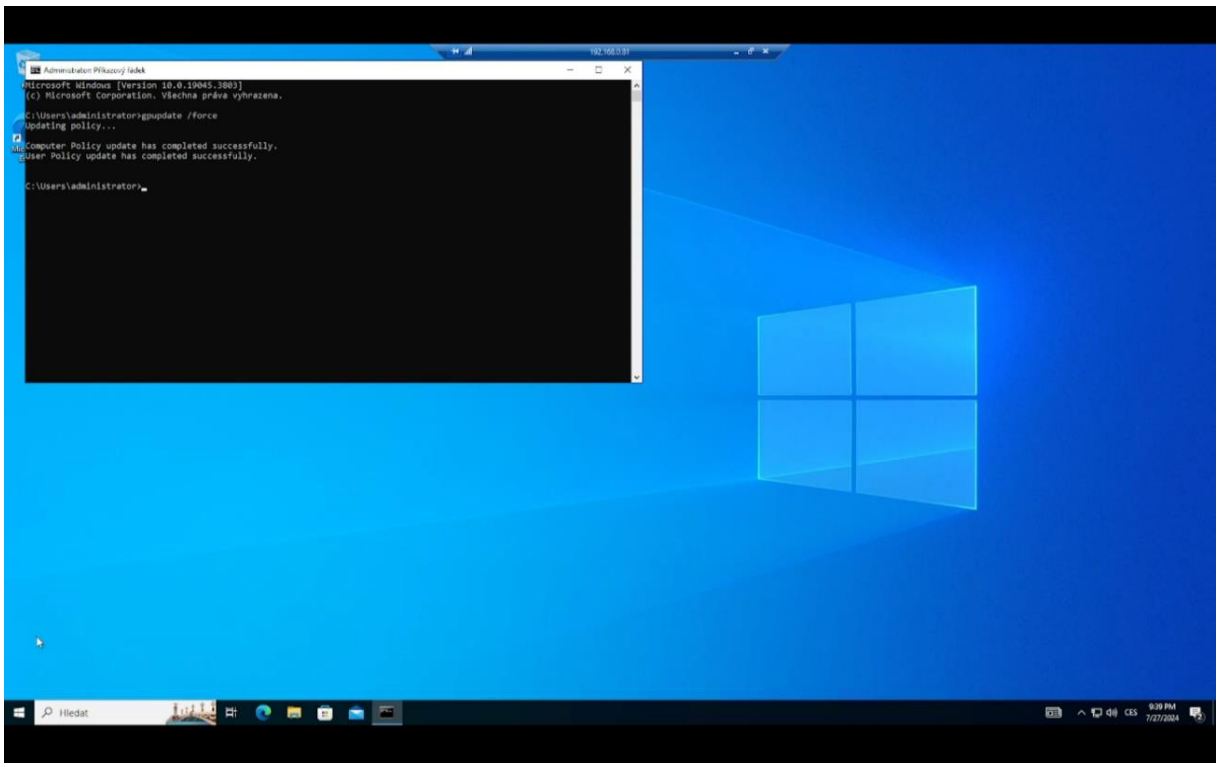
Obr. 53 Přidání skriptu do položky Vypnout. Zdroj: vlastní zpracování



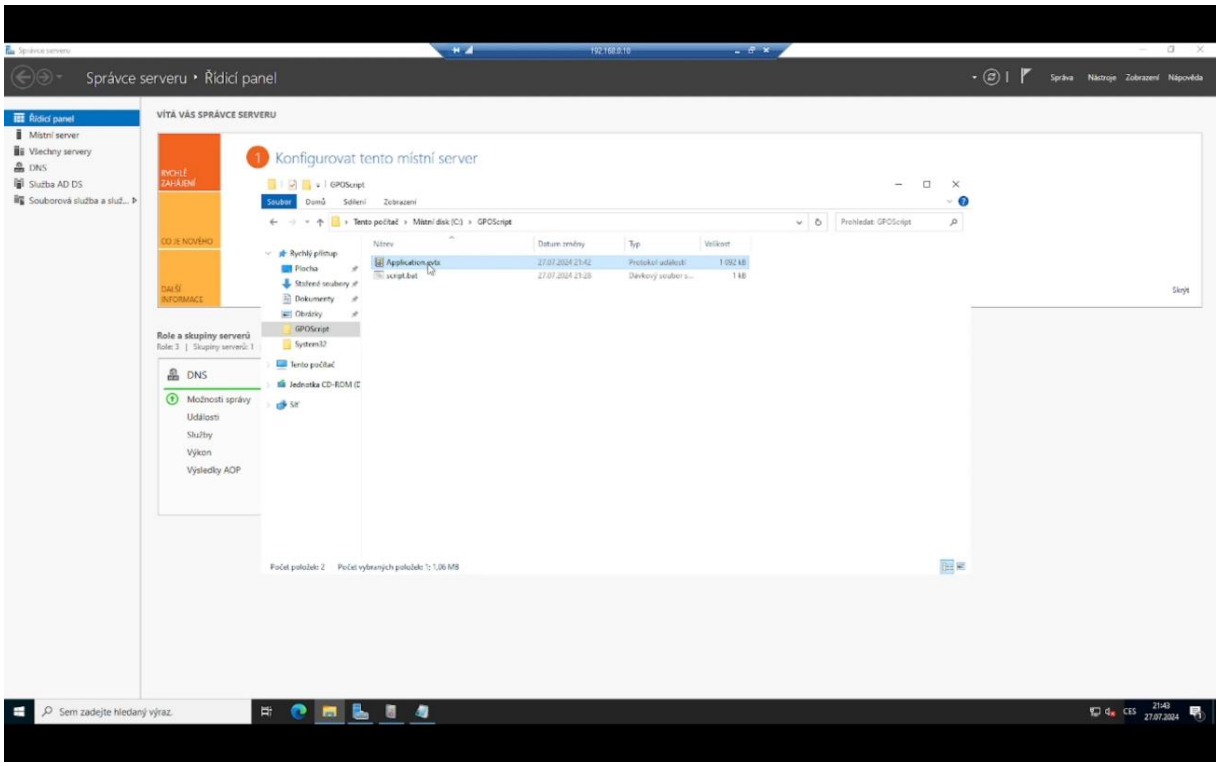
Obr. 54 Aplikování GPOScript. Zdroj: vlastní zpracování

Přejdeme na počítač, ze kterého Události chceme odesílat. Do příkazového řádku zadáme „gpupdate /force“, aby se nám politika propsala do počítače viz Obrázek 55. Poté restartujeme počítač.

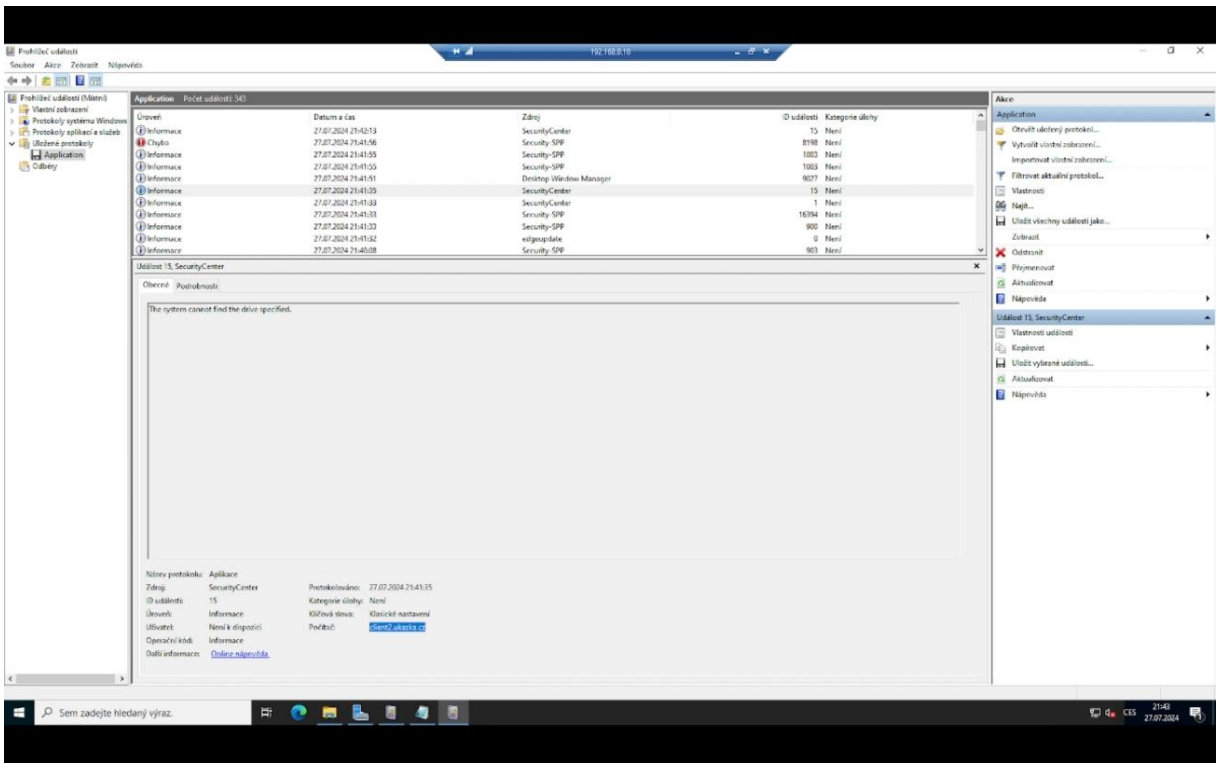
Podíváme se zpět na server do sdílené složky, zda se v ní vytvořil soubor s Událostí viz Obrázek 56. Na soubor poklikáme, tím otevřeme „Prohlížeč události“. Pokud se podíváme na záznamy, které zde jsou zobrazeny, zjistíme, že jsou z počítače, na kterém jsme provedli nastavení viz Obrázek 57.



Obr. 55 Aplikování politiky na uživatelský počítač. Zdroj: vlastní zpracování

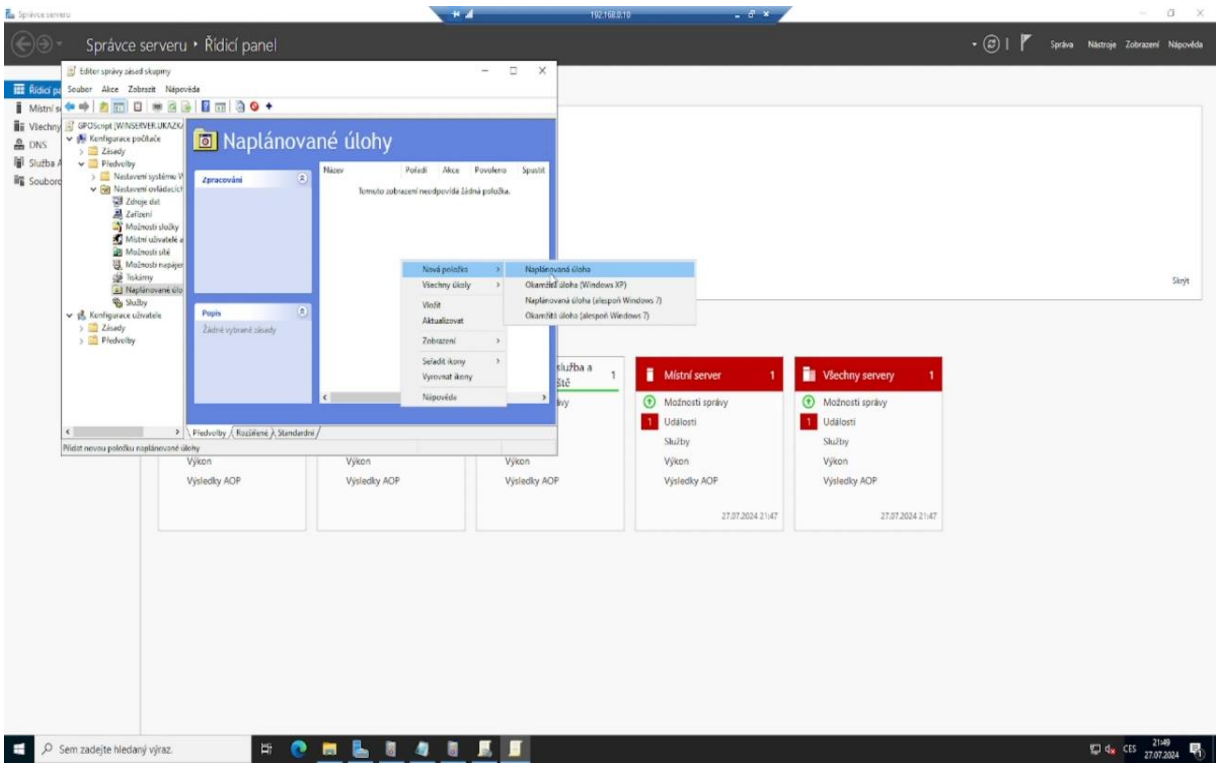


Obr. 56 Převzaté protokoly z uživatelského počítače. Zdroj: vlastní zpracování



Obr. 57 Prohlížeč události – uživatelské události. Zdroj: vlastní zpracování

Pokud bychom chtěli, můžeme ještě přes politiku nastavit, aby se Události odesílaly v konkrétním čase. A to lze nastavit takto: „Konfigurace počítače“, „Předvolby“, „Nastavení ovládacího panelu“, „Naplánované úlohy“. Zde přidáme novou naplánovanou úlohu, ve které nastavíme, aby se v příkazovém řádku spouštěl náš script viz Obrázek 58.



Obr. 58 Aplikování skriptu do Naplánované úlohy. Zdroj: vlastní zpracování

9 Závěry a doporučení

V teoretické části této bakalářské práce byly uvedeny základní informace o historii Windows, Windows serverů a Active direktory. Byla představena práce s logy a problematika logování s využitím Prohlížeče událostí. Dále byly uvedeny způsoby auditování, seznámení se se Skupinovou politikou a uvedení Sysinetrnals nástrojů, které byly dále použity v jednotlivých dílčích úlohách praktické části bakalářské práce. V praktické části bakalářské práci byly vytvořeny podpůrné materiály v oblasti bezpečnostního monitoringu s důrazem na konfiguraci a řešení v operačním systému Windows ve formě video tutoriálů.

Vznikla 4 videa s podpůrným obsahem. V prvním videu byl představen Prohlížeč událostí, rozdělení protokolů a typy jednotlivých událostí. Následující video bylo zaměřeno na využití Active Directory k zaznamenávání a auditování událostí. K tomu bylo využito GPO. Ve třetím videu byly představeny nástroje Sysinternals, které jsou užitečné pro vyhledávání hrozeb v počítači. Čtvrté video bylo zaměřeno na Sběr událostí z jednotlivých uživatelských počítačů různými způsoby.

Administrátorům doporučujeme nenásledovat slepě zažité postupy, ale i nadále prozkoumávat, jaké se nabízejí další možnosti a vybrat vždy tu nejvhodnější pro daný projekt.

V této oblasti softwarové bezpečnosti je kladen důraz na vybalancování bezpečnosti systému a přívětivého uživatelského komfortu. Nejbezpečněji se jeví monitorovat vše, co se v počítači děje, ale to by v praxi bylo nereálné z důvodu velkého objemu dat. Proto je důležité nalezení rovnováhy, aby správci systému nebyli zahlceni nadbytečnými informacemi.

Útočníci stále objevují další možnosti útoků na naši infrastrukturu a tím se zvyšuje počet nových hrozeb, na které musíme pružně reagovat.

10 Seznam použité literatury

1. *THE WINDOWS OPERATING PERATING SYSTEM*. Online. Sistemas Operacionais II. 2008, 15.6.2023. Dostupné z: http://rossano.pro.br/fatec/cursos/soii/Windows.pdf. [cit. 2023-06-15].

2. KROGH, Einar. *An Introduction to Windows Operating System*. 2. Bookboon, 2017. ISBN 978-87-403-1935-4.

3. BOUŠKA, Petr. *Active Directory komponenty - domain, tree, forest, site*. Online. Www.samuraj-cz.com. 2008. Dostupné z: https://www.samuraj-cz.com/clanek/active-directory-komponenty-domain-tree-forest-site/. [cit. 2023-06-15].

4. *Introducing AD FS 2.0*. Online. 2012. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/ff641697(v=ws.10)?redirectedfrom=MSDN. [cit. 2023-06-15].

5. *How to use Event Viewer in Windows*. Online. Blackbaud. Dostupné z: https://kb.blackbaud.com/knowledgebase/articles/Article/75433. [cit. 2024-03-07].

6. *Windows Event Log Definition*. Online. Solarwinds. Dostupné z: https://www.solarwinds.com/resources/it-glossary/windows-event-log. [cit. 2024-03-07].

7. *How to move Event Viewer log files to another location*. Online. Dostupné z: https://learn.microsoft.com/en-us/troubleshoot/windows-server/application-management/move-event-viewer-log-files#move-event-viewer-log-files-to-another-location. [cit. 2024-03-25].

8. *Audit Policies and Event Viewer. Online. Ultimate IT Security. Dostupné z: https://www.ultimatewindowssecurity.com/securitylog/book/page.aspx?spid=chapter2. [cit. 2024-03-07]*.

9. KRAUSE, Jordan. *Mastering Windows Group Policy: control and secure your Active Directory environment with Group Policy*. Birmingham: Packt Publishing, Limited, 2018. ISBN 978-17-8934-543-8.

10. BOUŠKA, Petr. *Group Policy - řízení aplikace politik*. Online. Www.samuraj-cz.com. 2010 Dostupné z: https://www.samuraj-cz.com/clanek/group-policy-rizeni-aplikace-politik/. [cit. 2024-03-25].

11. *Group Policy Overview*. Online. 2016. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-r2-and-2012/hh831791(v=ws.11). [cit. 2024-03-25].

12. *Configure Logging and Tracing*. Online. 2024. Dostupné z: https://learn.microsoft.com/en-us/microsoft-desktop-optimization-pack/agpm/configure-logging-and-tracing. [cit. 2024-03-25].

13. *Group Policy for Beginners*. Online. 2012. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-7/hh147307(v=ws.10)?redirectedfrom=MSDN. [cit. 2024-08-03].

14. *Enable Analytic and Debug Logs. Online. 2013. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc749492(v=ws.11)?redirectedfrom=MSDN. [cit. 2024-03-25].*

15. *Show or Hide Analytic and Debug Logs*. Online. 2013. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc766275(v=ws.11)?redirectedfrom=MSDN. [cit. 2024-03-25].

16. *Event Logs*. Online. 2012. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2008-R2-and-2008/cc722404(v=ws.10). [cit. 2024-03-25].

17 RUSSINOVICH, M.E. a MARGOSIS, A. *Windows Sysinternals Administrator's Reference*. Microsoft Press, 2011. ISBN 978-07-3566-360-2.

18 *Microsoft to shut down TechNet subscription service*. Online. 2013. Dostupné z: https://www.zdnet.com/article/microsoft-to-shut-down-technet-subscription-service/. [cit. 2024-04-05].

19 RUSSINOVICH, Mark a MARGOSIS, Aaron. *Windows Sysinternals – wykrywanie i rozwiązywanie problemów*. Warszawa: APN Promise, 2017. ISBN 978-83-7541-313-7.

20 *Sysinternals*. Online. 2024. Dostupné z: https://learn.microsoft.com/pdf?url=https%3A%2F%2Flearn.microsoft.com%2Fen-us%2Fsysinternals%2Ftoc.json. [cit. 2024-08-03].

21 *Sysmon.* Online. 2024. Dostupné z: https://learn.microsoft.com/cs-cz/sysinternals/downloads/sysmon. [cit. 2024-04-06].

22 *PsLogList*. Online. 2024. Dostupné z: https://learn.microsoft.com/cs-cz/sysinternals/downloads/psloglist. [cit. 2024-04-06].

23 *Event Viewer*. Online. 2019. Dostupné z: https://learn.microsoft.com/en-us/shows/inside/event-viewer. [cit. 2024-04-27].

24 *Autoruns*. Online. 2024. Dostupné z: https://learn.microsoft.com/en-us/sysinternals/downloads/autoruns. [cit. 2024-08-03].

25 *Process Explorer*. Online. 2024. Dostupné z: https://learn.microsoft.com/cs-cz/sysinternals/downloads/process-explorer. [cit. 2024-08-03].

26 *Task Manager*. Online. 2019. Dostupné z: https://learn.microsoft.com/en-us/shows/inside/task-manager. [cit. 2024-08-03].

27 *Should Passwords Be Regularly Changed?* Online. My 1 login. 2022. Dostupné z: https://www.my1login.com/blog/as-should-passwords-be-regularly-changed. [cit. 2024-08-05].

28 *Audit object access*. Online. 2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-object-access. [cit. 2024-08-05].

29 *Audit File System*. Online. 2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-file-system. [cit. 2024-08-05].

30 *Audit Audit Policy Change*. Online. 2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/audit-audit-policy-change. [cit. 2024-08-05].

31 *Audit logon events*. Online. 2021. Dostupné z: https://learn.microsoft.com/en-us/previous-versions/windows/it-pro/windows-10/security/threat-protection/auditing/basic-audit-logon-events. [cit. 2024-08-05].

32 *CIS Control 16: Account Monitoring and Control*. Online. Tenable. 2023. Dostupné z: https://docs.tenable.com/security-center/CIS-CAS/Content/Controls/Foundational/Control-16/Control-16.htm. [cit. 2024-08-05].

33 ČERMÁK, Miroslav. *Sledování prostředků aneb prověřujeme běžící služby ve Windows*. Online. Clever and smart. 2017. Dostupné z: https://www.cleverandsmart.cz/sledovani-prostredku-aneb-proverujeme-bezici-sluzby-ve-windows/. [cit. 2024-08-06].

34 NOREM, Josh. *Zjistěte využití jednotky CPU a operační paměti RAM ve svém počítači*. Online. Computerworld. 2022. Dostupné z: https://www.computerworld.cz/clanky/zjistete-vyuziti-jednotky-cpu-a-operacni-pameti-ram-ve-svem-pocitaci/. [cit. 2024-08-06].

11 Přílohy

Příloha č.1 – DVD obsahující čtyři podpůrná videa vytvořena v této bakalářské práci

12 Zadání práce z IS (eVŠKP)

Zadání bakalářské práce

Autor:	**Jan Loubek**
Studium:	I2000762
Studijní program:	B1802 Aplikovaná informatika
Studijní obor:	Aplikovaná informatika
Název bakalářské práce:	**Bezpečnostní dohled OS Windows - video tutoriály**
Název bakalářské práce AJ:	

Cíl, metody, literatura, předpoklady:

Cílem bakalářské práce je vytvořit podpůrné materiály v oblasti bezpečnostního monitoringu s důrazem na konfiguraci a řešení OS Windiws v podobě video tutoriálů. V teoretické části autor představí a podrobně popíše postupy a řešení dílčích úloh bezpečnostního monitoringu v OS Windows s důrazem na využití event logu a nastavení group policy. V praktické části pak autor vytvoří praktická řešení dílčích úloh ve formě video tutoriálů.

Zadávající pracoviště:	Katedra informačních technologií, Fakulta informatiky a managementu
Vedoucí práce:	Ing. Tomáš Svoboda, Ph.D.
Datum zadání závěrečné práce:	15.10.2021