

ADMINISTRATÍVNE NÁSTROJE

vo Windows Server



SERVER MANAGER

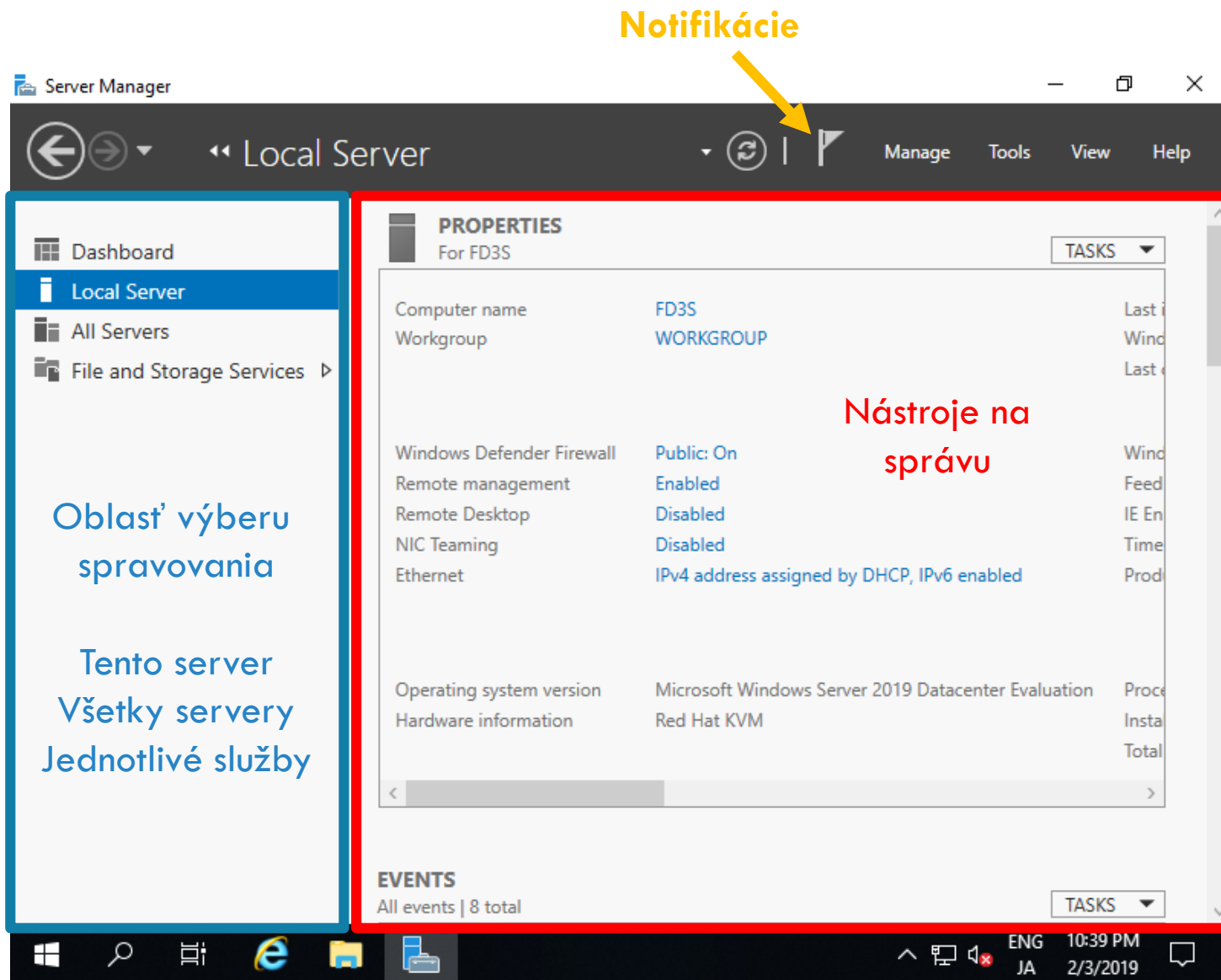
Správca servera

SERVER MANAGER

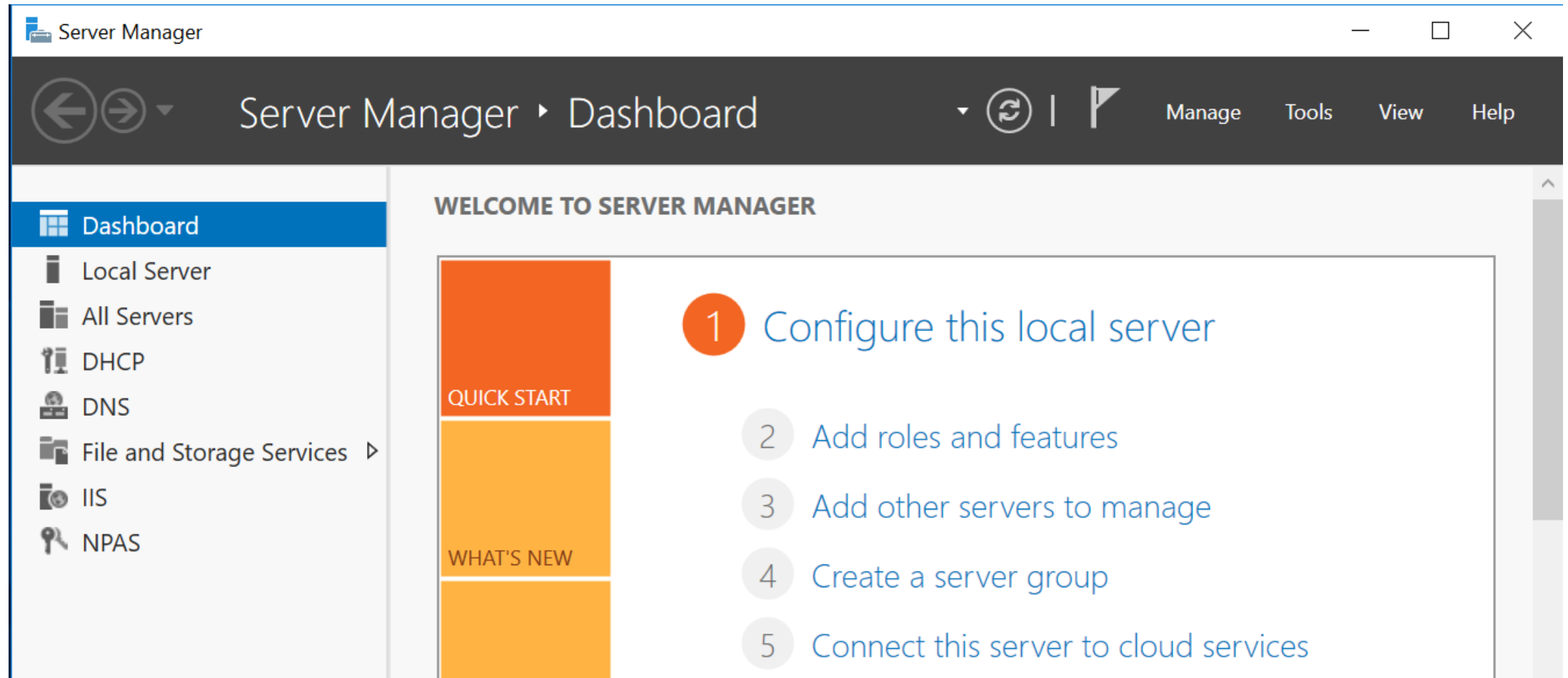
Nástroj na základnú správu aktuálnej inštalácie Windows Servera a služieb, ktoré na nej bežia

Umožňuje realizovať prvotnú poínštalačnú konfiguráciu servera

Umožňuje aj vzdialenú správu serverov



DASHBOARD — QUICK START

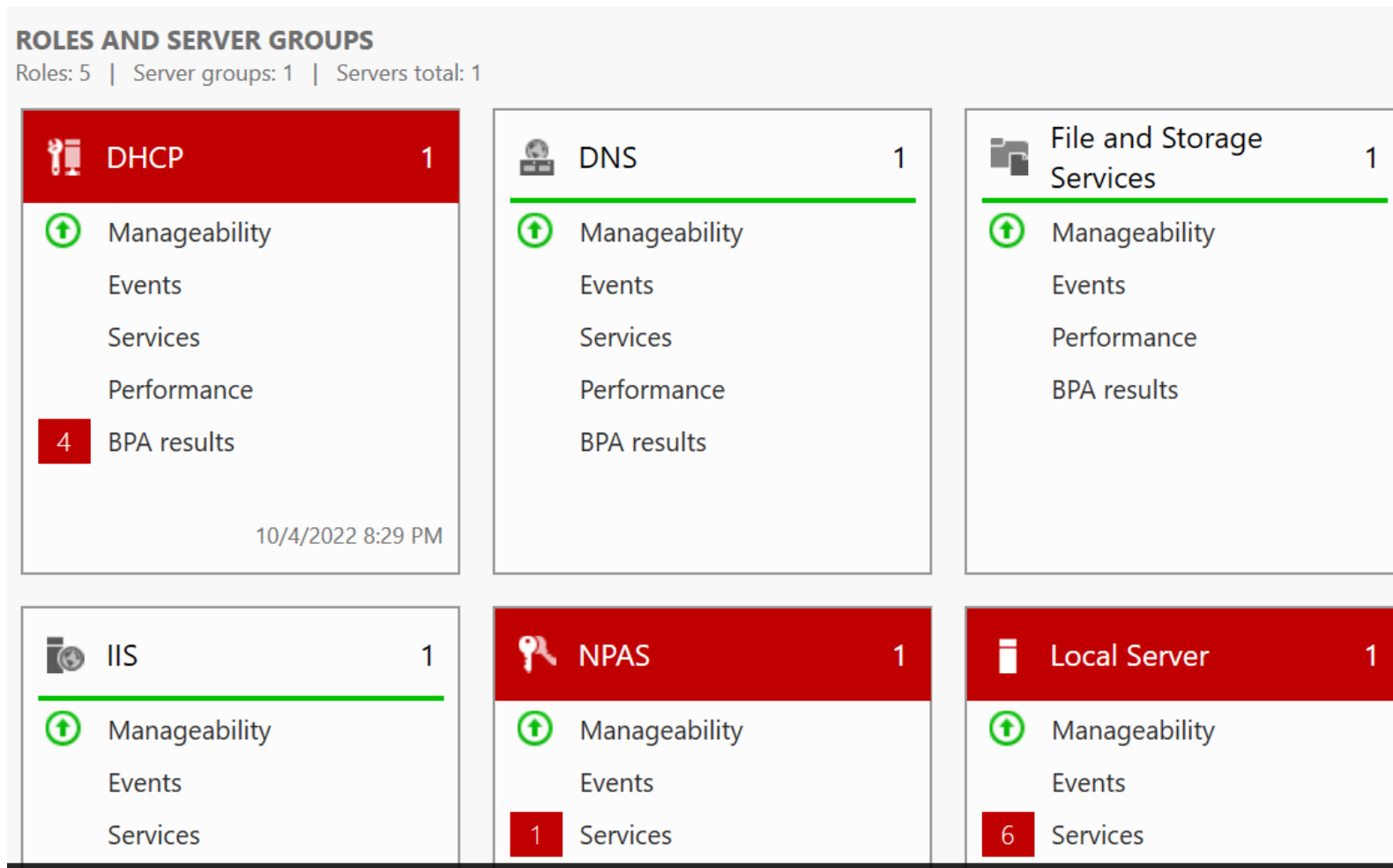


DASHBOARD — ROLES AND SERVER GROUPS


Zobrazuje udalosti hodné
zreteľa pre jednotlivé
roly bežiacie na serveri

Pre každú rolu upozorňuje na
problémy s:

- manažovateľnosťou
- kritickými udalosťami
- nefunkčnými službami
- preťažením CPU/RAM
- výsledkami analýzy BPA



LOCAL SERVER - PROPERTIES

 **PROPERTIES**
For WEBSERVER

TASKS ▼

Computer name	WEBSERVER	Last installed updates	Never
Workgroup	WORKGROUP	Windows Update	Download updates only, using Windows Update
		Last checked for updates	2/9/2022 9:59 PM
Windows Firewall	Public: Off	Windows Defender	Real-Time Protection: On
Remote management	Enabled	Feedback & Diagnostics	Settings
Remote Desktop	Disabled	IE Enhanced Security Configuration	On
NIC Teaming	Disabled	Time zone	(UTC+01:00) Belgrade, Bratislava, Budapest, Sarajevo, Sofia
Ethernet	IPv4 address assigned by DHCP, IPv6 enabled	Product ID	Not activated
Operating system version	Microsoft Windows Server 2016 Standard Evaluation	Processors	Intel(R) Core(TM) i5-8250U CPU @ 1.60 GHz
Hardware information	innotek GmbH VirtualBox	Installed memory (RAM)	2 GB
		Total disk space	49.51 GB

LOCAL SERVER — PROPERTIES (1)

Computer Name – umožňuje nastaviť meno počítača (platné v celej sieti)

Workgroup – umožňuje nastaviť pracovnú skupinu (počítače v skupine sa navzájom vidia a môžu zdieľať priečinky)

Windows Firewall – umožňuje meniť nastavenia firewallu

Remote management – umožňuje sprístupniť server pre vzdialenú správu cez administračné nástroje a PowerShell

Remote desktop – umožňuje vzdialenú správu servera cez vzdialenú plochu

NIC teaming – umožňuje zoskupiť viacero fyzických sieťových kariet do jednej logickej sieťovej karty (alternatíva k Etherchannelu/Cisco resp. Bondingu/Linux)

Ethernet – umožňuje zobrazit' a meniť nastavenia sieťových kariet

LOCAL SERVER - PROPERTIES (2)

Last installed update – informácia o poslednej aktualizácii systému

Windows Update – umožňuje zmeniť spôsob sťahovania a inštalácie aktualizácií

Last checked for updates – informácia o čase poslednej kontroly aktualizácií

Windows Defender – umožňuje meniť nastavenia antivírusovej ochrany

Feedback & Diagnostics – umožňuje nastaviť, aké informácie sa budú zdieľať so spoločnosťou Microsoft pri riešení problémov so systémom

IE Enhanced Security Configuration – umožňuje zapnúť/vypnúť zvýšenú ochranu v internetovom prehliadači Internet Explorer

Time zone – umožňuje nastaviť časovú zónu, v ktorej sa server nachádza

Product ID – zobrazenie/zmena informácií o aktivácii systému

LOCAL SERVER - EVENTS

Zobrazuje udalosti hodné zreteľa za posledné časové obdobie na aktuálnom serveri

These settings determine how Server Manager gathers event data from servers in the server group that you are currently managing. Changes to defaults that significantly increase the number of events in the Events tile can result in delayed responses from Server Manager.

Show events with these severity levels

☒ Critical ☒ Error ☒ Warning ☐ Informational

Get events that have occurred within the past

24 hours

Get events from the following event log files

Multiple

EVENTS

All events | 14 total

TASKS

Configure Event Data

Refresh

Filter



Server Name	ID	Severity	Source	Log	Date and Time
WEBSERVER	10016	Error	Microsoft-Windows-DistributedCOM	System	10/4/2022 7:10:23 PM
WEBSERVER	10016	Error	Microsoft-Windows-DistributedCOM	System	10/4/2022 7:10:15 PM
WEBSERVER	1014	Warning	Microsoft-Windows-DNS Client Events	System	10/4/2022 7:10:11 PM
WEBSERVER	1041	Error	Microsoft-Windows-DHCP-Server	System	10/4/2022 7:10:07 PM
WEBSERVER	10020	Warning	Microsoft-Windows-DHCP-Server	System	10/4/2022 7:10:07 PM
WEBSERVER	8193	Error	VSS	Application	10/4/2022 7:09:58 PM




LOCAL SERVER - SERVICES

Zobrazuje stav služieb v systéme – bežiacie a zastavené služby

SERVICES					
All services 196 total					
TASKS ▼					
Filter 🔍					
⌵					
Server Name	Display Name	Service Name	Status	Start Type	
WEBSERVER	Background Tasks Infrastructure Service	BrokerInfrastructure	Running	Automatic	⬆
WEBSERVER	Client License Service (ClipSVC)	ClipSVC	Stopped	Manual (Triggered)	
WEBSERVER	Update Orchestrator Service for Windows Update	UsoSvc	Running	Manual	
WEBSERVER	DNS Client	Dnscache	Running	Automatic (Triggered)	
WEBSERVER	WinHTTP Web Proxy Auto-Discovery Service	WinHttpAutoProxySvc	Running	Manual	
WEBSERVER	Radio Management Service	RmSvc	Stopped	Manual	
WEBSERVER	Hyper-V Heartbeat Service	vmicheartbeat	Stopped	Manual (Triggered)	⬇

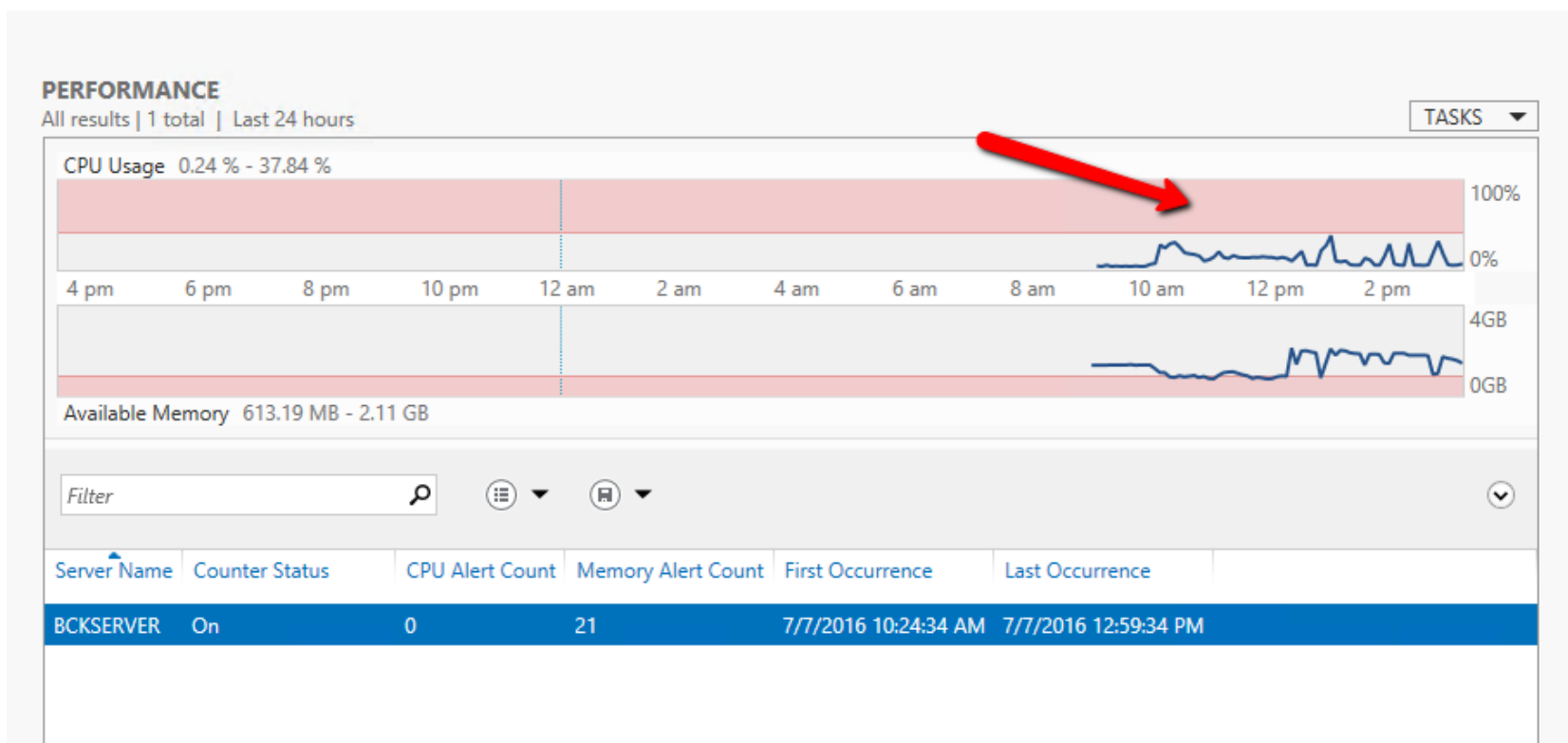
LOCAL SERVER — BEST PRACTICES ANALYZER

Obsahuje zoznam odporúčaní pre jednotlivé bežiacie služby pre zachovanie ich najlepšieho výkonu

BEST PRACTICES ANALYZER			TASKS ▼
Warnings or Errors 20 of 71 total			
Filter <input type="text"/> 🔍  ▼  ▼ 			
Filter applied. ✕ Clear All			
Server Name	Severity	Title	
WEBSERVER	Warning	DNS: Ethernet should have static IPv4 settings	
WEBSERVER	Warning	DNS: Root hint server 2001:500:2::c must respond to NS queries for the root zone.	
WEBSERVER	Warning	DNS: Root hint server 2001:dc3::35 must respond to NS queries for the root zone.	
WEBSERVER	Warning	DNS: Root hint server 2001:503:ba3e::2:30 must respond to NS queries for the root zone.	
WEBSERVER	Warning	DNS: Root hint server 2001:7fe::53 must respond to NS queries for the root zone.	
WEBSERVER	Warning	DNS: Root hint server 2001:7fd::1 must respond to NS queries for the root zone.	
WEBSERVER	Warning	DNS: Root hint server 2001:503:c27::2:30 must respond to NS queries for the root zone.	
WEBSERVER	Error	DHCP: The server should be bound to an IPv4 address	

LOCAL SERVER - PERFORMANCE

Obsahuje grafické zobrazenie využitia procesora a voľnej pamäte na serveri






LOCAL SERVER — ROLES AND FEATURES

Zobrazuje zoznam nainštalovaný rolí (roles) a súčastí systému (features) a možnosťou ich pridania alebo odinštalovania

ROLES AND FEATURES
All roles and features | 37 total

TASKS ▼

🔍  ▼  ▼ 

Server Name	Name	Type	Path
WEBSERVER	Web Server (IIS)	Role	Web Server (IIS)
WEBSERVER	Windows Defender	Feature	Windows Defender Features\Windows Defender
WEBSERVER	GUI for Windows Defender	Feature	Windows Defender Features\GUI for Windows Defender
WEBSERVER	Remote Server Administration Tools	Feature	Remote Server Administration Tools
WEBSERVER	Role Administration Tools	Feature	Remote Server Administration Tools\Role Administration Tools
WEBSERVER	DNS Server Tools	Feature	Remote Server Administration Tools\Role Administration Tools\DNS Server Tools

< >



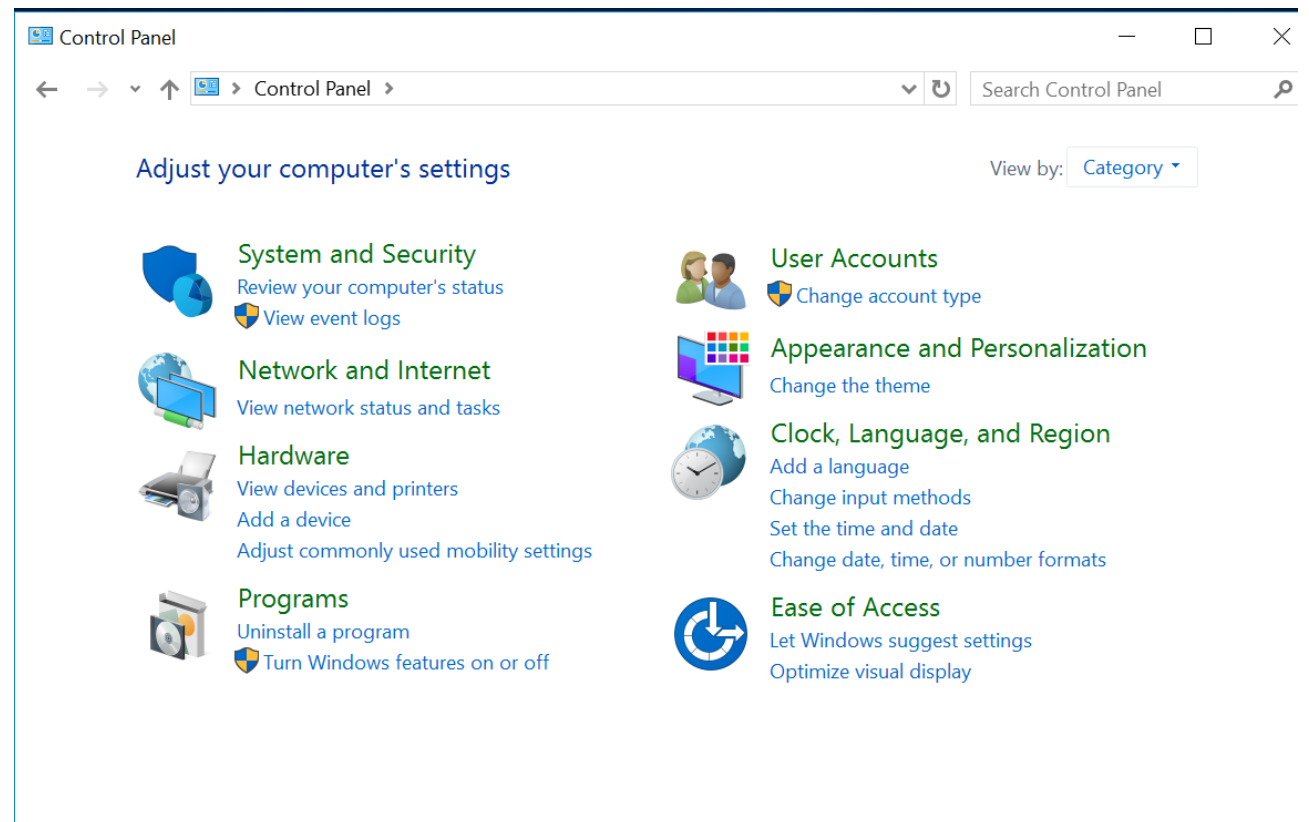
CONTROL PANEL

Panel nástrojov

CONTROL PANEL

Umožňuje spravovať ďalšie nastavenia operačného systému Windows Server

Nastavenia môžu byť zoskupené podľa kategórií alebo môžu byť zobrazené všetky nastavenia voľbou View by: Large icons



CONTROL PANEL



Administrative Tools

- zobrazí zoznam nástrojov na správu rolí a súčastí systému



AutoPlay

- zobrazí možnosti automatického spúšťania vložených médií



Color Management

- správa farieb pre lepšie zobrazenie na monitore



Credential Manager

- správa uložených loginov a hesiel v systéme



Date and Time

- nastavenia systémového dátumu a času



Default Programs

- predvolené programy pre zobrazovanie obrázkov, videí ...



Device Manager









- správa hardvéru v počítači, inštalácia ovládačov



Devices and Printers

- správa periférií – faxy, skenery, tlačiarne ...

CONTROL PANEL

-  Display
 - zobrazí nastavenia displeja (rozlíšenie, veľkosť textu ...)
-  Ease of Access Center
 - možnosti uľahčenia práce pre ľudí so zdravotným znevýhodnením
-  File Explorer Options
 - možnosti prieskumníka súborov
-  Fonts
 - správa písiem v systéme
-  Indexing Options
 - nastavenia indexácie súborov pre rýchlejšie vyhľadávanie
-  Internet Options
 - možnosti internetu (bezpečné zóny, proxy, certifikáty, história...)
-  iSCSI Initiator
 - umožňuje pripojenie vzdialených diskov cez zbernicu iSCSI
-  Keyboard
 - nastavenie správania klávesnice

CONTROL PANEL



Language

- nastavenia jazyka systému a rozloženia klávesnice



Mouse

- nastavenie správania myši



Network and Sharing Center

- nastavenia siete a VPN



Personalization

- nastavenia farebných schém, pozadia plochy ...



Phone and Modem

- nastavenia pripojenia do siete cez modem



Power Options

- možnosti napájania, zmena režimu výkonnosti a šetrenia energie



Programs and Features

- umožňuje spravovať nainštalované programy a súčasti systému



Recovery

- nastavenia tvorby záloh a obnovy systému

CONTROL PANEL



Region

- zmena regionálnych nastavení (zobrazenie času, desat. čiarky ...)



RemoteApp and Desktop
Connections

- spravovanie vzdialených pripojení na tento server



Security and Maintenance

- nastavenia bezpečnostných hlásení, UAC, riešenie problémov



Sound

- nastavenia systémového zvuku



Speech Recognition

- nastavenia rozpoznávania reči pre hlasové ovládanie



Sync Center

- nastavenia synchronizácie zdieľaných priečinkov a súborov



System

- zmena mnohých systémových nastavení (meno servera, doména ...)



Taskbar and Navigation

- nastavenia ponuky štart a panela úloh

CONTROL PANEL



Text to Speech

- nastavenia syntetizátora reči pre prevod textu na reč



Troubleshooting

- riešenie problémov s programami, hardvérom, sieťami, bezpečnosťou



User Accounts

- správa používateľských účtov, systémových premenných, šifrovanie



Windows Defender

- nastavenia antivírusového riešenia od Microsoftu



Windows Firewall

- nastavenia filtrovania sieťovej prevádzky (firewall)



Windows Mobility Center

- rýchle nastavenia jas, zvuku, viacerých monitorov, energ. profilu



EVENT VIEWER

Zobrazovač udalostí (logy)

Event Viewer

FileActionViewHelp

Event Viewer (Local)

Custom Views

Server Roles

Administrative Events

Windows Logs

Application

Security

Setup

System

Forwarded Events

Applications and Services Logs

DNS Server

Hardware Events

Internet Explorer

Key Management Service

Microsoft

Windows PowerShell

Subscriptions

Event Viewer (Local)

Overview and Summary

Last refreshed: 10/4/2022 9:14:48 PM

Overview

To view events that have occurred on your computer, select the appropriate source, log or custom view node in the console tree. The Administrative Events custom view contains all the administrative

Summary of Administrative Events

Event Type	Event ID	Source	Log	Last hour
Critical	-	-	-	0

Recently Viewed Nodes

Name	Description	Modified	Create
Windows Logs\Forwarded...	N/A		

Log Summary

Log Name	Size (Current)	Modified	Enabled
Application	1.07 MB/2...	10/4/2022 8:29:31 PM	Enabled

Actions

Event Viewer (Local)

Open Saved Log...

Create Custom View...

Import Custom View...

Connect to Another Computer...

View

Refresh

Help

EVENT VIEWER

Nástroj na prezeranie udalostí (eventov), ktoré vznikli v systéme

Udalosti zapisujú programy a služby (programátori pri ošetrovaní rôznych chýb a udalostí vo svojich aplikáciách využili funkcie operačného systému, ktoré im umožňujú zapisovať tieto udalosti do spoločnej databázy)

Každý program, služba alebo komponent v systéme môže zapisovať údaje o svojom štandardnom alebo neštandardnom správaní do denníka (logu), kde sa dajú pozrieť cez program Event Viewer

EVENT VIEWER

Je to mechanizmus zapisovania denníkov vstavaný do Windows systémov

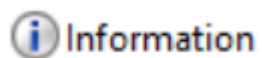
Uchováva záznamy z operačného systému

Uchováva záznamy z aplikácií nainštalovaných do systému

Je veľmi užitočný pri odhaľovaní problémov

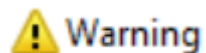
Je tiež užitočný pre riešenie bezpečnostných incidentov

ÚROVNE HLÁSENÍ



Information

- bežný chod programu, nastala nejaká zmena stavu, vykonalo sa úspešné nastavenie, podarila sa nejaká operácia



Warning

- nastala nejaká neštandardná situácia (napr. málo miesta na disku), ktorá neumožnila úplné fungovanie programu, ale neohrozila jeho chod; program sa zotavil po neočakávanej udalosti



Error

- vážny problém, ktorý mohol mať za následok stratu dát, neočakávané ukončenie programu, stratu funkcionality, zlyhanie jeho spustenia, alebo príslušnej služby



Audit Success

- bezpečnostná udalosť, ktorá umožnila vykonanie príslušnej operácie (vstup do systému, prístup k priečinku, otvorenie programu ...)



Audit Failure

- bezpečnostná udalosť, ktorá neumožnila vykonanie príslušnej operácie (zadanie zlého hesla, nedostatočné práva pre otvorenie súboru...)

HLAVNÉ DENNÍKY (LOGY)

Application

- Obsahuje informácie od doplnkových programov Windowsu

Security

- Obsahuje informácie o prístupe k zdrojom, prihláseniach a odhláseniach do systému, prístupu k súborom

Setup

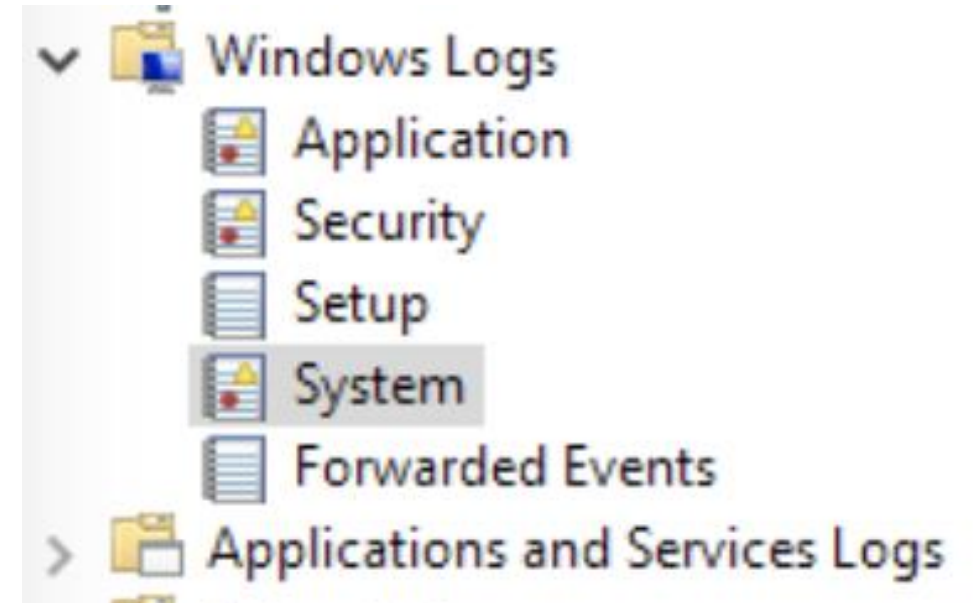
- Obsahuje informácie o inštalácií programov, updatov, rolí a súčastí systému

System

- Obsahuje informácie o problémoch s hardvérom, ovládačmi, sieťou a ďalšími core súčast'ami systému

Application and Services

- Obsahuje detailnejšie informácie od súčastí systému + informácie od nainštalovaných programov tretích strán



ŠTRUKTÚRA ZÁZNAMOV V DENNÍKU

Log Name – umiestnenie logu

- Application, System, Security

Event ID

- Unikátne číslo, ktoré korešponduje so špecifickým správaním danej aplikácie, špecifickou chybou a pod.

Log Level

- Information, Warning, Error

Message

- Podrobnejšia správa o danom hlásení v logu

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	DESKTOP-82A5J9C\$
Account Domain:	WORKGROUP
Logon ID:	0x3E7

Log Name: Security

Source: Microsoft Windows security : Logged: 4/5/2018 9:21:22 AM

Event ID: 4624 Task Category: Logon

Level: Information Keywords: Audit Success

User: N/A Computer: DESKTOP-82A5J9C

OpCode: Info

More Information: [Event Log Online Help](#)

Copy Close

PRÍKLAD NIEKTORÝCH EVENTOV — SEXY SIX

Šesť eventov, ktoré používajú bezpečnostní analytici pre vyšetrovanie incidentu:

4688/592 (Security) — New Process executed

- Spustil sa nový proces, ktorý mohol byť škodlivým kódom
- Nie všetky procesy sú zlé

4624/528/540 (Security) — Account logged in

- Útočník sa mohol prihlásiť do systému
- Samozrejme, nie všetky loginy sú zlé
- **4625** — Failed logon attempt

5140/560 (Security) — A share was accessed

- Bol vykonaný prístup do zdieľanej zložky
- Útok sa šíri ďalej po sieti

PRÍKLAD NIEKTORÝCH EVENTOV — SEXY SIX

5156 (Security) — Windows Firewall Network connection by process

- Proces sa snaží vytvoriť nové spojenie po sieti
- Možnosť zapojenia počítača do Botnetu alebo pripojenie cez RAT

7045/601 (System) — New Service installed

- Nové služby sa spúšťajú po inštalácii programov alebo aktualizáciách, nemajú dôvod sa spúšťať inak

4663/567 (Security) — File and Registry auditing

- Modifikácie nastavení systému, vytváranie súborov

PRÍKLAD ĎALŠÍCH EVENTOV

4720 (Security) – A user account was created

- Útočník si mohol vytvoriť účet pre vzdialený prístup

4732/4728 (Security) - A member was added to a group

- Útočník si mohol pridať svoj účet do skupiny s vyššími privilégiami (Operators, Admins ...)

ČO SA VŠETKO LOGUJE

Nová inštalácia Windowsu prichádza s prednastavenou sadou toho, čo sa má zapisovať do logov

Ak by sme zapisovali do logov všetko, viedlo by to k zahlteniu procesora, pamäte a disku samotným monitorovaním všetkých parametrov a zápismi do logov

Špecializovaný monitoring súčastí systému je možné zapnúť cez nástroj Lokálnych politík zabezpečenia (gpedit.msc)

PRÍKLAD ZAPNUTIA LOGOVANIA PROCESOV

Computer Configuration → Windows Settings → Security Settings → Advanced Audit Policy Configuration → System Audit Policies → Detailed Tracking

Audit Process Creation → Configure following audit events: Success, Failure

Computer Configuration → Administrative Templates → System → Audit Process Creation

Include command line in process creation events: Enable

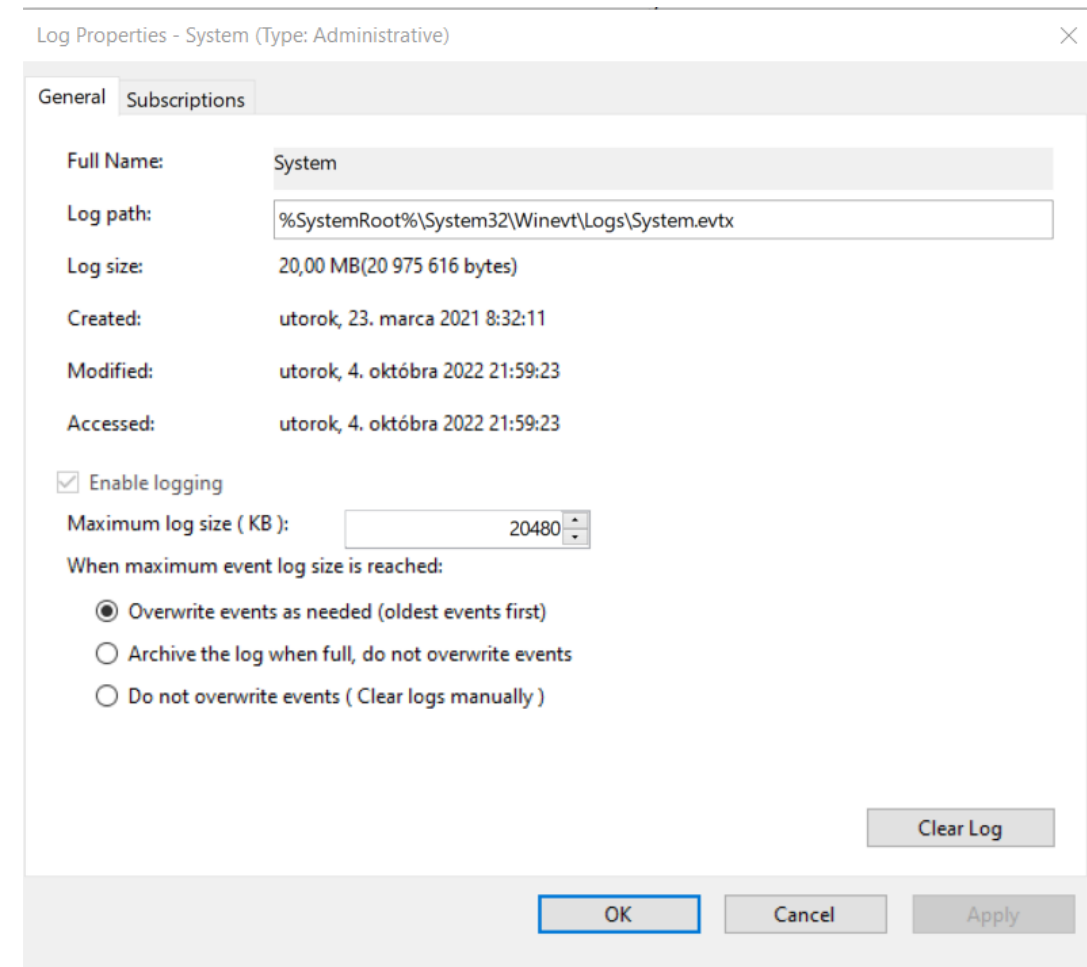
NASTAVENIA LOGOVANIA

Kliknutím cez pravé tlačidlo myši na konkrétny log a voľbou Properties (Vlastnosti)

Je možné nastaviť veľkosť súboru pre logovanie (teda ako ďaleko do histórie „vidíme“)

Možné akcie po zaplnení logu:

- Staré záznamy sa postupne vymazávajú a nahrádzajú novšími
- Súbor sa uzatvorí, pridá sa k nemu poradové číslo a otvorí sa nový
- Prestane sa zapisovať do denníka



FILTROVANIE V LOGOCH

V pravom paneli je možné kliknutím na „Filter current log“ vytvoriť filter na základe:

- Kritikalita (information, error, warning)
- Zdroja (aplikácia alebo súčasť systému)
- Event ID (jednotlivo alebo cez rozsahy vymedzené pomlčkou)
- Kľúčových slov
- Používateľského účtu, pod ktorým sa záznam vytvoril
- Počítača, ktorý záznam vytvoril (pri sumarizácii logov)

Filter Current Log

Filter XML

Logged: Any time

Event level: ☐ Critical ☐ Warning ☐ Verbose
☐ Error ☐ Information

☒ By log Event logs: System

☐ By source Event sources:

Includes/Excludes Event IDs: Enter ID numbers and/or ID ranges separated by commas. To exclude criteria, type a minus sign first. For example 1,3,5-99,-76

<All Event IDs>

Task category:

Keywords:

User: <All Users>

Computer(s): <All Computers>

Clear

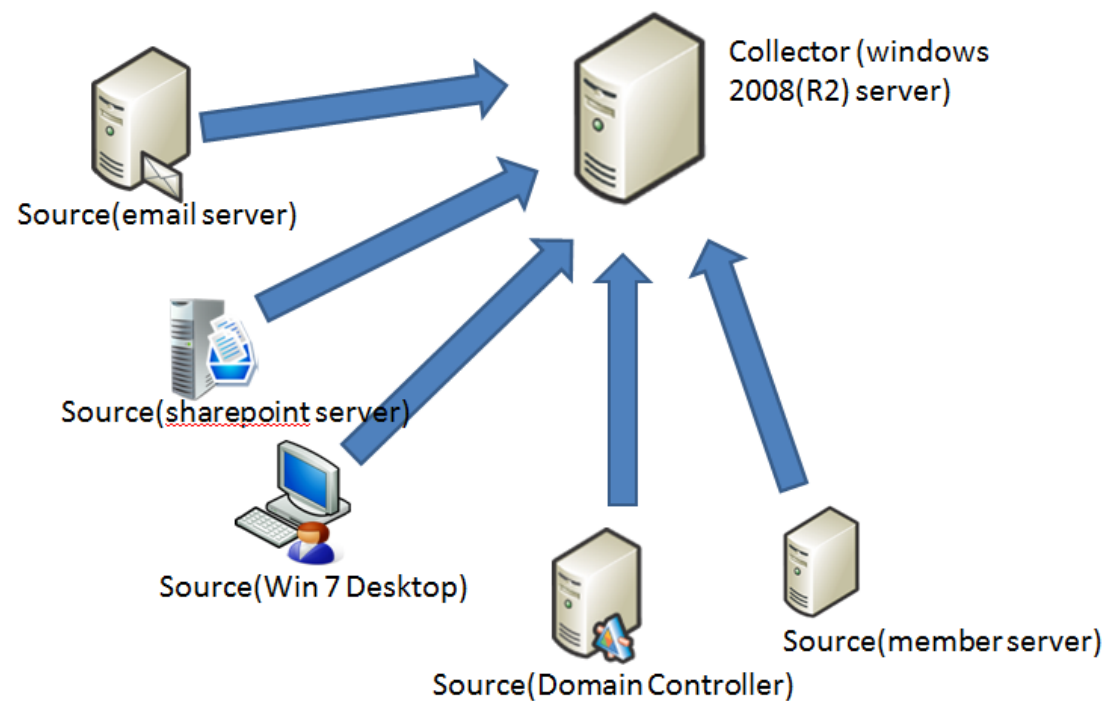
OK Cancel

SUMARIZÁCIA LOGOV

Počítače môžeme nastaviť tak, aby svoje (vybrané) logy zasielali na centrálny zberný počítač (collector)

To nám umožňuje lepšiu kontrolu nad tým, čo sa na počítačoch v sieti deje, rýchlejšiu detekciu bezpečnostných incidentov, či riešenie problémov

Na zdrojových počítačoch musíme definovať tzv. subscription



SUBSCRIPTION

Subscription obsahuje:

- Meno (a popis)
- Cieľ, kam sa majú logy ukladať
- Kto vyvoláva zápis – kolektor alebo zdrojový počítač
- Zoznam udalostí pre zber (definuje sa rovnako ako filter log)
- Účet, pod ktorým sa majú kontaktovať vzdialené počítače pre zber logov

