

Windows Server, PowerShell и WMI

Урок 2. Установка и настройка Windows Server

Домашнее задание:

1. Создайте нового пользователя, с необходимостью смены пароля при первом входе в систему и добавьте его в группу Пользователи удаленного рабочего стола

Full name:

Description:

☒ User must change password at next logon

☐ User cannot change password

☐ Password never expires

☐ Account is disabled

☐ Account is locked out

gb-test-user Properties

Remote control Remote Desktop Services Profile Dial-in

General Member Of Profile Environment Sessions

Member of:

- Remote Desktop Users
- Users

2. Остановите и запустите службу SSTP (SstpSvc) из графической оболочки и из командной строки

```
Get-Service -Name SstpSvc | Stop-Service
Get-Service -Name SstpSvc | Start-Service
```

Secure Socket Tunneling Protocol Service	Name	Description	Status	Startup Type
<p>Stop the service</p> <p>Restart the service</p> <p>Description: Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.</p>	Remote Registry	Enables rem...		Automatic (T
	Resultant Set of Policy Provi...	Provides a n...		Manual
	Routing and Remote Access	Offers routi...		Disabled
	RPC Endpoint Mapper	Resolves RP...	Running	Automatic
	Secondary Logon	Enables star...		Manual
	Secure Socket Tunneling Pr...	Provides su...	Running	Manual
	Security Accounts Manager	The startup ...	Running	Automatic
	Sensor Data Service	Delivers dat...		Manual (Trig.
	Sensor Monitoring Service	Monitors va...		Manual (Trig.
	Sensor Service	A service fo...		Manual (Trig.
	Server	Supports fil...	Running	Automatic

Secure Socket Tunneling Protocol Service

[Start](#) the service

Description:
Provides support for the Secure Socket Tunneling Protocol (SSTP) to connect to remote computers using VPN. If this service is disabled, users will not be able to use SSTP to access remote servers.

Name	Description	Status
Remote Registry	Enables rem...	
Resultant Set of Policy Provi...	Provides a n...	
Routing and Remote Access	Offers routi...	
RPC Endpoint Mapper	Resolves RP...	Running
Secondary Logon	Enables star...	
Secure Socket Tunneling Pr...	Provides su...	
Security Accounts Manager	The startup ...	Running
Sensor Data Service	Delivers dat...	
Sensor Monitoring Service	Monitors va...	
Sensor Service	A service fo...	
Server	Supports fil	Running

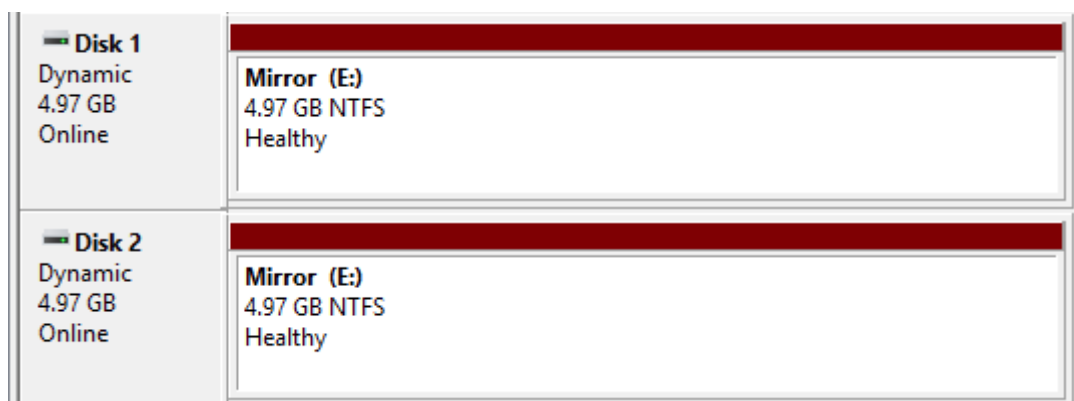
3. Сожмите том, создайте раздел, потом верните в исходное состояние

Disk 0 Basic 15.00 GB Online	System Reserved 500 MB NTFS Healthy (System, Active, Prim	(C:) 13.51 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary	1.00 GB Unallocated
Disk 0 Basic 15.00 GB Online	System Reserved 500 MB NTFS Healthy (System, Active, Prim	(C:) 13.51 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary	Poor (E:) 1023 MB NTFS Healthy (Primary Partition)
Disk 0 Basic 15.00 GB Online	System Reserved 500 MB NTFS Healthy (System, Active, Primary Partition)	(C:) 14.51 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Partition)	

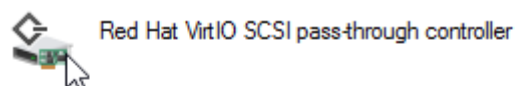
4. Подключите второй диск, преобразуйте его в GPT

Disk 0 Basic 15.00 GB Online	System Reserved 500 MB NTFS Healthy (System, Active, Primary	(C:) 14.51 GB NTFS Healthy (Boot, Page File, Crash Dump, Primary Parti
Disk 1 Basic 4.97 GB Online	4.97 GB Unallocated	

5. Добавьте третий диск, создайте из 2 и 3 диска зеркальный том



6. Найдите ИД оборудования (pci\ven например контроллер жесткого диска или видеокарта) и сайт в интернете, откуда можно скачать драйвера для этого устройства



Property

Hardware Ids

Value

PCI\VEN_1AF4&DEV_1004&SUBSYS_00081AF4&REV_00
PCI\VEN_1AF4&DEV_1004&SUBSYS_00081AF4
PCI\VEN_1AF4&DEV_1004&CC_010000
PCI\VEN_1AF4&DEV_1004&CC_0100



Windows Guest Virtual Machines on Red Hat Enterprise Linux...

[access.redhat.com > articles/2470791](https://access.redhat.com/articles/2470791) копия ещё

VEN_1AF4&DEV_1004 or VEN_1AF4&DEV_1048, the SCSI block device. ...

VEN_QEMU&DEV_0001, the guest panic device. Right-click the device whose driver you wish to ... Find the device in the Multifunction adapters group (1x QEMU PCI Serial Card), Network adapters group (Red Hat VirtIO Ethernet Adapter)...

7. В диспетчере задач отфильтруйте приложения которые больше всего потребляют ресурсов процессора и оперативную память

Name	PID	Status	User name	CPU	Memory (p...	Description
MsMpEng.exe	1584	Running	SYSTEM	64	184,440 K	Antimalware Service Exe...
svchost.exe	1004	Running	SYSTEM	02	25,068 K	Host Process for Windo...
dwm.exe	792	Running	DWM-1	01	24,616 K	Desktop Window Mana...
explorer.exe	2812	Running	Administr...	00	23,004 K	Windows Explorer
WmiPrvSE.exe	3380	Running	SYSTEM	00	19,660 K	WMI Provider Host
TiWorker.exe	828	Running	SYSTEM	00	17,216 K	Windows Modules Insta...
ShellExperienceHost....	3064	Suspended	Administr...	00	15,108 K	Windows Shell Experien...
svchost.exe	860	Running	LOCAL SE...	00	13,280 K	Host Process for Windo...
System Idle Process	0	Running	SYSTEM	00	0 K	System Idle Process
Name	PID	Status	User name	CPU	Memory (p...	Description
mscorsvw.exe	4908	Running	SYSTEM	32	14,328 K	.NET Runtime Optimizat...
MsMpEng.exe	1584	Running	SYSTEM	26	164,744 K	Antimalware Service Exe...
TiWorker.exe	828	Running	SYSTEM	23	26,204 K	Windows Modules Insta...
DismHost.exe	5076	Running	Administr...	08	1,536 K	Dism Host Servicing Pro...
System	4	Running	SYSTEM	05	28 K	NT Kernel & System
System Idle Process	0	Running	SYSTEM	04	4 K	Percentage of time the ...
Taskmgr.exe	5040	Running	Administr...	02	8,612 K	Task Manager
System interrupts	-	Running	SYSTEM	00	0 K	Deferred procedure calls...
dwm.exe	792	Running	DWM-1	00	24,616 K	Desktop Window Mana...

8. Отфильтруйте системные события с кодом 6013 или 7036

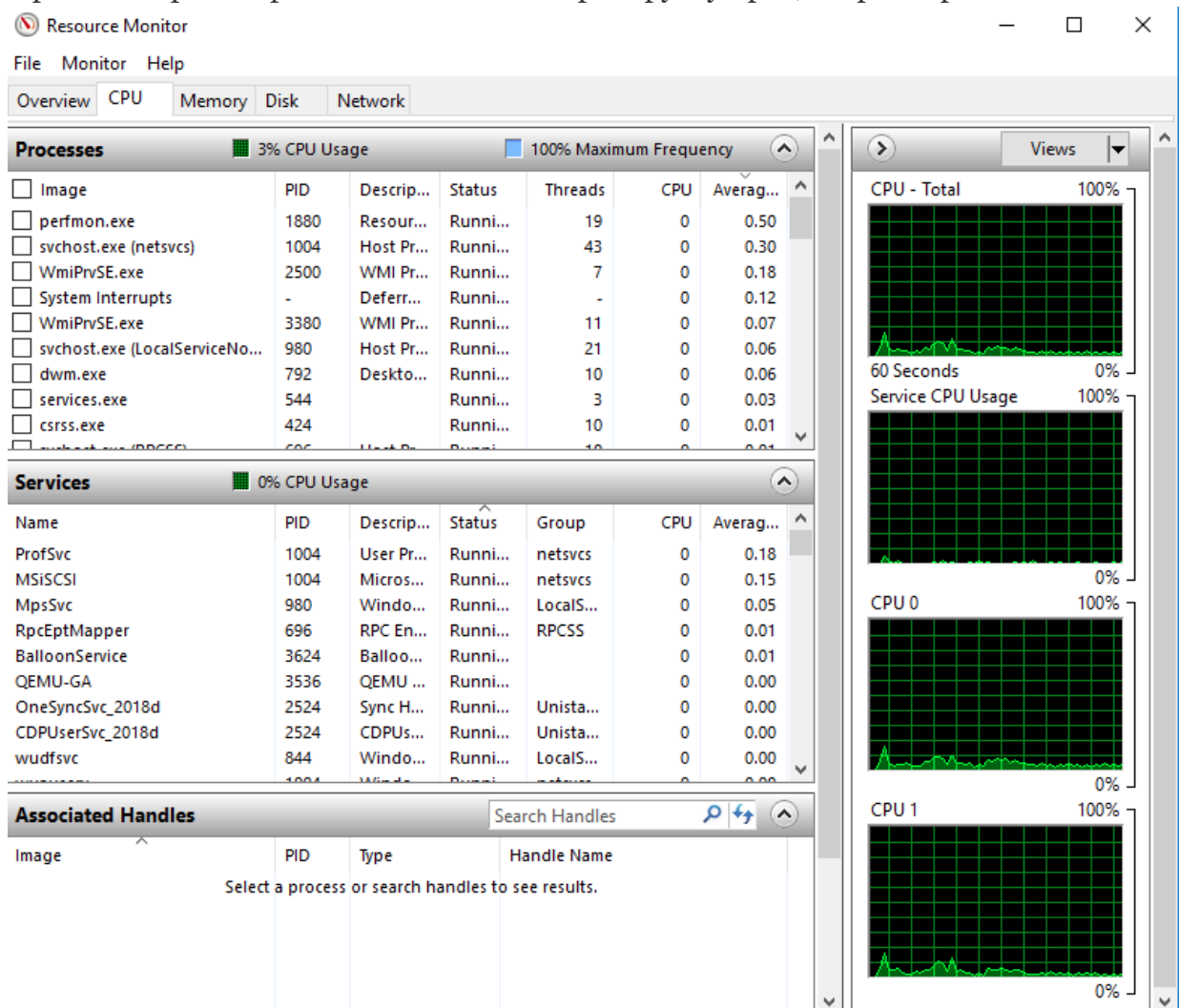
System Number of events: 875				
Filtered: Log: System; Source: ; Event ID: 6013,7036. Number of events: 594				
Level	Date and Time	Source	Event ID	Task C...
Information	3/31/2022 4:52:57 AM	Service...	7036	None
Information	3/31/2022 4:52:55 AM	Service...	7036	None
Information	3/31/2022 4:52:55 AM	Service...	7036	None
Information	3/31/2022 4:52:55 AM	Service...	7036	None
Information	3/31/2022 4:52:21 AM	Service...	7036	None
Information	3/31/2022 4:51:40 AM	Service...	7036	None
Information	3/31/2022 4:51:25 AM	Service...	7036	None
Information	3/31/2022 4:51:13 AM	Service...	7036	None
Information	3/31/2022 4:50:46 AM	Service...	7036	None
Information	3/31/2022 4:50:21 AM	Service...	7036	None

```
Get-EventLog -LogName System | ?{$_.EventID -in 6013,7036}
```

9. Создайте задание, которое будет в 14.00 в рабочие дни запускать команду ping 8.8.8.8

```
PS C:\Users\Administrator> Get-ScheduledTask -TaskName "PING 8.8.8.8" | Select * | FL
State                : Ready
Actions              : {MSFT_TaskExecAction}
Author               : WIN-DCVFC0N41AU\Administrator
Date                : 2022-03-31T04:58:48.5826026
Description          :
Documentation        :
Principal            : MSFT_TaskPrincipal2
SecurityDescriptor   :
Settings             : MSFT_TaskSettings3
Source              :
TaskName             : PING 8.8.8.8
TaskPath             : \
Triggers             : {MSFT_TaskWeeklyTrigger}
URI                 : \PING 8.8.8.8
Version              :
PSComputerName       :
CimClass             : Root/Microsoft/Windows/TaskScheduler:MSFT_ScheduledTask
CimInstanceProperties : {Actions, Author, Date, Description...}
CimSystemProperties  : Microsoft.Management.Infrastructure.CimSystemProperties
```

10. Промониторьте через Системный монитор загрузку процессора и пришлите лог



11. Через Монитор ресурсов просмотрите в разделе Диск-Процессы с дисковой активностью-System какие используются файлы

Processes with Disk Activity				
<input type="checkbox"/> Image		Read (B/sec)	Write (B/sec)	Total (B/sec)
<input type="checkbox"/> System	4	0	4,868	4,868
<input type="checkbox"/> perfmon.exe	1880	228	0	228

Disk Activity						
		0 KB/sec Disk I/O		1% Highest Active Time		
Image	PID	File	Read ...	Write...	Total ...	I/O Pr... Resp
System	4	C:\ProgramData\Microsoft\Windows Defender\Scans\mpengine.db-wal	0	2,150	2,150	Nor...
System	4	C:\\$Extend\\$UsnJrnl:\$J	0	26	26	Nor...
perfmon.exe	1880	C:\Windows\System32\wdc.dll	228	0	228	Nor...
System	4	C:\Users\Administrator\ntuser.dat.LOG1	0	610	610	Nor...
System	4	C:\\$LogFile (NTFS Volume Log)	0	3,687	3,687	Nor...
System	4	C:\Windows\ServiceProfiles\LocalService\AppData\Local\lastalive0.dat	0	146	146	Nor...
System	4	C:\\$Mft (NTFS Master File Table)	0	205	205	Nor...
System	4	C:\Windows\System32\winevt\Logs\Microsoft-Windows-WMI-Activity%4Ope...	0	640	640	Nor...
System	4	C:\Windows\ServiceProfiles\LocalService\AppData\Local	0	68	68	Nor...
System	4	C:\\$BitMap (NTFS Free Space Map)	0	68	68	Nor...

