



O MAIOR FESTIVAL HACKER DA AMERICA LATINA

ROADSEC

2022



黑客文化



Windows logon: dos logs aos processos

Marcus Oliveira

Especialista de Cyber
Segurança



Disclaimer

Essa palestra é um estudo pessoal e não tem relação com a empresa a qual trabalho.

O intuito é divulgar conhecimento, não me responsabilizando pelo o que terceiros possam fazer com ele.

\$whoami



Marcus Oliveira
Especialista em Cyber
Segurança

- Twitter: @Marcus_mcs
- E-mail: marcus.oliveira5@fatec.sp.gov.br
- Telegram: @mvvamo
- Linkedin: <https://www.linkedin.com/in/mvmoliveira/>
- Não sou o CR7
- Tricolor Fanático
- Pratico natação e musculação
- Purple Team mindset
- 8 anos de experiência em TI/SI
- Tecnólogo em Segurança da Informação pela Fatec São Caetano do Sul
- Focos de estudo e pesquisa:
 - Segurança Ofensiva (Red Team)
 - Segurança Defensiva (Blue Team)
 - Buffer Overflow



Agenda

O que é uma sessão?

 O que é um logon?

Logs/eventos de logon

 Windows Authentication Architecture

Cenários



 Processo de logon

Dúvidas?



 Referências



O que é um logon?



O que é um logon?

Segundo Chirag Savla, logon é:

- “In simple words logon is a process of gaining access to local or remote systems using valid credentials. The user information is validated by Local Security Authority (LSA), incase of local account it will verify the information from Security Accounts Manager (SAM) database and incase of domain account it will verify the information from the Domain Controller.”

O que é uma sessão?



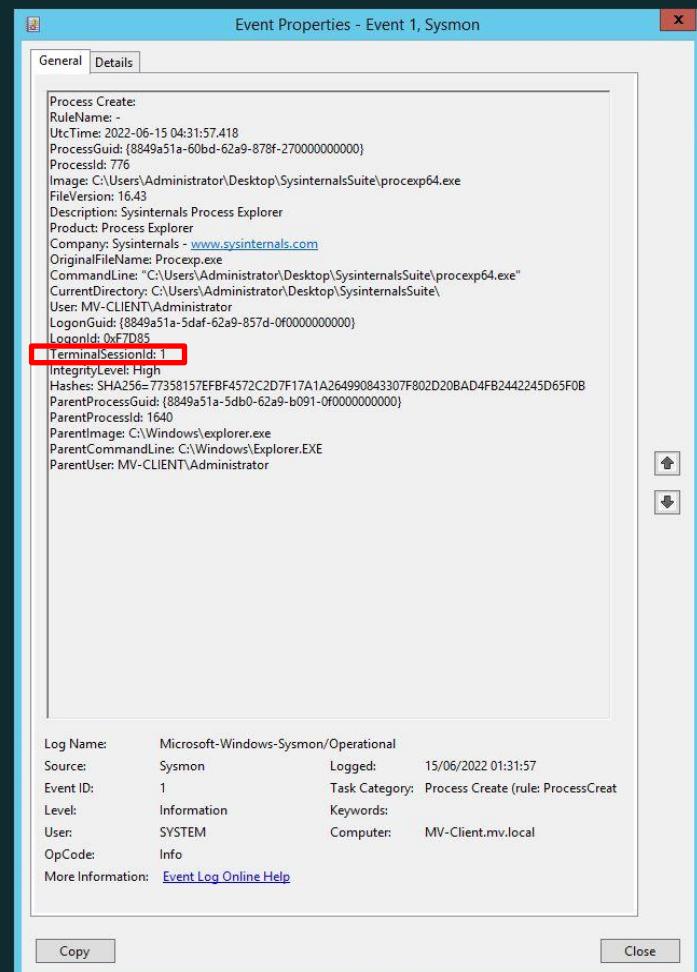
O que é uma sessão?

- Segundo Craig Marcho sessão é:
 - “A session consists of all of the processes and other system objects that represent a single user’s logon session.”
- Cada sessão recebe um número, sendo 0 sempre a do sistema operacional e cada logon de usuário vai recebendo n+1 como número de sessão.
- No Sysmon o campo TerminalSessionId no EventID 1, mostra a sessão do usuário que originou o processo.

```
Windows PowerShell

PS C:\Users\Administrator> quser
USERNAME          SESSIONNAME
administrator      console
bob               rdp-tcp#1
PS C:\Users\Administrator>
PS C:\Users\Administrator>
PS C:\Users\Administrator> qwinsta
SESSIONNAME      USERNAME
services
>console        Administrator
rdp-tcp#1       bob
rdp-tcp
PS C:\Users\Administrator>
```

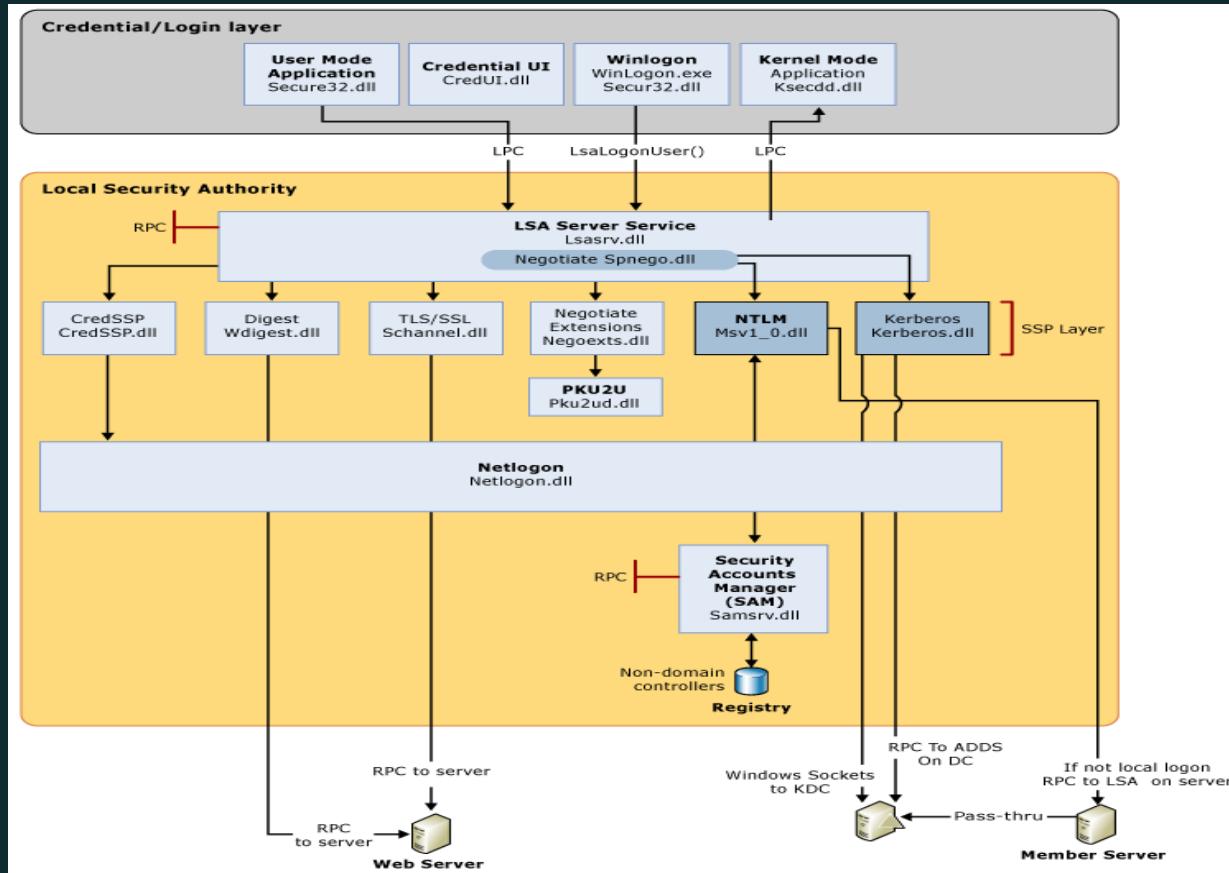
SESSIONNAME	USERNAME	ID	STATE	TYPE	DEVICE
services		0	Disc		
>console	Administrator	1	Active		
rdp-tcp#1	bob	2	Active		
rdp-tcp		65536	Listen		



Windows Authentication Architecture



Windows Authentication Architecture



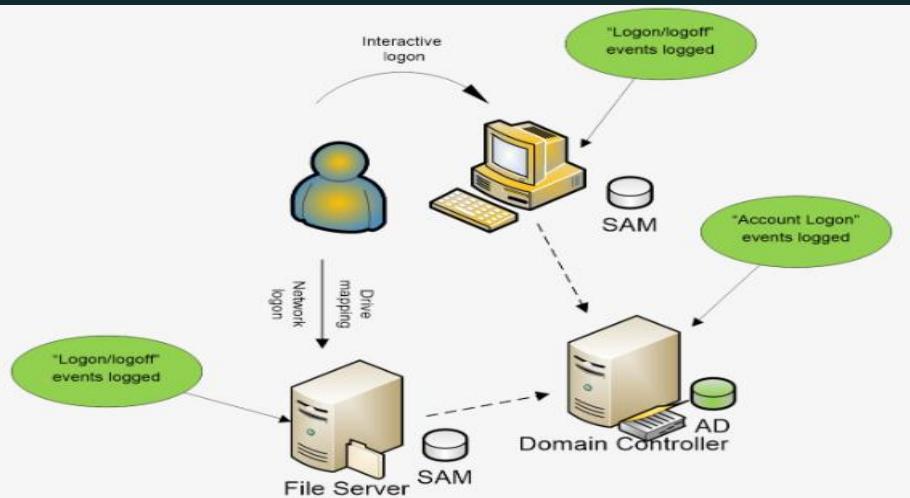
Account logon events vs Logon events



Account logon events VS Logon events

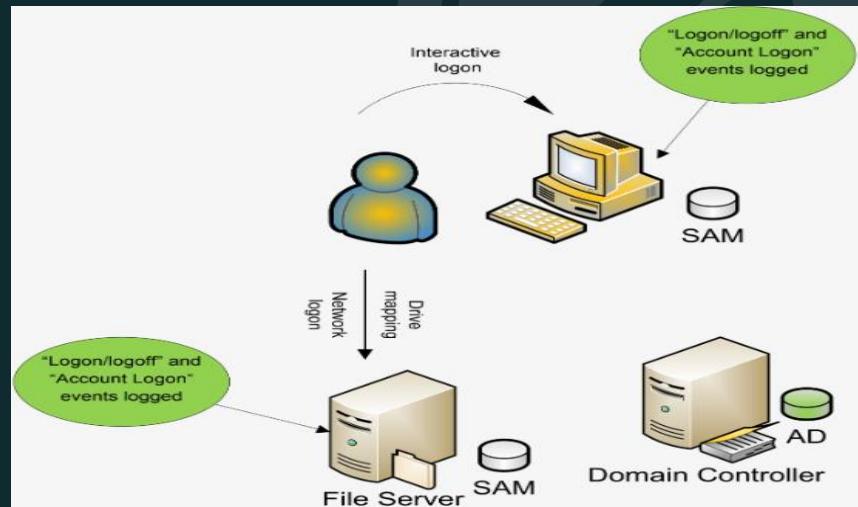
Account Logon Events:

- Corresponde a categoria Audit account logon events nas politicas de auditoria
- Autenticação (ocorre onde o usuário reside)



Logon Events:

- Corresponde a categoria Audit logon events nas politicas de auditoria
- Logon Sessions (ocorre onde o usuário está obtendo acesso ao sistema)



Logs/eventos de Account logon



Logs/eventos de Account logon

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
672	672	4768	An authentication service (AS) ticket was successfully issued and validated (2000). An authentication service (AS) ticket was requested (2008). It is logged on DC Only.
673	673	4769	A ticket granting service (TGS) ticket was granted. Win2003 and Win2008 use this for both successful and failed service ticket requests with the proper Kerberos result/failure code.
674	674	4770	A security principal renewed an AS ticket or TGS ticket.
675	675	4771	Preattentation failed. This event is generated on a Key Distribution Center (KDC) for the Kerberos errors during authentication.
676	672	4768	Authentication ticket request failed. See the Kerberos Error Code.
677	673	4769	A TGS ticket was not granted (failed). This event 677 in Windows 2000 is replaced with 673 in Windows XP/2003 family) and 4769 with later versions with audit type/codes for failures.
678	678	4774	An account was successfully mapped for logon to a domain account. Not common.
680	680	4776	Account used for logon by. Logged for local user (local SAM) authentication. DC logs this event for NTLM authentication.
681	680	4776	Logon failure on Windows 2000 for NTLM authentication. A domain account logon was attempted. This event is replaced with 680 in Windows XP/2003 family and 4776 with Windows 2008/Vista onwards with the audit type/codes for failures.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

Logs/eventos de logon



Logs/eventos de logon

Windows 2000 Family	Windows XP & 2003 Family	Windows Vista, 7, 8 & 2008, 2012 Family	Description
528	528	4624	Successful logon: A user successfully logged on to a computer. For information about the type of logon, see the next section.
529	529	4625	Logon failure. A logon attempt was made with an unknown user name or a known user name with a bad password. For Windows 2008 and above, event ID 4625 logs every failed logon attempt with failure status code regardless of logon type or type of account.
530	530	4625	Logon failure for a logon attempt to log on outside of the allowed time.
531	531	4625	Logon failure for a logon attempt using a disabled account.
532	532	4625	Logon failure for a logon attempt using an expired account.
533	533	4625	Logon failure. A logon attempt was made by a user who is not allowed to log on at this computer.
534	534	4625	Logon failure. The user attempted to log on with a type that is not allowed.
535	535	4625	Logon failure. The password for the specified account has expired.
536	536	4625	Logon failure. The Net Logon service is not active.
537	537	4625	Logon failure. The logon attempt failed for other reasons. In some cases, the reason for the logon failure may not be known.
538	538	4634	The logoff process was completed for a user.
539	539	4625	Logon failure. The account was locked out at the logon.
540	540	4624	Successful network logon: A user successfully logged on over a network.
538	551	4647	A user initiated the logoff process. It is logged for Interactive and RemoteInteractive logons in place of logoff event 538/4634.
552	552	4648	A user successfully logged on to a computer using explicit credentials while already logged on as a different user.
682	682	4778	A user has reconnected to a disconnected terminal session.
683	683	4779	A user disconnected a terminal session without logging off.

Logon type:

Logon Type	Description
2	Interactive (logon at keyboard and screen of system)
3	Network (i.e. connection to shared folder on this computer from elsewhere on network)
4	Batch (i.e. scheduled task)
5	Service (Service startup)
7	Unlock (i.e. unattended workstation with password protected screen saver)
8	NetworkCleartext (Logon with credentials sent in the clear text. Most often indicates a logon to IIS with "basic authentication") See this article for more information.
9	NewCredentials such as with RunAs or mapping a network drive with alternate credentials. This logon type does not seem to show up in any events. If you want to track users attempting to logon with alternate credentials see 4648 . MS says "A caller cloned its current token and specified new credentials for outbound connections. The new logon session has the same local identity, but uses different credentials for other network connections."
10	RemoteInteractive (Terminal Services, Remote Desktop or Remote Assistance)
11	CachedInteractive (logon with cached domain credentials such as when logging on to a laptop when away from the network)

Cenários de logon

- Interactive Logon:
 - In an Interactive logon, user enters credentials into the Log On to Windows dialog box or user inserts a smart card into the smart card reader. User's authentication is then checked against the security database on the user's local computer or to an Active Directory domain. User can perform an interactive logon in two different ways:
 - Locally, when the user has direct access to the console.
 - Remotely, through Terminal Services.
- Network Logon:
 - Network logon are very common to Windows environment. They are only used after an account authentication such as user, computer, service has already taken place. For network logon, the process does not use the initial logon dialog box to enter the credentials. Instead, already established credentials for the account are used, or credentials are collected using in a different way. This is typically invisible to the user unless alternate credentials are used. Network logon confirms the users' identification to the network service such as mapped drive on another server that the user is attempting to access (Microsoft TechNet, 2003). Windows logs logon type 3 for network logons such as accessing shared folders, printers, GPOs, and most logons to IIS.

Logs/eventos de logon: 4624 - An account was successfully logged on

Event Properties - Event 4624,

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENT\$
Account Domain:	MV
Logon ID:	0x3E7

Logon Type: 10

Impersonation Level: Impersonation

New Logon:

Security ID:	MV\bob
Account Name:	bob
Account Domain:	MV
Logon ID:	0xB461F7
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0xfdfc
Process Name:	C:\Windows\System32\winlogon.exe

Network Information:

Workstation Name:	MV-CLIENT
Source Network Address:	192.168.157.131
Source Port:	0

Detailed Authentication Information:

Logon Process:	User32
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

Log Name: Security

Source: Microsoft Windows security **Logged:** 26/11/2021 15:56:08

Event ID: 4624 **Task Category:** Logon

Level: Information **Keywords:** Audit Success

User: N/A **Computer:** MV-Client.mv.local

OpCode: Info

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

Campos úteis:

- Em subject:
 - Logon Type: Determina o tipo de logon;
- New Logon:
 - Security ID: Dominio + username
 - Logon ID: Identificador único dentro da sessão
- Process Information:
 - Process Name: Nome do processo que gerou o login;
- Network Information:
 - Workstation Name: Nome do computador que fez autenticação
 - Source Network Address: IP de origem;
 - Source Port: Porta de origem
- Detailed Authentication Information:
 - Logon Process: Nome do processo de logon que realizou o login;
 - Authentication Package: Nome do pacote usado para autenticação

Logs/eventos de logon: 4648 - A logon was attempted using explicit credentials

Event Properties - Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:

Security ID:	MV\Administrator
Account Name:	Administrator
Account Domain:	MV
Logon ID:	0x863C0F
Logon GUID:	{e3a7294f-b8da-e145-5a80-ab506a2c62ff}

Account Whose Credentials Were Used:

Account Name:	bob
Account Domain:	MV
Logon GUID:	{12f7a00f-6e74-9016-d51b-cb730ec8bc78}

Target Server:

Target Server Name:	localhost
Additional Information:	localhost

Process Information:

Process ID:	0x3ec
Process Name:	C:\Windows\System32\svchost.exe

Network Information:

Network Address:	::1
Port:	0

This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.

Log Name: Security
Source: Microsoft Windows security Logged: 26/11/2021 16:02:17
Event ID: 4648 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

- Campos uteis:
 - Security ID: Dominio + username que gerou a autenticação;
- Subject:
 - Account Name: User impersonificado
 - Account Domain: Dominio do usuário impersonificado
- Account Whose Credentials...
 - Account Name: User impersonificado
- Process information:
 - Process ID: Id do processo criado;
 - Process Name: Nome do processo criado;
- Network Information:
 - Network Address: IP de origem que fez ação
 - Source Port: Porta de origem

Processo de logon



Processo de logon

Processos importantes:

- Wininit.exe:
 - A principal função desse processo é lançar a maioria das aplicações que rodam em background (segundo plano) e estão constantemente em execução. O “wininit.exe” é também responsável por iniciar o Service Control Manager (services.exe), o Local Security Authority process (lsass.exe) e o Local Session Manager (lsm.exe). Também cria a windows station (Winsta0) interativa.

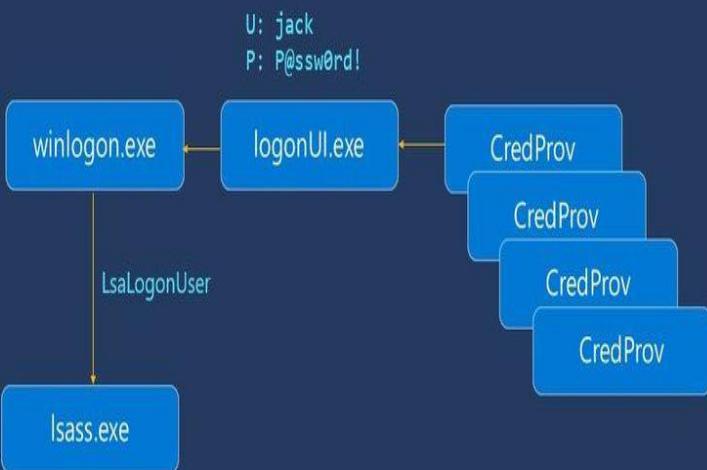
Login interativo

- Winlogon.exe:
 - Responsável pelo logon e logoff;
 - Carregar o perfil do usuário quando o usuário inicia a sessão;
 - Secure Attention Sequence (SAS): SAS é a combinação de chaves para que os usuários possam pressionar, antes do logon (Ctrl + alt + del). O winlogon.exe é responsável por assegurar que o usuário tenha uma tela segura para logar e prevenir roubo de credenciais;
 - Travar o computador e executar um protetor de tela (screensaver): O winlogon.exe é responsável por monitorar atividades do mouse e teclado, travar a tela e executar o protetor de tela (screensaver) no caso de um período de inatividade;
- LogonUI.exe:
 - Envia as credenciais para o lsass.exe;
 - Iniciado pelo winlogon.exe
- Userinit.exe :
 - Processo que inicia o shell do usuário;
- Explorer.exe:
 - Shell padrão do usuário;
 - É iniciado pelo userinit.exe.

Processo de logon

Step 1

Logon UI



Step 2

Local Security Authority

LsaLogonUser

lsass.exe

Auth Packages

Negotiate

Who supports cached logon?

NegoEx

Kerberos

NTLM



Netlogon cache

pbkdf2 @ ~10k rounds

Step 3

Logon UI Part II



Step 4

Local Security Authority Part II

LsaLogonUser

lsass.exe

Create background thread

Negotiate

Who supports online logon?

NegoEx

Kerberos

NTLM

Domain Controller

Processo de logon

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)

Process	CPU	Privat...	Work...	PID	Description	Company Name	User Name	Session	Command Line
System Idle Process	97.25	0 K	4 K	0		NT AUTHORITY\SYSTEM			
System	< 0.01	104 K	280 K	4	n/a Hardware Interrupts and DPCs	NT AUTHORITY\SYSTEM		0	
Interrupts	< 0.01	0 K	0 K			NT AUTHORITY\SYSTEM		0	
smss.exe		292 K	1.080 K	216	Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	\SystemRoot\System32\smss.exe
csrss.exe		1.604 K	3.588 K	308	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	\SystemRoot\System32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDl=basevsl.1 ServerDl=winsv:Use
csrss.exe	< 0.01	1.744 K	21.932 K	404	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	\SystemRoot\System32\csrss.exe ObjectDirectory=\\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDl=basevsl.1 ServerDl=winsv:Use
wininit.exe		716 K	3.576 K	412	Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	wininit.exe
services.exe	1.50	2.760 K	7.164 K	504	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\services.exe
svchost.exe		3.780 K	10.112 K	568	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe -k DcomLaunch
unseccapp.exe		912 K	4.112 K	1540	Link to receive asynchronous callbacks f...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wbem\unseccapp.exe -Embedding
WmiPrvSE.exe		5.908 K	11.512 K	1776	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\wbem\wmiPrvse.exe
WmiPrvSE.exe		15.848 K	21.244 K	2344	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wbem\wmiPrvse.exe
svchost.exe		2.396 K	6.256 K	598	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k RPCSS
vm3dservice.exe		940 K	3.552 K	716	VMware SVGA Helper Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\vm3dservice.exe
svchost.exe		10.004 K	13.164 K	764	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\System32\svchost.exe +k LocalServiceNetworkRestricted
svchost.exe		16.848 K	31.128 K	808	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe +k netsvcs
taskhost.exe	1.624 K	5.940 K	1228	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	0	1 taskhost.exe	
svchost.exe	5.272 K	10.864 K	852	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalService	
svchost.exe	7.900 K	16.360 K	920	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k NetworkService	
svchost.exe	6.012 K	10.084 K	280	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork	
spooler.exe		3.008 K	8.732 K	236	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\spooler.exe
Symmon64.exe		4.424 K	11.136 K	1088	System activity monitor	Sysinternals - www.s...	NT AUTHORITY\SYSTEM	0	0 C:\Windows\Symmon64.exe
svchost.exe		8.824 K	10.536 K	1156	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\svchost.exe +k LocalSystemNetworkRestricted
VGAuthService.exe	2.572 K	8.240 K	1188	VMware Guest Authentication Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"	
vmvmtold.exe	< 0.01	7.808 K	17.068 K	1240	VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Program Files\VMware\VMware Tools\vmvmtold.exe"
wlms.exe		468 K	2.604 K	1284	Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wlms.wlms.exe
svchost.exe		3.344 K	7.796 K	1660	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe +k termevs
svchost.exe		1.100 K	4.360 K	1888	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe +k NetworkServiceNetworkRestricted
dllhost.exe		3.156 K	9.988 K	2028	COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{02D4B3F1-FD88-11D1-960D-00805FC79235}
msdtc.exe		2.420 K	6.872 K	2080	Microsoft Distributed Transaction Coordinator	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\System32\msdtc.exe
svchost.exe		544 K	2.644 K	2912	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\svchost.exe +k WerSvcGroup
lsass.exe		3.740 K	10.584 K	512	Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\lsass.exe
winlogon.exe		1.324 K	5.784 K	440	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 winlogon.exe
dwm.exe	< 0.01	26.560 K	49.084 K	704	Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-1	1	1 "dwm.exe"
explorer.exe	< 0.01	31.160 K	75.452 K	1792	Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	1	1 C:\Windows\Explorer EXE
vmtold.exe		12.540 K	21.768 K	2852	VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator	1	1 "C:\Program Files\VMware\VMware Tools\vmvmtold.exe" +n vmsvr
vm3dservice.exe		1.076 K	4.328 K	2884	VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator	1	1 "C:\Windows\System32\vm3dservice.exe" +u
process64.exe	1.50	18.672 K	38.444 K	3932	Syinternals Process Explorer	Syinternals - www.s...	MV-CLIENT\Administrator	1	1 "C:\Users\Administrator\Desktop\Syinternals Suite\process64.exe"

Processo de logon

Process Tree - C:\Users\Administrator\Desktop\Logfile-process-logon-example-user-console.PML

Only show processes still running at end of current trace

Timelines cover displayed events only

Process	Description	Image Path	Life Time	Company	Owner	Command	Start Time
Idle (0)	Idle	C:\Windows\system32\idle.exe	NT AUTHORITY\SYSTEM	Microsoft Corporation	NT AUTHORITY\SYSTEM	\SystemRoot\System32\sms.exe	25/06/2022 23:4...
System (4)	Windows Session Manager	C:\Windows\System32\sms.exe	System	Microsoft Corporation	NT AUTHORITY\SYSTEM	%SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Wind...	25/06/2022 23:4...
smss.exe (216)	Client Server Runtime Process	C:\Windows\system32\csrss.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	wininit.exe	%SystemRoot%\system32\wininit.exe	25/06/2022 23:4...
cars.exe (308)	Windows Start-Up Application	C:\Windows\system32\wininit.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe	C:\Windows\system32\svchost.exe -DoomLaunch	25/06/2022 23:4...
wininit.exe (400)	Services and Controller app	C:\Windows\system32\services.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm.exe	C:\Windows\system32\wbtm\unsecapp.exe -Embedding	25/06/2022 23:4...
services.exe (508)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\unsecapp.exe	C:\Windows\system32\wbtm\unsecapp.exe -Embedding	25/06/2022 23:4...
svchost.exe (572)	Sink to receive asynchronous callback...	C:\Windows\system32\wbtm\unsecapp.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\unsecapp.exe	C:\Windows\system32\wbtm\unsecapp.exe -Embedding	25/06/2022 23:4...
unsecapp.exe (1432)	WMI Provider Host	C:\Windows\system32\wbtm\unsecapp.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\unsecapp.exe	C:\Windows\system32\wbtm\unsecapp.exe -Embedding	25/06/2022 23:4...
wpvrse.exe (1316)	WMI Provider Host	C:\Windows\system32\wbtm\wpvrse.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\wpvrse.exe	C:\Windows\system32\wbtm\wpvrse.exe	25/06/2022 23:4...
wpvrse.exe (2416)	WMI Provider Host	C:\Windows\system32\wbtm\wpvrse.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\wpvrse.exe	C:\Windows\system32\wbtm\wpvrse.exe	25/06/2022 23:4...
DllHost.exe (1696)	COM Surrogate	C:\Windows\SysWOW64\dllhost.exe	Microsoft Corporation	MV\CLIENT\Administrator	C:\Windows\SysWOW64\dllHost.exe /ProcessId:{0662D85-6856-4460-8DE1-A81921B41C4B}	25/06/2022 23:5...	
wpvrse.exe (392)	WMI Provider Host	C:\Windows\system32\wbtm\wpvrse.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\wbtm\wpvrse.exe	C:\Windows\system32\wbtm\wpvrse.exe -Embedding	25/06/2022 23:5...
winlogon.exe (444)	Windows Logon Application	C:\Windows\system32\winlogon.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	winlogon.exe	LogonUI.exe -flags 0x0	25/06/2022 23:4...
LogonUI.exe (700)	Windows Logon User Interface Host	C:\Windows\system32\LogonUI.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	dwm.exe	dwm.exe	25/06/2022 23:4...
dwm.exe (756)	Desktop Window Manager	C:\Windows\system32\dwm.exe	Microsoft Corporation	Window Manager\DWIM-1	userinit.exe	C:\Windows\system32\userinit.exe	25/06/2022 23:4...
dwm.exe (1890)	Userinit Application	C:\Windows\system32\userinit.exe	Microsoft Corporation	MV\CLIENT\Administrator	Explorer EXE	C:\Windows\Explorer EXE	25/06/2022 23:5...
Explorer EXE (2936)	Windows Explorer	C:\Windows\Explorer.EXE	Microsoft Corporation	MV\CLIENT\Administrator	vmtoolsd.exe	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe -n vmsur	25/06/2022 23:5...
vmtoolsd.exe (2036)	VMware Tools Core Service	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	VMware, Inc.	MV\CLIENT\Administrator	vm3dservice.exe	C:\Windows\system32\vm3dservice.exe -u	25/06/2022 23:5...
vm3dservice.exe (1980)	VMware SVGA Helper Service	C:\Windows\System32\vm3dservice.exe	VMware, Inc.	MV\CLIENT\Administrator			25/06/2022 23:5...
svchost.exe (600)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\system32\svchost.exe -k RPCSS		25/06/2022 23:4...
vm3dservice.exe (728)	VMware SVGA Helper Service	C:\Windows\system32\vm3dservice.exe	VMware, Inc.	NT AUTHORITY\SYSTEM	C:\Windows\system32\vm3dservice.exe		25/06/2022 23:4...
svchost.exe (824)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe -k LocalService\NetworkRestricted		25/06/2022 23:4...
svchost.exe (848)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\system32\svchost.exe -k netsvcs		25/06/2022 23:4...
taskhost.exe (2688)	Host Process for Windows Tasks	C:\Windows\system32\taskhost.exe	Microsoft Corporation	MV\Vm	taskhost.exe	taskhost.exe	25/06/2022 23:4...
taskhost.exe (2968)	Host Process for Windows Tasks	C:\Windows\system32\taskhost.exe	Microsoft Corporation	MV\CLIENT\Administrator	taskhost.exe	C:\Windows\system32\ServerManagerLauncher.exe	25/06/2022 23:5...
ServerManagerLauncher.exe (2176)	Server Manager Launcher	C:\Windows\system32\ServerManagerLauncher.exe	Microsoft Corporation	MV\CLIENT\Administrator	taskhost.exe	"C:\Windows\system32\ServerManager.exe"	25/06/2022 23:5...
ServerManager.exe (2944)	Server Manager	C:\Windows\system32\ServerManager.exe	Microsoft Corporation	MV\CLIENT\Administrator	taskhost.exe	taskhost.exe USER	25/06/2022 23:5...
taskhost.exe (2340)	Host Process for Windows Tasks	C:\Windows\system32\taskhost.exe	Microsoft Corporation	MV\CLIENT\Administrator	taskhost.exe	C:\Windows\system32\svchost.exe -k LocalService	25/06/2022 23:4...
svchost.exe (892)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	taskhost.exe	C:\Windows\system32\svchost.exe -k NetworkService	25/06/2022 23:4...
svchost.exe (956)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	taskhost.exe	C:\Windows\system32\svchost.exe -k NetworkServiceNoNetwork	25/06/2022 23:4...
svchost.exe (312)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	taskhost.exe	C:\Windows\System32\spoolsv.exe	25/06/2022 23:4...
spoolsv.exe (1060)	Spooler SubSystem App	C:\Windows\System32\spoolsv.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	taskhost.exe	C:\Windows\System32\spoolsv.exe	25/06/2022 23:4...
syomon64.exe (1108)	System activity monitor	C:\Windows\syomon64.exe	Syinternals - www...	NT AUTHORITY\SYSTEM	taskhost.exe	C:\Windows\syomon64.exe	25/06/2022 23:4...
svchost.exe (1140)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	taskhost.exe	C:\Windows\System32\svchost.exe -k LocalSystem\NetworkRestricted	25/06/2022 23:4...
VGAuthService.exe (1164)	VMware Guest Authentication Service	C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe	VMware, Inc.	NT AUTHORITY\SYSTEM	taskhost.exe	"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"	25/06/2022 23:4...
vmtoolsd.exe (1224)	VMware Tools Core Service	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	VMware, Inc.	NT AUTHORITY\SYSTEM	taskhost.exe	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"	25/06/2022 23:4...
wlms.exe (1280)	Windows License Monitoring Service	C:\Windows\system32\wlms.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	taskhost.exe	C:\Windows\system32\wlms\wlms.exe	25/06/2022 23:4...
svchost.exe (1748)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	taskhost.exe	C:\Windows\System32\svchost.exe -k termsvc	25/06/2022 23:4...
rdclip.exe (328)	RDP Clipboard Monitor	C:\Windows\System32\rdclip.exe	Microsoft Corporation	MV\Vm	rdclip		25/06/2022 23:4...
svchost.exe (1800)	Host Process for Windows Services	C:\Windows\system32\svchost.exe	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	rdclip	C:\Windows\System32\svchost.exe -k NetworkService\NetworkRestricted	25/06/2022 23:4...
dhflhost.exe (1044)	COM Surrogate	C:\Windows\system32\dhflhost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	C:\Windows\System32\dhflhost.exe /ProcessId:{02D4B3F1-FD88-11D1-96D0-00805FC79235}	25/06/2022 23:4...
msdsc.exe (2088)	Microsoft Distributed Transaction Coordinator Coord.	C:\Windows\System32\msdsc.exe	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	rdclip	C:\Windows\System32\msdsc.exe	25/06/2022 23:4...
medic.exe (2088)	Microsoft Distributed Transaction Coordinator Service	C:\Windows\System32\medic.exe	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	rdclip	C:\Windows\System32\medic.exe	25/06/2022 23:4...
WmiApSrv.exe (2168)	WMI Performance Reverse Adapter	C:\Windows\system32\wbem\WmiApSrv.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	C:\Windows\system32\wbem\WmiApSrv.exe	25/06/2022 23:4...
svchost.exe (712)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	C:\Windows\System32\svchost.exe -k WebsvcGroup	25/06/2022 23:4...
lsass.exe (515)	Local Security Authority Process	C:\Windows\System32\lsass.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	C:\Windows\System32\lsass.exe	25/06/2022 23:4...
csrss.exe (408)	Client Server Runtime Process	C:\Windows\System32\csrss.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	%SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Wind...	25/06/2022 23:4...
csrss.exe (2052)	Client Server Runtime Process	C:\Windows\System32\csrss.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	%SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Wind...	25/06/2022 23:4...
winlogon.exe (764)	Windows Logon Application	C:\Windows\system32\winlogon.exe	Microsoft Corporation	NT AUTHORITY\SYSTEM	rdclip	C:\Windows\system32\winlogon.exe	25/06/2022 23:4...
dwm.exe (2560)	Desktop Window Manager	C:\Windows\system32\dwm.exe	Microsoft Corporation	Window Manager\DWIM-2	rdclip	dwm.exe	25/06/2022 23:4...
Explorer EXE (2924)	Windows Explorer	C:\Windows\Explorer.EXE	Microsoft Corporation	MV\Vm	rdclip	C:\Windows\Explorer EXE	25/06/2022 23:4...
vm3dservice.exe (2732)	VMware SVGA Helper Service	C:\Windows\System32\vm3dservice.exe	VMware, Inc.	MV\Vm	rdclip	"C:\Windows\System32\vm3dservice.exe" -u	25/06/2022 23:4...
Procmon64.exe (2280)	Process Monitor	C:\SysinternalsSuite\Procmon64.exe	Syinternals - www...	MV\Vm	rdclip	"C:\SysinternalsSuite\Procmon64.exe"	25/06/2022 23:4...

Processo de logon

Only show processes still running at end of current trace
 Timelines cover displayed events only

Process Tree						
Process	Description	Image Path	Life Time	Company	Owner	Command
idle (0)	Idle	idle	00:00:00.000 - 00:00:00.000	NT AUTHORITY\SYSTEM		
System (4)	System	C:\Windows\System32\system.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe
smss.exe (216)	Windows Session Manager	C:\Windows\System32\smss.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe 00000000 00000000
smss.exe (1072)	Windows Session Manager	C:\Windows\System32\smss.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	\SystemRoot\System32\smss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Wind...
Client Server Runtime Process (1980)	Client Server Runtime Process	C:\Windows\System32\csrss.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	
winlogon.exe (2596)	Windows Logon Application	C:\Windows\System32\winlogon.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	winlogon.exe
LogonUI.exe (2144)	Windows Logon User Interface Host	C:\Windows\System32\LogonUI.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	"LogonUI.exe" /flags:0x0
dwm.exe (2988)	Desktop Window Manager	C:\Windows\System32\dwm.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	Window Manager\DWIM-2	"dwm.exe"
userinit.exe (2536)	Userinit Logon Application	C:\Windows\System32\userinit.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	MV\bob	C:\Windows\System32\userinit.exe
Explorer.EXE (1008)	Windows Explorer	C:\Windows\Explorer.EXE	00:00:00.000 - 00:00:00.000	Microsoft Corporation	MV\bob	C:\Windows\Explorer.EXE
vmtoolsd.exe (1032)	VMware Tools Core Service	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	MV\bob	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
vm3dservice.exe (2516)	VMware VGA Helper Service	C:\Windows\System32\vm3dservice.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	MV\bob	"C:\Windows\System32\vm3dservice.exe" -u
carss.exe (308)	Client Server Runtime Process	C:\Windows\System32\carss.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	%SystemRoot%\System32\carss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Wind...
carss.exe (404)	Client Server Runtime Process	C:\Windows\System32\carss.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	%SystemRoot%\System32\carss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Wind...
wininit.exe (412)	Windows Start-Up Application	C:\Windows\System32\wininit.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	wininit.exe
services.exe (504)	Services and Controller app	C:\Windows\System32\services.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\services.exe
svchost.exe (568)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe < DcomLaunch
unseccapp.exe (1540)	Sink to receive asynchronous callback...	C:\Windows\System32\wbeim\unseccapp.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\wbeim\unseccapp.exe -Embedding
wmprvse.exe (1776)	WMI Provider Host	C:\Windows\System32\wmprvse.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\wmprvse.exe
wmprvse.exe (2344)	WMI Provider Host	C:\Windows\System32\wmprvse.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\wmprvse.exe
TSTheme.exe (2540)	TSTheme Server Module	C:\Windows\System32\TSTheme.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\TSTheme.exe -Embedding
DllHost.exe (2280)	COM Surrogate	C:\Windows\System32\DllHost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\DllHost.exe /ProcessId:{AB8902B4-09CA-4BB6-B7D0-A8F59079ABD5}
DllHost.exe (2196)	COM Surrogate	C:\Windows\System32\WOW64\DllHost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\WOW64\DllHost.exe /ProcessId:{06622085-6B56-4460-8DE1-A81921841C4B}
svchost.exe (596)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe & RPCSS
vm3dservice.exe (716)	VMware VGA Helper Service	C:\Windows\System32\vm3dservice.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	NT AUTHORITY\SYSTEM	C:\Windows\System32\vm3dservice.exe
svchost.exe (764)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	C:\Windows\System32\svchost.exe < LocalServiceNetworkRestricted
svchost.exe (808)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe < netvcs
taskhost.exe (1228)	Host Process for Windows Tasks	C:\Windows\System32\taskhost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	MC-CLIENT\Administrator	taskhost.exe
taskhost.exe (1560)	Host Process for Windows Tasks	C:\Windows\System32\taskhost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	taskhost.exe USER
taskhost.exe (1840)	Host Process for Windows Tasks	C:\Windows\System32\taskhost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe < LocalService
svchost.exe (852)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe < NetworkService
svchost.exe (920)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe < LocalServiceNoNetwork
svchost.exe (280)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
spoolsv.exe (236)	Spooler SubSystem App	C:\Windows\System32\spoolsv.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\spoolsv.exe
System64.exe (1088)	System activity monitor	C:\Windows\System64.exe	00:00:00.000 - 00:00:00.000	Sysinternals - www	NT AUTHORITY\SYSTEM	C:\Windows\System64.exe
svchost.exe (1156)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe < LocalSystemNetworkRestricted
VGAuthService.exe (1188)	VMware Guest Authentication Service	C:\Program Files\VMware\VMware Tools\VGAuthService.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	NT AUTHORITY\SYSTEM	"C:\Program Files\VMware\VMware Tools\VGAuthService.exe"
vmtoolsd.exe (1240)	VMware Tools Core Service	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	NT AUTHORITY\SYSTEM	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
wlms.exe (1284)	Windows License Monitoring Service	C:\Windows\System32\wlms.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\wlms.exe
Client Server Runtime Process (1860)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe < termsvc
rdclip.exe (2252)	RDP Clipboard Monitor	C:\Windows\System32\rdclip.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	MV\bob	rdclip
svchost.exe (1888)	Host Process for Windows Services	C:\Windows\System32\svchost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	C:\Windows\System32\svchost.exe < NetworkServiceNetworkRestricted
dllhost.exe (2028)	COM Surrogate	C:\Windows\System32\ dllhost.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\ dllhost.exe /ProcessId:{02D43F1-FD88-11D1-96D0-00805FC79235}
mdtc.exe (2080)	Microsoft Distributed Transaction Coordination	C:\Windows\System32\mdtc.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\mdtc.exe
lsass.exe (512)	Local Security Authority Process	C:\Windows\System32\lsass.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	C:\Windows\System32\lsass.exe
winlogon.exe (440)	Windows Logon Application	C:\Windows\System32\winlogon.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	NT AUTHORITY\SYSTEM	winlogon.exe
dwm.exe (704)	Desktop Window Manager	C:\Windows\System32\dwm.exe	00:00:00.000 - 00:00:00.000	Microsoft Corporation	Window Manager\DWIM-1	"dwm.exe"
Explorer.EXE (1792)	Windows Explorer	C:\Windows\Explorer.EXE	00:00:00.000 - 00:00:00.000	Microsoft Corporation	MV-CLIENT\Administrator	C:\Windows\Explorer.EXE
vmtoolsd.exe (2852)	VMware Tools Core Service	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	MV-CLIENT\Administrator	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr
vm3dservice.exe (2864)	VMware VGA Helper Service	C:\Windows\System32\vm3dservice.exe	00:00:00.000 - 00:00:00.000	VMware, Inc.	MV-CLIENT\Administrator	"C:\Windows\System32\vm3dservice.exe" -u
Procmon64.exe (1416)	Process Monitor	C:\Users\Administrator\Desktop\SysinternalsSuite\Procmon64.exe	00:00:00.000 - 00:00:00.000	Sysinternals - www	MV-CLIENT\Administrator	"C:\Users\Administrator\Desktop\SysinternalsSuite\Procmon64.exe"

Processo de logon

Registry Editor

File Edit View Favorites Help

Name Type Data
ab|(Default) REG_SZ (value not set)
ab|AutoAdminLogon REG_SZ 0
ab|AutoLogonSID REG_SZ S-1-5-32
ab|AutoRestartShell REG_DWORD 0x00000001 (1)
ab|Background REG_SZ 0 0
ab|CachedLogonsCount REG_SZ 10
ab|DebugServerCommand REG_SZ no
ab|DisableCAD REG_DWORD 0x00000001 (1)
ab|ForceUnlockLogon REG_DWORD 0x00000000 (0)
ab|LastUsedUsername REG_SZ
ab|LegalNoticeCaption REG_SZ
ab|LegalNoticeText REG_SZ
ab|PasswordExpiryWarning REG_DWORD 0x00000005 (5)
ab|PowerdownAfterShutdown REG_SZ 0
ab|PreCreateKnownFolders REG_SZ (A520A1A4-1780-4FF6-BD18-167343C5AF16)
ab|PreloadFontFile REG_SZ SC_LockAll
ab|ReportBootOk REG_SZ 1
ab|scrmveoption REG_SZ 0

Shell REG_SZ explorer.exe

ShutdownFlags REG_DWORD 0x00000007 (7)

ShutdownWithoutLogon REG_SZ 0

Userinit REG_SZ C:\Windows\system32\userinit.exe

VMApplet REG_SZ SystemPropertiesPerformance.exe /pagefile

WinStationsDisabled REG_SZ 0

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon

Registry Editor

File Edit View Favorites Help

Name Type Data
ab|(Default) REG_SZ (value not set)
ab|DefaultShell REG_SZ explorer.exe

ProfileList
ProfileLoader
ProfileNotification
related.desc
RemoteRegistry
Schedule
SCW
SecEdit
Sensor
Server
setup
SoftwareProtectionPlatform
Superfetch
Svchost
Terminal Server
Time Zones
Tracing
Userinstallable.drivers
WbemPerf
Windows
WindowsServerBackup
Winlogon
AlternateShells
AvailableShells
AutoLogonChecked
GPExtensions
WSService
WUDF
Windows Script Host
Windows Search

Shell REG_SZ explorer.exe

ShutdownFlags REG_DWORD 0x00000007 (7)

ShutdownWithoutLogon REG_SZ 0

Userinit REG_SZ C:\Windows\system32\userinit.exe

VMApplet REG_SZ SystemPropertiesPerformance.exe /pagefile

WinStationsDisabled REG_SZ 0

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells

Registry Editor

File Edit View Favorites Help

Name Type Data
ab|(Default) REG_SZ (value not set)
ab|30000 REG_SZ cmd.exe /c "cd /d \"%USERPROFILE%\" & start cmd.exe /k runonce.exe /AlternateShellStartup"
ab|60000 REG_SZ explorer.exe

ProfileList
ProfileLoader
ProfileNotification
related.desc
RemoteRegistry
Schedule
SCW
SecEdit
Sensor
Server
setup
SoftwareProtectionPlatform
Superfetch
Svchost
Terminal Server
Time Zones
Tracing
Userinstallable.drivers
WbemPerf
Windows
WindowsServerBackup
Winlogon
AlternateShells
AvailableShells
AutoLogonChecked
GPExtensions
WSService
WUDF
Windows Script Host
Windows Search

Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows NT\CurrentVersion\Winlogon\AlternateShells\AvailableShells

Cenários



Cenário 1 – Logon comum – Console/interativo

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: SYSTEM
Account Name: MV-CLIENTS
Account Domain: MV
Logon ID: 0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:
Security ID: Window Manager\DWIM-2
Account Name: DWM-2
Account Domain: Window Manager
Logon ID: 0x32AA5A
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0xbfb8
Process Name: C:\Windows\System32\winlogon.exe

Network Information:
Workstation Name: -
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: Advapi
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is

Log Name: Security
Source: Microsoft Windows security
Logged: 15/06/2022 02:28:12
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: SYSTEM
Account Name: MV-CLIENTS
Account Domain: MV
Logon ID: 0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:
Security ID: Window Manager\DWIM-2
Account Name: DWM-2
Account Domain: Window Manager
Logon ID: 0x32AA5A
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0xbfb8
Process Name: C:\Windows\System32\winlogon.exe

Network Information:
Workstation Name: -
Source Network Address: -
Source Port: -

Detailed Authentication Information:
Logon Process: Advapi
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is

Log Name: Security
Source: Microsoft Windows security
Logged: 15/06/2022 02:28:12
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: SYSTEM
Account Name: MV-CLIENTS
Account Domain: MV
Logon ID: 0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:
Security ID: MV-CLIENT\Administrator
Account Name: Administrator
Account Domain: MV-CLIENT
Logon ID: 0x32C1B2
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0xbfb8
Process Name: C:\Windows\System32\winlogon.exe

Network Information:
Workstation Name: MV-CLIENT
Source Network Address: 127.0.0.1
Source Port: 0

Detailed Authentication Information:
Logon Process: User32
Authentication Package: Negotiate
Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is

Log Name: Security
Source: Microsoft Windows security
Logged: 15/06/2022 02:29:05
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Cenário 1 – Logon comum – Console/interativo

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)

File Options View Process Find Users Help

Process	PID	Description	Company Name	User Name	Session	Command Line
System Idle Process	0		NT AUTHORITY\SYSTEM			
System	4		NT AUTHORITY\SYSTEM		0	
Interrups		n/a Hardware Interrupts and DPCs			0	
smss.exe		216 Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	\SystemRoot\System32\smss.exe
cssrs.exe		309 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	%SystemRoot%\system32\cssrs.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubS
wininit.exe		400 Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	wininit.exe
services.exe		488 Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\services.exe
svchost.exe		572 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k DcomLaunch
		1432 Sink to receive asynchronou...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\wben\unseccapp.exe -Embedding
		1800 WMI Provider Host	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\wben\wmpnprov.exe
		2516 WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\wben\wmiprovce.exe
		1172 COM Surrogate	Microsoft Corporation	MV-CLIENT\Administrator	1	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{3EB3C871-F16-487C-9050-104BCD66683}
		600 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k RPCSS
		800 VMware SVGA Helper Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\vm3dservice.exe
		832 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
		852 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\svchost.exe -k netsvcs
		2224 Host Process for Windows T...	Microsoft Corporation	MV-CLIENT\Administrator	1	taskhost.exe
		896 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k LocalService
		964 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k NetworkService
		300 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
		1060 Spooler Sub-System App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\System32\spoolsv.exe
		1112 System activity monitor	Sysinternals - www.s...	NT AUTHORITY\SYSTEM	0	C:\Windows\System32\systrace.exe
		1164 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
		1200 VMware Guest Authenticatio...	VMware, Inc.	NT AUTHORITY\SYSTEM	0	"C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuth Service.exe"
		1236 VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
		1296 Windows License Monitoring...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\system32\wlmns.exe
		1768 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\System32\svchost.exe -k termsvc
		1836 Host Process for Windows S...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
		1924 COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{02D4B3F1-FD88-11D1-960D-000805FC7925}
		2164 Microsoft Distributed Trans...	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	C:\Windows\System32\msdsc.exe
		500 Local Security Authority Proc...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	C:\Windows\System32\lsass.exe
		2840 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	%SystemRoot%\system32\cssrs.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows=On SubS
		2900 Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	winlogon.exe
		1644 Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-1	1	dwm.exe
		1640 Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	1	C:\Windows\Explorer.EXE
		2316 VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator	1	"C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmsur
		2996 VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator	1	C:\Windows\System32\vm3dservice.exe"-u
		2404 Sysinternals Process Explorer	Sysinternals - www.s...	MV-CLIENT\Administrator	1	C:\Users\Administrator\Desktop\SysinternalsSuite\nmcsn64.exe"

CPU Usage: 6.15% Commit Charge: 48.78% Processes: 37 Physical Usage: 53.19%

01:31 15/06/2022

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName:
UtcTime: 2022-06-15 04:31:57.418
ProcessGuid: {8849a51a-60bd-62a9-878f-270000000000}
ProcessId: 776
Image: C:\Users\Administrator\Desktop\SysinternalsSuite\procexp64.exe
FileVersion: 16.43
Description: Sysinternals Process Explorer
Product: Process Explorer
Company: Sysinternals - www.sysinternals.com
OriginalFileName: procexp.exe

CommandLine: "C:\Users\Administrator\Desktop\SysinternalsSuite\procexp64.exe"
CurrentDirectory: C:\Users\Administrator\Desktop\SysinternalsSuite
User: MV-CLIENT\Administrator

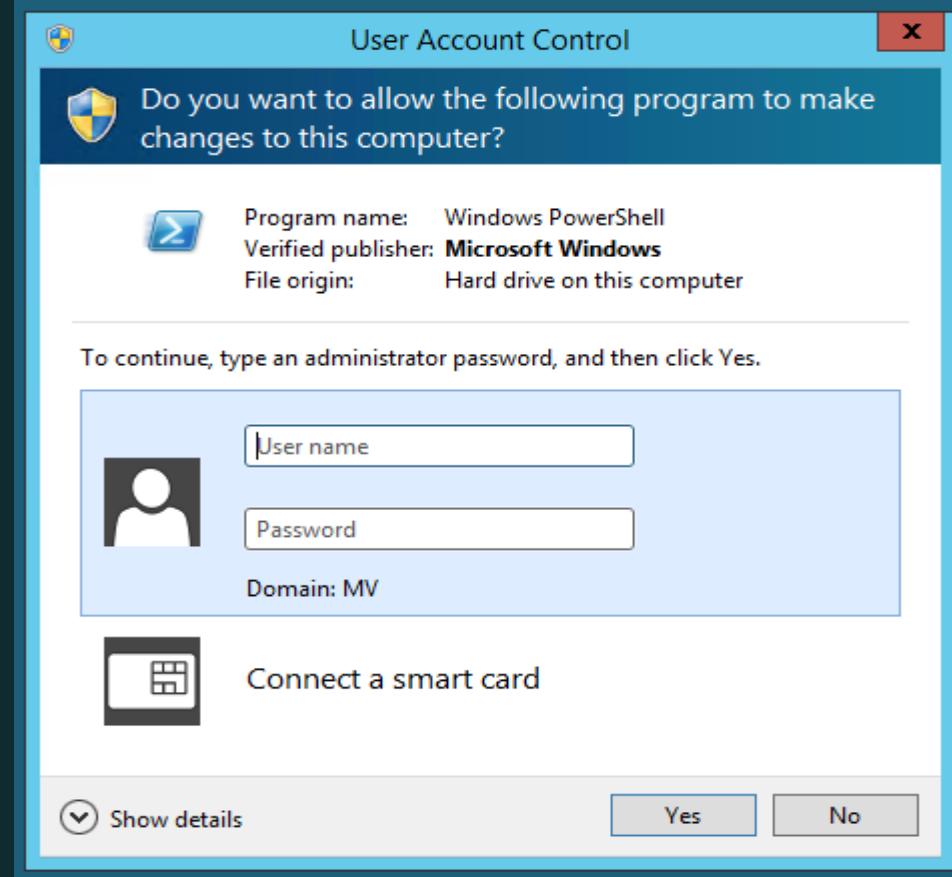
LogonGuid: {8849a51a-5db0-62a9-b091-0f0000000000}
LogonId: 0x7085
TerminalSessionId: 1
IntegrityLevel: High
Hashes: SHA256-77359157EBF4572C2D7F17A1A264990843307F802D20BAD4FB2442245D65F0B
ParentProcessGuid: {8849a51a-5db0-62a9-b091-0f0000000000}
ParentProcessId: 1640
ParentImage: C:\Windows\explorer.exe
ParentCommandLine: C:\Windows\Explorer.EXE
ParentUser: MV-CLIENT\Administrator

Log Name: Microsoft-Windows-Sysmon/Operational
Source: Sysmon
Event ID: 1
Level: Information
User: SYSTEM
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Cenário 2 – Consent.exe

Start



Cenário 2 – Consent.exe

Event Properties - Event 4624, Microsoft Windows security auditing.

General **Details**

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENT\$
Account Domain:	MV
Logon ID:	0x3E7

Logon Type: 11

Impersonation Level: Impersonation

New Logon:

Security ID:	MV\mv
Account Name:	mv
Account Domain:	MV
Logon ID:	0x6681FA
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x68
Process Name:	C:\Windows\System32\consent.exe

Network Information:

Workstation Name:	MV-CLIENT
Source Network Address:	-1
Source Port:	0

Detailed Authentication Information:

Logon Process:	CredPro
Authentication Package:	Negotiate

Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

Log Name: Security
Source: Microsoft Windows security **Logged:** 15/06/2022 16:05:43
Event ID: 4624 **Task Category:** Logon
Level: Information **Keywords:** Audit Success
User: N/A **Computer:** MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing.

General **Details**

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENT\$
Account Domain:	MV
Logon ID:	0x3E7

Logon Type: 11

Impersonation Level: Impersonation

New Logon:

Security ID:	MV\mv
Account Name:	mv
Account Domain:	MV
Logon ID:	0x6681F9
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x68
Process Name:	C:\Windows\System32\consent.exe

Network Information:

Workstation Name:	MV-CLIENT
Source Network Address:	-1
Source Port:	0

Detailed Authentication Information:

Logon Process:	CredPro
Authentication Package:	Negotiate

Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

Log Name: Security
Source: Microsoft Windows security **Logged:** 15/06/2022 16:05:43
Event ID: 4624 **Task Category:** Logon
Level: Information **Keywords:** Audit Success
User: N/A **Computer:** MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing.

General **Details**

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENT\$
Account Domain:	MV
Logon ID:	0x3E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:

Security ID:	MV-CLIENT\Administrator
Account Name:	Administrator
Account Domain:	MV-CLIENT
Logon ID:	0x13B276
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x8c
Process Name:	C:\Windows\System32\consent.exe

Network Information:

Workstation Name:	MV-CLIENT
Source Network Address:	-1
Source Port:	0

Detailed Authentication Information:

Logon Process:	CredPro
Authentication Package:	Negotiate

Transited Services: -
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security **Logged:** 19/06/2022 02:47:30
Event ID: 4624 **Task Category:** Logon
Level: Information **Keywords:** Audit Success
User: N/A **Computer:** MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Cenário 2 – Consent.exe

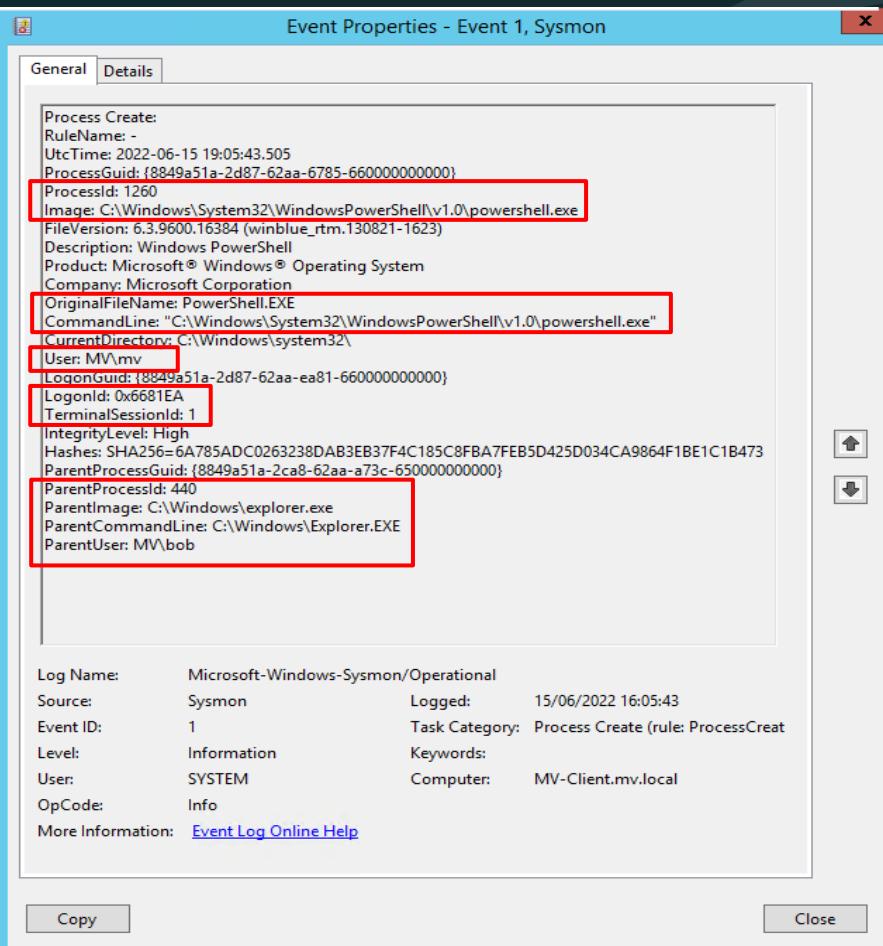
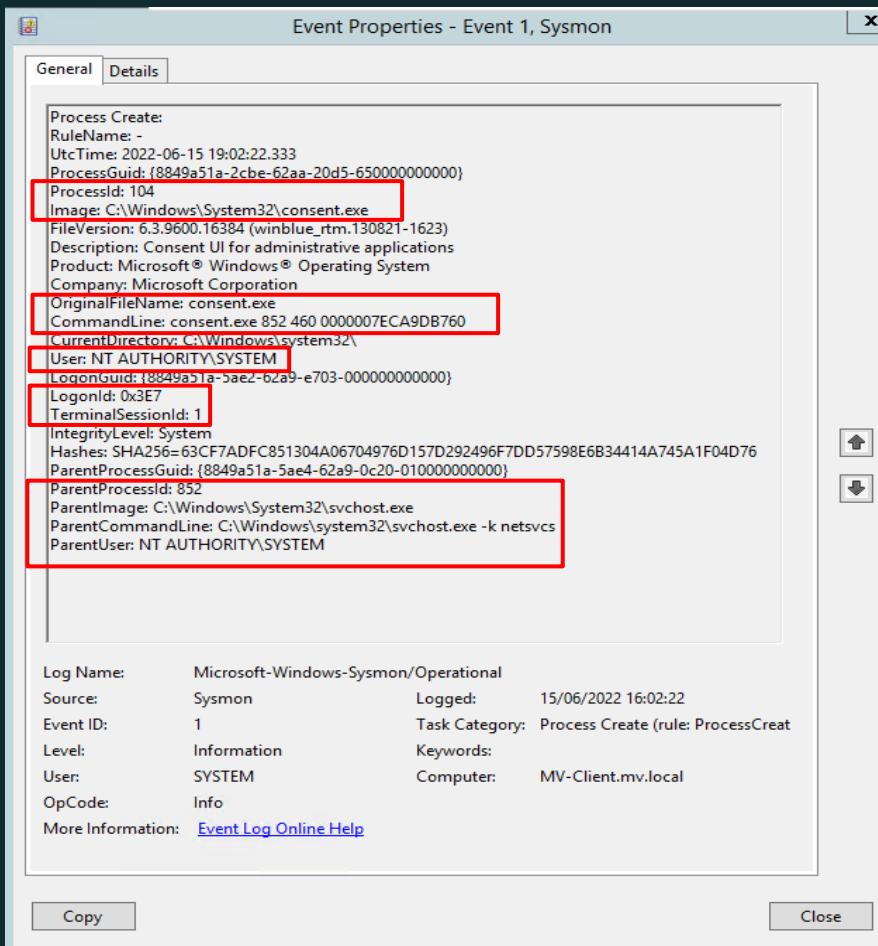
Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)											
File	Options	View	Process	Find	Users	Help	<Filter by name>				
Process	CPU	Private	Working	PID	Description	Company Name	User Name	Session	Command Line		
System Idle Process	98.36	0 K	4 K	0		NT AUTHORITY\SYSTEM	NT AUTHORITY\SYSTEM	0			
System	< 0.01	100 K	276 K	4	n/a Hardware Interrupts and DPCs		NT AUTHORITY\SYSTEM	0			
smss.exe		292 K	568 K	216	Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 \SystemRoot\System32\smss.exe		
csrss.exe	1.640 K	3.680 K	308	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Windows=On SubSystemType=Windows ServerDl=basebsrv.1 ServerDl=winsrv:User			
wininit.exe	804 K	3.612 K	408	Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 wininit.exe			
services.exe	2.400 K	4.392 K	488	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\services.exe			
svchost.exe	< 0.01	4 160 K	8 528 K	572	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe -k DcomLaunch		
uncapp.exe		940 K	4 160 K	1432	Sink to receive asynchronous callbacks f...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wbem\uncapp.exe -Embedding		
WmiPrvSE.exe	8.004 K	12.808 K	1800	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\wbem\wmiaprse.exe			
svchost.exe	3.136 K	5.416 K	600	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k RPCSS			
vm3dservice.exe	952 K	2.260 K	800	VMMware SVGA Helper Service	Vmware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\vm3dservice.exe			
svchost.exe	20.588 K	23.508 K	832	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted			
taskhost.exe	18.992 K	34.528 K	852	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe -k netsvcs			
taskhost.exe	1.812 K	6.528 K	2108	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	3	taskhost.exe			
taskhost.exe	1.624 K	6.036 K	1904	Host Process for Windows Tasks	Microsoft Corporation	MV\bob	1	taskhost.exe			
client.exe	5.932 K	25.904 K	104	Connected UI for administrative applications	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 client.exe 8924800000007E5A0D760			
svchost.exe	5.888 K	12.024 K	896	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalService			
svchost.exe	7.520 K	16.772 K	964	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k Network Service			
svchost.exe	6.224 K	10.292 K	300	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork			
spoolsv.exe	4.680 K	11.068 K	106	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\spoolsv.exe			
Symon64.exe	4.176 K	10.024 K	1112	System activity monitor	Sysinternals - www.s...	NT AUTHORITY\SYSTEM	0	0 C:\Windows\Syomon64.exe			
svchost.exe	7.996 K	12.468 K	1164	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted			
VGAuthService.exe	2.716 K	8.264 K	1200	VMware Guest Authentication Service	Vmware, Inc.	NT AUTHORITY\SYSTEM	0	0 "C:\Program Files\VMware\VMware Tools\VMware VGauth\VGAuthService.exe"			
vmtools.exe	8.276 K	17.968 K	1236	VMware Tools Core Service	Vmware, Inc.	NT AUTHORITY\SYSTEM	0	0 "C:\Program Files\VMware\VMware Tools\vmtools.exe"			
wlms.exe		484 K	2.612 K	1296	Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wlms.exe		
svchost.exe	< 0.01	56.536 K	53.460 K	1768	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\System32\svchost.exe -k termsvc		
rdpclip.exe	1.808 K	7.000 K	1652	RDP Clipboard Monitor	Microsoft Corporation	MV\bob	1	1 rdpclip			
svchost.exe	1.044 K	2.456 K	1834	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted			
dllhost.exe	3.104 K	5.668 K	1924	COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{02D4B3F1-FD88-11D1-96D0-00805FC79235}			
msdtc.exe	2.256 K	3.484 K	2164	Microsoft Distributed Transaction Coordinator	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\System32\msdtc.exe			
lsass.exe	4.952 K	10.800 K	500	Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\lsass.exe			
cssrs.exe	< 0.01	1.888 K	28.448 K	972	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	3	3 %SystemRoot%\system32\cssrs.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Windows=On SubSystemType=Windows ServerDl=basebsrv.1 ServerDl=winsrv:User		
winlogon.exe	1.104 K	4.892 K	2540	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	3	3 winlogon.exe			
dwm.exe	1.56 K	29.680 K	58.228 K	688	Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-3	3	3 dwm.exe"		
explorer.exe	< 0.01	35.344 K	87.544 K	156	Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	3	3 C:\Windows\Explorer EXE		
vmtoolsd.exe	< 0.01	7.528 K	16.684 K	2284	VMware Tools Core Service	Vmware, Inc.	MV-CLIENT\Administrator	3	3 "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmsvr		
vm3dservice.exe	1.040 K	4.244 K	2328	VMMware SVGA Helper Service	Vmware, Inc.	MV-CLIENT\Administrator	3	3 "C:\Windows\System32\vm3dservice.exe" -u			
procexp64.exe	< 0.01	18.008 K	36.172 K	2668	Sysinternals Process Explorer	Sysinternals - www.s...	MV-CLIENT\Administrator	3	3 "C:\Users\Administrator\Desktop\Sysinternals Suite\procexp64.exe"		
cssrs.exe	< 0.01	1.560 K	19.208 K	1448	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 %SystemRoot%\system32\cssrs.exe ObjectDirectory=Windows SharedSection=1024.20480.768 Windows=On SubSystemType=Windows ServerDl=basebsrv.1 ServerDl=winsrv:User		
winlogon.exe	1.264 K	5.072 K	792	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 winlogon.exe			
dwm.exe	< 0.01	8.376 K	43.156 K	2776	Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-1	1	1 dwm.exe"		
explorer.exe	< 0.01	27.636 K	67.048 K	440	Windows Explorer	Microsoft Corporation	MV\bob	1	1 C:\Windows\Explorer EXE		
vm3dservice.exe	1.044 K	4.288 K	2628	VMMware SVGA Helper Service	Vmware, Inc.	MV\bob	1	1 "C:\Windows\System32\vm3dservice.exe" -u			

Cenário 2 – Consent.exe

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)

Process	CPU	Private	Working	PID	Description	Company Name	User Name	Session	Command Line
System Idle Process	100.00	0 K	4 K	0		NT AUTHORITY\SYSTEM			
System	< 0.01	100 K	276 K	4		NT AUTHORITY\SYSTEM			
Intempts		0 K	0 K		n/a Hardware Interrupts and DPCs				
smss.exe		292 K	568 K	216	Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 \SystemRoot\System32\smss.exe
csrss.exe		1.640 K	3.684 K	308	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 \SystemRoot\System32\csrss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDl=basev1,1 ServerDl=winsv:Us
wininit.exe		728 K	3.596 K	400	Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 wininit.exe
services.exe		2.452 K	4.412 K	488	Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\services.exe
svchost.exe	< 0.01	4.212 K	8.548 K	572	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe -k DoomLaunch
unseccapp.exe		940 K	4.160 K	1432	Sink to receive asynchronous callbacks f...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wbem\unseccapp.exe -Embedding
WmiPrvSE.exe		8.228 K	12.936 K	1800	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\wbem\wmprvse.exe
svchost.exe		3.188 K	5.432 K	600	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k RPCSS
vm3dservice.exe		952 K	2.260 K	800	VMware SVGA Helper Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\vm3dservice.exe
svchost.exe		20.500 K	23.476 K	832	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
svchost.exe		18.500 K	34.416 K	852	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\svchost.exe -k netsvcs
taskhost.exe		1.812 K	6.528 K	2104	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	3	3 taskhost.exe
taskhost.exe		1.624 K	6.036 K	1904	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT	3	1 taskhost.exe
svchost.exe		5.868 K	12.024 K	896	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalService
svchost.exe		7.520 K	16.772 K	964	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k NetworkService
svchost.exe		6.260 K	10.356 K	300	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork
spoolsv.exe		4.628 K	11.052 K	1060	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\spoolsv.exe
sytem64.exe		4.176 K	10.024 K	1112	System activity monitor	Sytematials - www.s...	NT AUTHORITY\SYSTEM	0	0 C:\Windows\Symem64.exe
svchost.exe		7.940 K	12.452 K	1164	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted
VGAuthService.exe		2.716 K	8.264 K	1200	VMware Guest Authentication Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuthService.exe"
vmtoolsd.exe		8.276 K	17.968 K	1236	VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0 C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"
wlm5.exe		484 K	2.612 K	1296	Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\wlm5.exe
svchost.exe		56.536 K	54.716 K	1768	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\System32\svchost.exe -k tempsvc
rdclip.exe		1.808 K	7.000 K	1652	RDP Clipboard Monitor	Microsoft Corporation	MV-CLIENT	1	1 rdclip
svchost.exe		1.044 K	2.456 K	1836	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted
dilihst.exe		3.104 K	5.868 K	1924	COM Sumologic	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\SYSTEM32\DLLHOST.EXE /PROCESSID:(02DAB3F1-FD88-11D1-96D0-00805FC79235)
msdc.exe		2.256 K	3.484 K	2164	Microsoft Distributed Transaction Coordinator	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0 C:\Windows\System32\msdc.exe
svchost.exe		552 K	2.620 K	2568	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\System32\svchost.exe < WerSvcGroup
lsass.exe		4.968 K	10.840 K	500	Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0 C:\Windows\system32\lsass.exe
carss.exe	< 0.01	1.888 K	28.424 K	972	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	3	3 %SystemRoot%\System32\carss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDl=basev1,1 ServerDl=winsv:Us
winlogon.exe		1.104 K	4.892 K	2540	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	3	3 winlogon.exe
dwm.exe	< 0.01	29.680 K	58.204 K	688	Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-3	3	3 "dwm.exe"
explorer.exe		35.344 K	87.548 K	156	Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	3	3 C:\Windows\Explorer EXE
vmtoolsd.exe	< 0.01	11.468 K	21.088 K	2284	VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator	3	3 "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmsvr
vm3dservice.exe		1.040 K	4.244 K	2328	VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator	3	3 C:\Windows\System32\vm3dservice.exe" -u
procexp64.exe	< 0.01	18.008 K	36.156 K	2660	Sytematials Process Explorer	Sytematials - www.s...	MV-CLIENT\Administrator	3	3 "C:\Users\Administrator\Desktop\Sytematials Suite\procexp64.exe"
crss.exe		1.552 K	13.772 K	1448	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 %SystemRoot%\System32\crss.exe ObjectDirectory=\Windows SharedSection=1024,20480,768 Windows=On SubSystemType=Windows ServerDl=basev1,1 ServerDl=winsv:Us
winlogon.exe		1.356 K	12.000 K	792	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 winlogon.exe
dwm.exe	< 0.01	8.260 K	37.412 K	2776	Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-1	1	1 "dwm.exe"
explorer.exe	< 0.01	27.200 K	66.560 K	4400	Windows Explorer	Microsoft Corporation	MV-CLIENT	1	1 C:\Windows\Explorer EXE
vm3dservice.exe		1.044 K	4.288 K	2828	VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT	1	1 "C:\Windows\System32\vm3dservice.exe" -u
powershell.exe		64.680 K	64.048 K	1260	Windows PowerShell	Microsoft Corporation	MV\mv	1	1 "C:\Windows\System32\WindowsPowerShell\v1.0\powershell.exe"
conhost.exe	< 0.01	1.768 K	7.324 K	2288	Console Window Host	Microsoft Corporation	MV\mv	1	1 \??C:\Windows\system32\conhost.exe 0x4

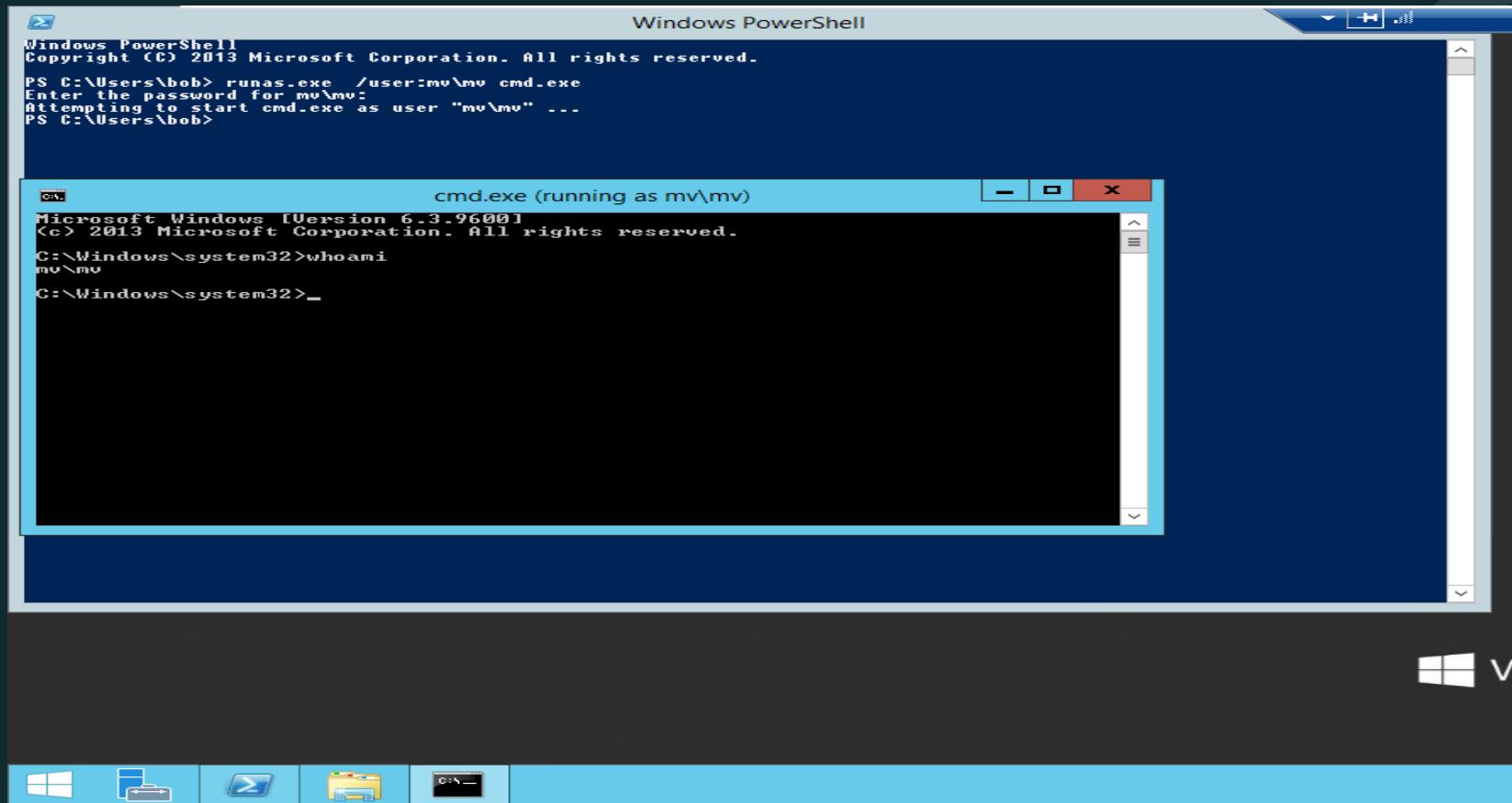
Cenário 2 – Consent.exe



Cenário 3 - Runas

Windows PowerShell
Copyright (C) 2013 Microsoft Corporation. All rights reserved.
PS C:\Users\bob> runas.exe /user:mv\mv cmd.exe
Enter the password for mv\mv:
Attempting to start cmd.exe as user "mv\mv" ...
PS C:\Users\bob>

cmd.exe (running as mv\mv)
Microsoft Windows [Version 6.3.9600]
<C> 2013 Microsoft Corporation. All rights reserved.
C:\Windows\system32>whoami
mv\mv
C:\Windows\system32>_



Cenário 3 - Runas

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: MV\bob
Account Name: bob
Account Domain: MV
Logon ID: 0x84124

Logon Type: 2

Impersonation Level: Impersonation

New Logon:
Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0xd084d
Logon GUID: {058fa89e-e5bc-c805-018c-ce7f23899477}

Process Information:
Process ID: 0x324
Process Name: C:\Windows\System32\svchost.exe

Network Information:
Workstation Name: MV-CLIENT
Source Network Address: -1
Source Port: 0

Detailed Authentication Information:
Logon Process: seologo
Authentication Package: Negotiate

Transited Services:
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

Log Name: Security
Source: Microsoft Windows security Logged: 19/06/2022 00:06:04
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:
Security ID: MV\bob
Account Name: bob
Account Domain: MV
Logon ID: 0x84124

Logon Type: 2

Impersonation Level: Impersonation

New Logon:
Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0xd084d
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x324
Process Name: C:\Windows\System32\svchost.exe

Network Information:
Workstation Name: MV-CLIENT
Source Network Address: -1
Source Port: 0

Detailed Authentication Information:
Logon Process: seologo
Authentication Package: Negotiate

Transited Services:
Package Name (NTLM only): -
Key Length: 0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

Log Name: Security
Source: Microsoft Windows security Logged: 19/06/2022 00:06:04
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4648, Microsoft Windows security auditing.

General Details

A logon was attempted using explicit credentials.

Subject:
Security ID: MV\bob
Account Name: bob
Account Domain: MV
Logon ID: 0x84124
Logon GUID: {366670c1-b6fc-9244-0824-e9824fb6b3e6}

Account Whose Credentials Were Used:
Account Name: mv
Account Domain: MV
Logon GUID: {058fa89e-e5bc-c603-618c-ce7f23899477}

Target Server:
Target Server Name: localhost
Additional Information: localhost

Process Information:
Process ID: 0x324
Process Name: C:\Windows\System32\svchost.exe

Network Information:
Network Address: ::1
Port: 0

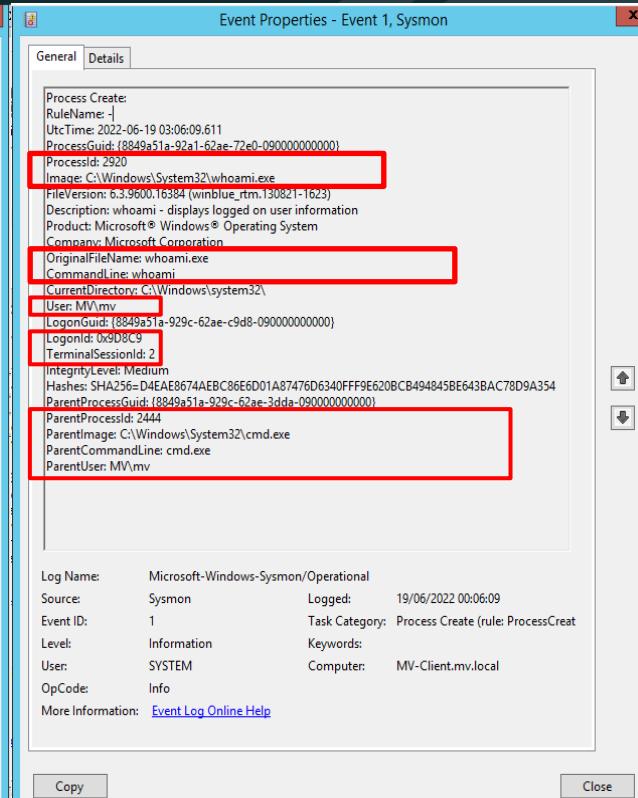
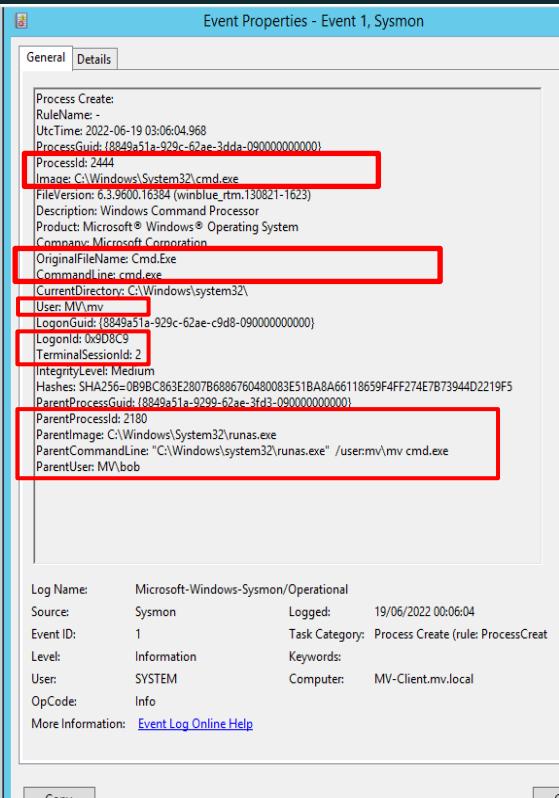
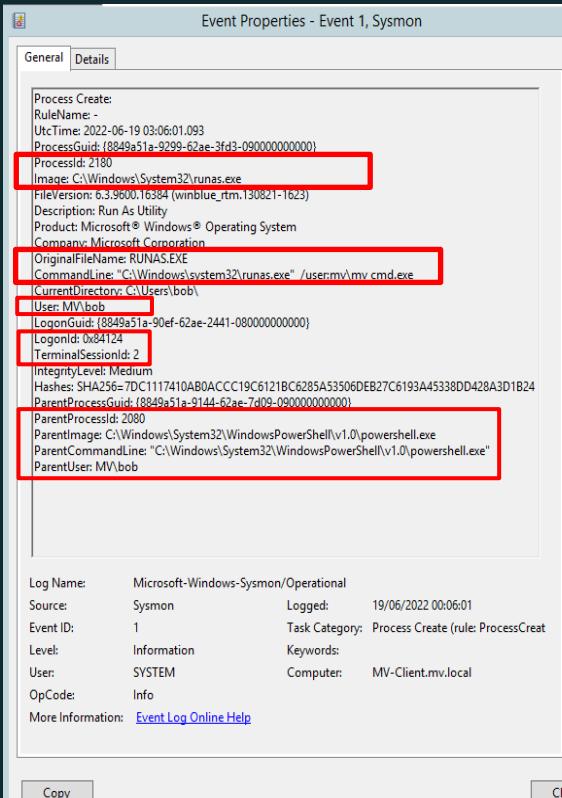
This event is generated when a process attempts to log on an account by explicitly specifying that account's credentials. This most commonly occurs in batch-type configurations such as scheduled tasks, or when using the RUNAS command.

Log Name: Security
Source: Microsoft Windows security Logged: 19/06/2022 00:06:04
Event ID: 4648 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

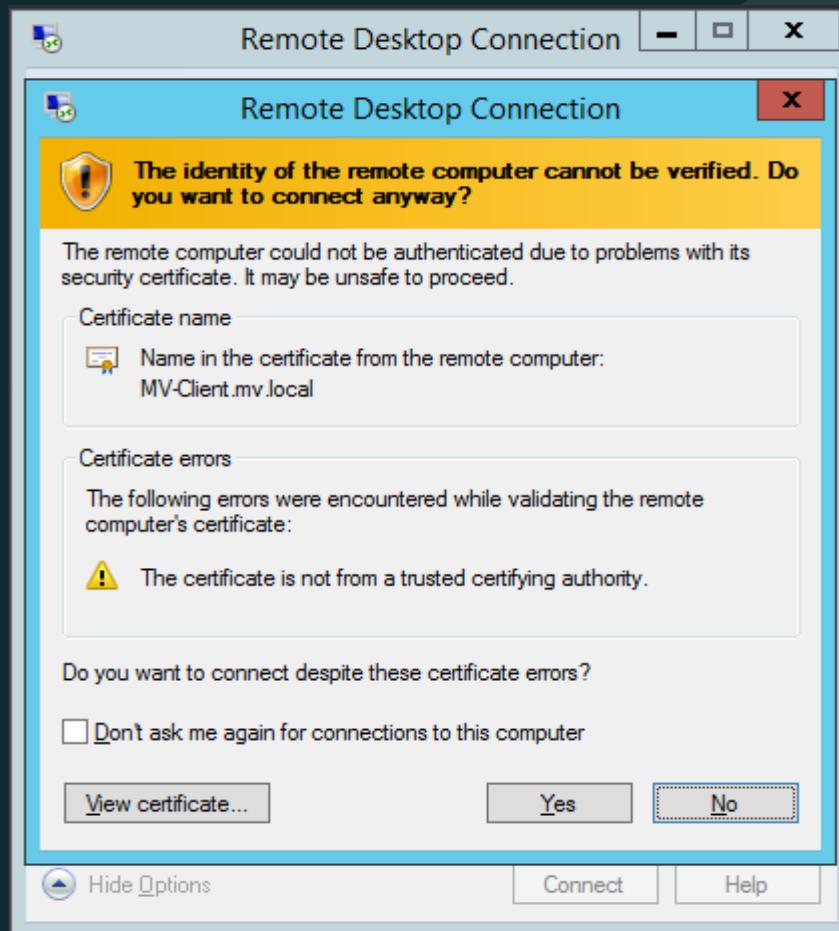
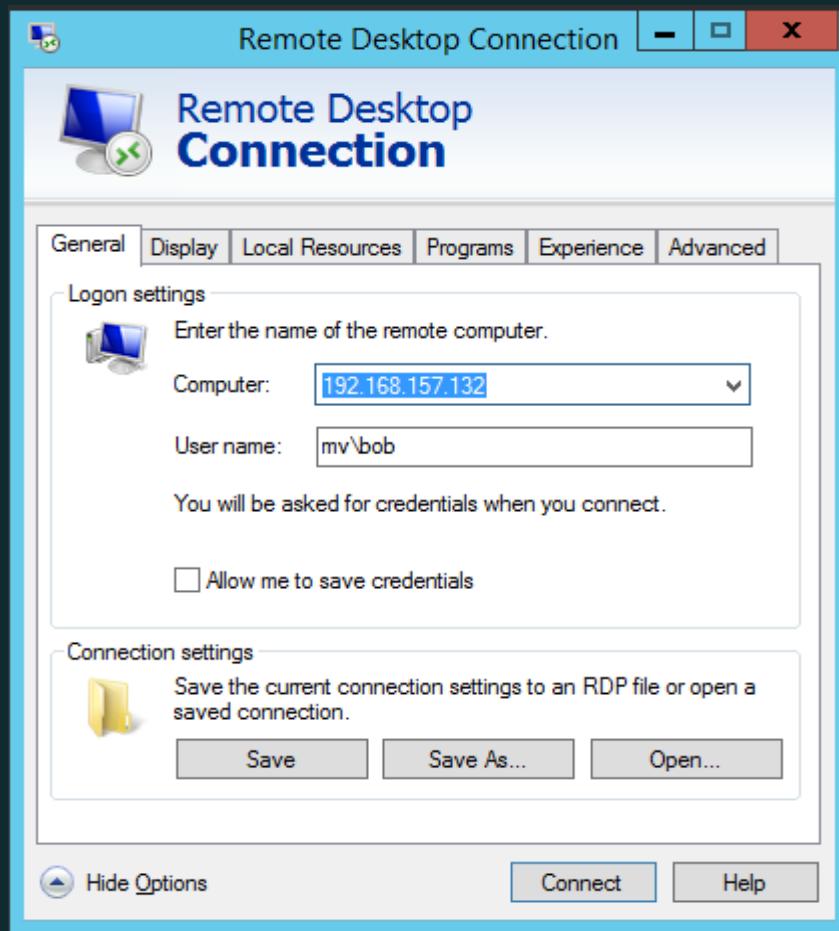
Copy **Close**

Cenário 3 - Runas

Cenário 3 - Runas



Cenário 4 – Logon TS/RDP



Cenário 4 – Logon TS/RDP

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	NULL SID
Account Name:	-
Account Domain:	-
Logon ID:	0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon:

Security ID:	MV\bob
Account Name:	bob
Account Domain:	MV
Logon ID:	0x29C03
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	DC01
Source Network Address:	-
Source Port:	-

Detailed Authentication Information:

Logon Process:	NtLmSpn
Authentication Package:	NTLM
Transited Services:	-
Package Name (NTLM only):	NTLM V2
Key Length:	128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Logged: 19/06/2022 19:30:31
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENTS
Account Domain:	MV
Logon ID:	0x0E7

Logon Type: 3

Impersonation Level: Impersonation

New Logon:

Security ID:	Window Manager(DWM-2)
Account Name:	DWM-2
Account Domain:	Window Manager
Logon ID:	0x29C7C
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	-

Network Information:

Workstation Name:	DC01
Source Network Address:	-
Source Port:	-

Detailed Authentication Information:

Logon Process:	Advapi
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Logged: 19/06/2022 19:30:34
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENTS
Account Domain:	MV
Logon ID:	0x0E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:

Security ID:	Window Manager(DWM-2)
Account Name:	DWM-2
Account Domain:	Window Manager
Logon ID:	0x29C7C
Logon GUID:	{00000000-0000-0000-0000-000000000000}

Process Information:

Process ID:	0x0
Process Name:	C:\Windows\System32\winlogon.exe

Network Information:

Workstation Name:	-
Source Network Address:	-
Source Port:	-

Detailed Authentication Information:

Logon Process:	Advapi
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Logged: 19/06/2022 19:30:35
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Event Properties - Event 4624, Microsoft Windows security auditing.

General Details

An account was successfully logged on.

Subject:

Security ID:	SYSTEM
Account Name:	MV-CLIENTS
Account Domain:	MV
Logon ID:	0x0E7

Logon Type: 2

Impersonation Level: Impersonation

New Logon:

Security ID:	MV\bob
Account Name:	bob
Account Domain:	MV
Logon ID:	0x29E7D
Logon GUID:	{0C36B833-1A5C-d185-f109-de334B94c67}

Process Information:

Process ID:	0x0
Process Name:	C:\Windows\System32\winlogon.exe

Network Information:

Workstation Name:	MV-CLIENT
Source Network Address:	192.168.157.131
Source Port:	0

Detailed Authentication Information:

Logon Process:	Usez32
Authentication Package:	Negotiate
Transited Services:	-
Package Name (NTLM only):	-
Key Length:	0

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Logged: 19/06/2022 19:30:35
Event ID: 4624 Task Category: Logon
Level: Information Keywords: Audit Success
User: N/A Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy Close

Cenário 4 – Logon TS/RDP

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)

Process	CPU	Privat...	Workd...	PID	Description	Company Name	User Name	Session	Command Line
System Idle Process	98.74	0 K	4 K	0		Microsoft Corporation	NT AUTHORITY\SYSTEM	0	
System	1.54	104 K	280 K	4	n/a Hardware Interrupts and DPCs	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
Interrups	< 0.01	0 K	0 K			Microsoft Corporation	NT AUTHORITY\SYSTEM	0	
smss.exe	332 K	1.104 K	216 Windows Session Manager	216	Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
csrss.exe	1.556 K	3.668 K	308 Client Server Runtime Process	308	Windows Shared Section	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
wininit.exe	948 K	3.624 K	428 Windows Start-Up Application	428	Windows Shared Section	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
services.exe	3.196 K	7.404 K	500 Services and Controller app	500	Windows Shared Section	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
svchost.exe	< 0.01	4.128 K	11.036 K	564 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0	0 C:\Windows\system32\svchost.exe -k DcomLaunch
unscapp.exe	884 K	4.124 K	1560 Sink to receive asynchronous callbacks f...	1560	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
WmiPrvSE.exe	8.720 K	13.200 K	1804 WMI Provider Host	1804	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
WmiPrvSE.exe	1.688 K	5.392 K	2552 WMI Provider Host	2552	WMI Provider Host	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
dhcph.exe	1.324 K	4.680 K	3056 COM Surrogate	3056	Windows Shared Section	Microsoft Corporation	MV\bob	0	2 C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:{3EB3C877-1F16-487C-9050-104DBCD66683}
svchost.exe	3.284 K	7.108 K	592 Host Process for Windows Services	592	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0
vm3dservice.exe	940 K	3.544 K	720 VMware SVGA Helper Service	720	VMware SVGA Helper Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0
svchost.exe	19.844 K	23.064 K	764 Host Process for Windows Services	764	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0
svchost.exe	21.196 K	36.616 K	800 Host Process for Windows Services	800	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
taskhost.exe	1.604 K	5.972 K	1244 Host Process for Windows Tasks	1244	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	1	taskhost.exe
taskhost.exe	1.596 K	5.960 K	2092 Host Process for Windows Tasks	2092	Host Process for Windows Tasks	Microsoft Corporation	MV\bob	2	taskhost.exe
svchost.exe	6.380 K	12.244 K	828 Host Process for Windows Services	828	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0
svchost.exe	8.888 K	18.548 K	908 Host Process for Windows Services	908	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0
spoolsv.exe	6.152 K	10.308 K	280 Host Process for Windows Services	280	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0	0
spoolsv.exe	4.084 K	11.200 K	204 Spooler Sub-System App	204	Spooler Sub-System App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
Symon64.exe	4.964 K	10.208 K	1088 System activity monitor	1088	System activity monitor	Syintemals - www.s...	NT AUTHORITY\SYSTEM	0	0
svchost.exe	9.128 K	12.136 K	1160 Host Process for Windows Services	1160	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
VGAuthService.exe	2.724 K	8.304 K	1188 VMware Guest Authentication Service	1188	VMware Guest Authentication Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0
vm vmtold.exe	8.256 K	17.828 K	1220 VMware Tools Core Service	1220	VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0	0
wlms.exe	476 K	2.604 K	1256 Windows License Monitoring Service	1256	Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
svchost.exe	< 0.01	62.080 K	54.172 K	1908 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0	0 C:\Windows\system32\svchost.exe -k tempsvc
rdpclip.exe	1.868 K	6.872 K	2396 RDP Clipboard Monitor	2396	RDP Clipboard Monitor	Microsoft Corporation	MV\bob	0	rdpclip
svchost.exe	1.064 K	2.944 K	1928 Host Process for Windows Services	1928	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0
dhcph.exe	3.224 K	6.388 K	1072 COM Surrogate	1072	COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
msdtc.exe	2.336 K	4.908 K	1812 Microsoft Distributed Transaction Coordinator	1812	Microsoft Distributed Transaction Coordinator	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0	0
lsass.exe	4.584 K	12.356 K	508 Local Security Authority Process	508	Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0
csrss.exe	< 0.01	1.892 K	31.416 K	3064 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0	0	1 %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows\On SubSystemType=Windows ServerDl...1 ServerDl...=winsrv
winlogon.exe	1.092 K	4.896 K	2704 Windows Logon Application	2704	Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1	1 winlogon.exe
dwm.exe	< 0.01	28.736 K	59.092 K	164 Desktop Window Manager	Microsoft Corporation	Window Manager\DW...1	1	1 dwm.exe	
explorer.exe	< 0.01	36.352 K	88.024 K	684 Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	1	1 C:\Windows\Explorer EXE	
vm vmtold.exe	< 0.01	6.128 K	15.316 K	2852 VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator	1	1 C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr	
vm3dservice.exe	1.076 K	4.248 K	1472 VMware SVGA Helper Service	1472	VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator	1	1 C:\Windows\System32\vm3dservice.exe" -u
procexp64.exe	< 0.01	16.880 K	35.716 K	2472 Syintemals Process Explorer	Syintemals - www.s...	MV-CLIENT\Administrator	1	1 C:\Users\Administrator\Desktop\Syintemals Suite\procexp64.exe"	
csrss.exe	< 0.01	1.304 K	12.084 K	1460 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	2	2 %SystemRoot%\system32\csrss.exe ObjectDirectory=Windows SharedSection=1024,20480,768 Windows\On SubSystemType=Windows ServerDl...1 ServerDl...=winsrv	
winlogon.exe	< 0.01	1.320 K	5.064 K	2360 Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	2	2 winlogon.exe	
dwm.exe	< 0.01	6.600 K	36.392 K	748 Desktop Window Manager	Microsoft Corporation	Window Manager\DW...2	2	2 dwm.exe	
explorer.exe	< 0.01	28.876 K	67.508 K	1640 Windows Explorer	Microsoft Corporation	MV\bob	2	2 C:\Windows\Explorer EXE	
vm3dservice.exe	1.056 K	4.280 K	1508 VMware SVGA Helper Service	1508	VMware SVGA Helper Service	VMware, Inc.	MV\bob	2	2 C:\Windows\System32\vm3dservice.exe" -u

Cenário 4 – Logon TS/RDP

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: -
UtcTime: 2022-06-19 22:30:36.689
ProcessGuid: {884951a-a38c-62af-e0e7-290000000000}
ProcessId: 1
Image: C:\Windows\System32\TTheme.exe
FileVersion: 0.3.900.16264 (mbibus_rtm_150821-1623)
Description: TTheme Server Module
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
[OriginalFileName] TTheme.exe
CommandLine: C:\Windows\System32\TTheme.exe -Embedding
[CurrentDirectory] C:\Windows\system32
[User] MV\bob
[LogonGuid] {884951a-a38c-62af-e0e7-290000000000}
LogonId: 0x2E7E0
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA256:AF4FAD184B16335770D9F82C69C1D0A6F3E32C59FFF53B80ADB2287EE483FB
ParentProcessId: 64
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\System32\svchost.exe -k DcomLaunch
ParentUser: NT AUTHORITY\SYSTEM

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: -
UtcTime: 2022-06-19 22:30:36.783
ProcessGuid: {884951a-a38c-62af-e0e7-290000000000}
ProcessId: 229
Image: C:\Windows\System32\rpcclip.exe
FileVersion: 0.3.900.16264 (mbibus_rtm_150915-2141)
Description: RDP Clipboard Monitor
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
[OriginalFileName] rpcclip.exe
CommandLine: rpcclip.exe
[CurrentDirectory] C:\Windows\system32
[User] MV\bob
[LogonGuid] {884951a-a38c-62af-e0e7-290000000000}
LogonId: 0x2E7E0
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA256:AC3984D9BD150CE3EB98244E0CD22C6C80A722AECD1756DDE9F1102E56696
ParentProcessId: 1
ParentImage: C:\Windows\System32\svchost.exe
ParentCommandLine: C:\Windows\System32\svchost.exe -k termsvc
ParentUser: NT AUTHORITY\SYSTEM

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: -
UtcTime: 2022-06-19 22:30:36.954
ProcessGuid: {884951a-a38c-62af-e0e7-290000000000}
ProcessId: 1640
Image: C:\Windows\explorer.exe
FileVersion: 0.3.900.16264 (mbibus_rtm_140721-1952)
Description: Windows Explorer
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
[OriginalFileName] EXPLORER.EXE
CommandLine: C:\Windows\Explorer.EXE
[CurrentDirectory] C:\Windows\system32
[User] MV\bob
[LogonGuid] {884951a-a38c-62af-e0e7-290000000000}
LogonId: 0x2E7E0
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA256:EBC4905FA3CFD1A7B861869BF70CE1D4B52B835CB76DD8B2D42189A7B
ParentProcessId: 1
ParentImage: C:\Windows\System32\userinit.exe
ParentCommandLine: C:\Windows\System32\userinit.exe
ParentUser: NT AUTHORITY\SYSTEM

Event Properties - Event 1, Sysmon

General Details

Process Create:
RuleName: -
UtcTime: 2022-06-19 22:30:36.985
ProcessGuid: {884951a-a38c-62af-e0e7-290000000000}
ProcessId: 1
Image: C:\Windows\explorer.exe
FileVersion: 0.3.900.16264 (mbibus_rtm_140721-1952)
Description: Windows Explorer
Product: Microsoft® Windows® Operating System
Company: Microsoft Corporation
[OriginalFileName] EXPLORER.EXE
CommandLine: C:\Windows\Explorer.EXE
[CurrentDirectory] C:\Windows\system32
[User] MV\bob
[LogonGuid] {884951a-a38c-62af-e0e7-290000000000}
LogonId: 0x2E7E0
TerminalSessionId: 2
IntegrityLevel: Medium
Hashes: SHA256:85270240A5FD51924F0627C92B2282749D071FDC9AC351B81039CED5B10F798B
ParentProcessId: 1
ParentImage: C:\Windows\System32\userinit.exe
ParentCommandLine: C:\Windows\System32\userinit.exe
ParentUser: MV\bob

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 19/06/2022 19:30:36

Event ID: 1 Task Category: Process Create (rule:ProcessCreat)

Level: Information Keywords:

User: SYSTEM Computer: MV-Client.mv.local

OpCode: Info

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

Copy Close

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 19/06/2022 19:30:36

Event ID: 1 Task Category: Process Create (rule:ProcessCreat)

Level: Information Keywords:

User: SYSTEM Computer: MV-Client.mv.local

OpCode: Info

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

Copy Close

Log Name: Microsoft-Windows-Sysmon/Operational

Source: Sysmon Logged: 19/06/2022 19:30:36

Event ID: 1 Task Category: Process Create (rule:ProcessCreat)

Level: Information Keywords:

User: SYSTEM Computer: MV-Client.mv.local

OpCode: Info

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

Copy Close

Cenário 5 – Logon powershell session

File Edit View Tools Debug Add-ons Help

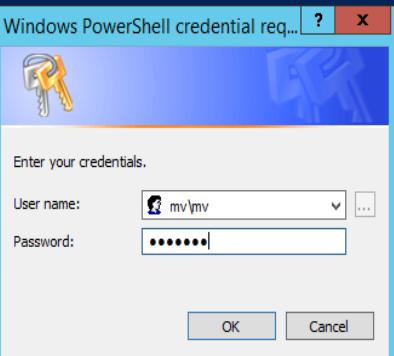
Untitled1.ps1*(Recovered) X

```
1 $session = New-PSSession -ComputerName 192.168.157.132 -Credential "mv\mv"
2 Enter-PSSession $session
```

PS C:\Users\Administrator> hostname
DC01

PS C:\Users\Administrator> \$session = New-PSSession -ComputerName 192.168.157.132 -Credential "mv\mv"
Enter-PSSession \$session

Windows PowerShell credential req... ? X



The dialog box shows a key icon and the text 'Enter your credentials.' It has two input fields: 'User name:' containing 'mv\mv' and 'Password:' containing '*****'. There are 'OK' and 'Cancel' buttons at the bottom.

Administrator: Windows PowerShell ISE

File Edit View Tools Debug Add-ons Help

Untitled1.ps1*(Recovered) X

```
1 $session = New-PSSession -ComputerName 192.168.157.132 -Credential "mv\mv"
2 Enter-PSSession $session
```

PS C:\Users\Administrator> hostname
DC01

PS C:\Users\Administrator> \$session = New-PSSession -ComputerName 192.168.157.132 -Credential "mv\mv"
Enter-PSSession \$session

[192.168.157.132]: PS C:\Users\MV\Documents> hostname
MV-Client

[192.168.157.132]: PS C:\Users\MV\Documents> whoami
mv\mv

[192.168.157.132]: PS C:\Users\MV\Documents>

Cenário 5 – Logon powershell session

An account was successfully logged on.

Subject: Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon: Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0x02248
Logon GUID: [redacted]

Process Information: Process ID: 0x0
Process Name: -

Network Information: Workstation Name: DC01
Source Network Address: -
Source Port: -

Detailed Authentication Information: Logon Process: NtLmSp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

An account was successfully logged on.

Subject: Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon: Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0x02256
Logon GUID: [redacted]

Process Information: Process ID: 0x0
Process Name: -

Network Information: Workstation Name: DC01
Source Network Address: -
Source Port: -

Detailed Authentication Information: Logon Process: NtLmSp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

An account was successfully logged on.

Subject: Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon: Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0x0220E
Logon GUID: [redacted]

Process Information: Process ID: 0x0
Process Name: -

Network Information: Workstation Name: DC01
Source Network Address: -
Source Port: -

Detailed Authentication Information: Logon Process: NtLmSp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

An account was successfully logged on.

Subject: Security ID: NULL SID
Account Name: -
Account Domain: -
Logon ID: 0x0

Logon Type: 3

Impersonation Level: Impersonation

New Logon: Security ID: MV\mv
Account Name: mv
Account Domain: MV
Logon ID: 0x0220E
Logon GUID: [redacted]

Process Information: Process ID: 0x0
Process Name: -

Network Information: Workstation Name: DC01
Source Network Address: -
Source Port: -

Detailed Authentication Information: Logon Process: NtLmSp
Authentication Package: NTLM
Transited Services: -
Package Name (NTLM only): NTLM V2
Key Length: 128

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

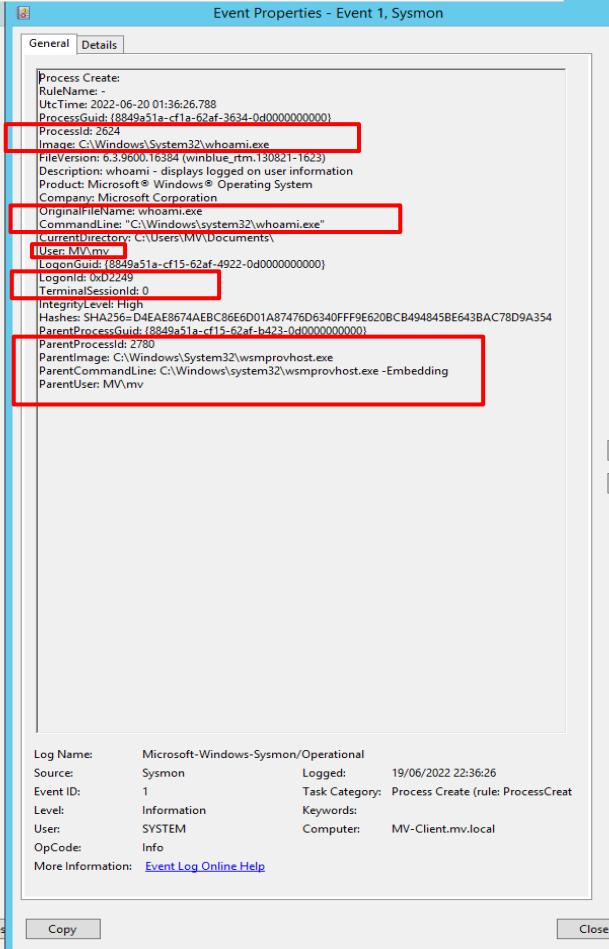
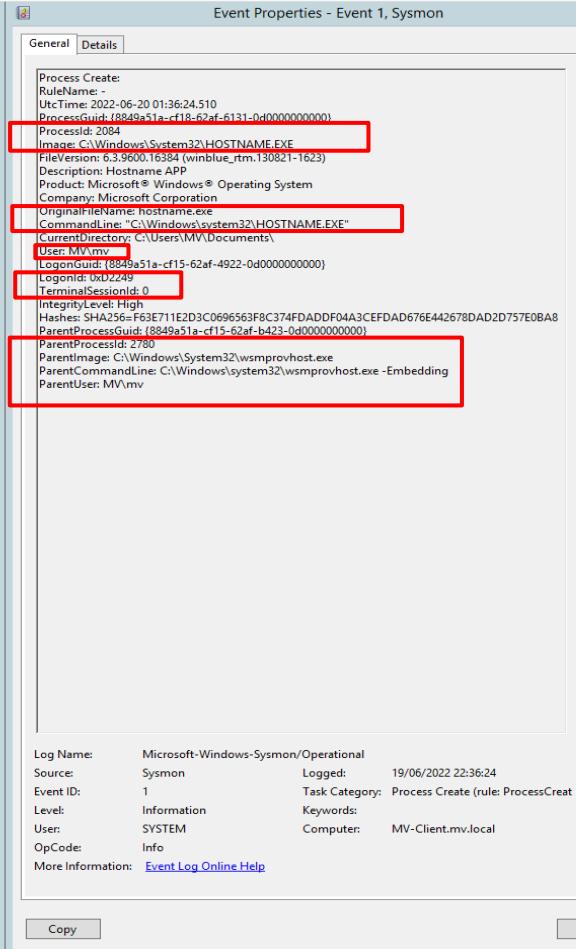
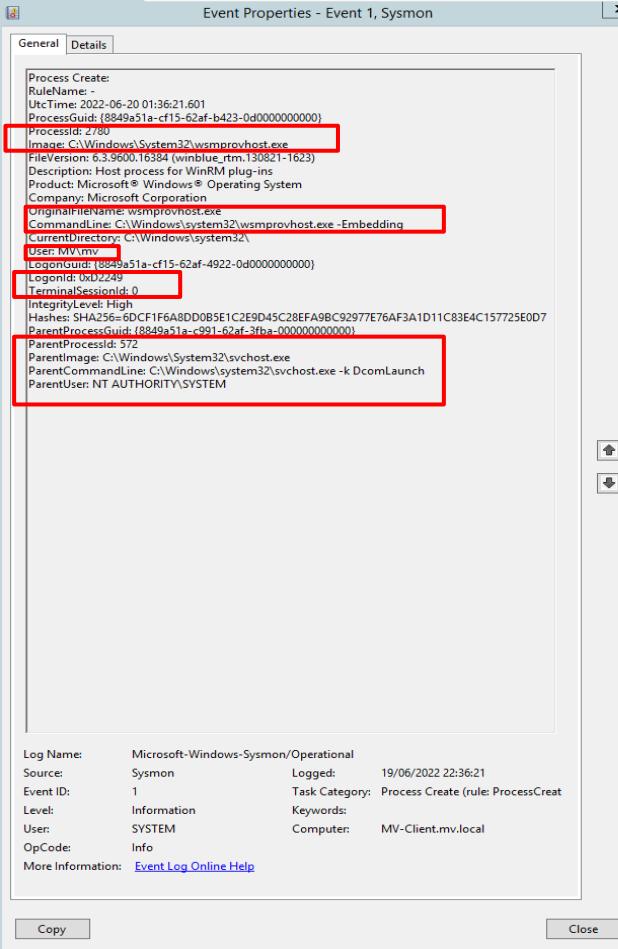
The network fields indicate where a remote logon request originated. Workstation name is not always available and may be left blank in some cases.

Log Name: Security
Source: Microsoft Windows security
Event ID: 4624
Level: Information
User: N/A
OpCode: Info
More Information: [Event Log Online Help](#)

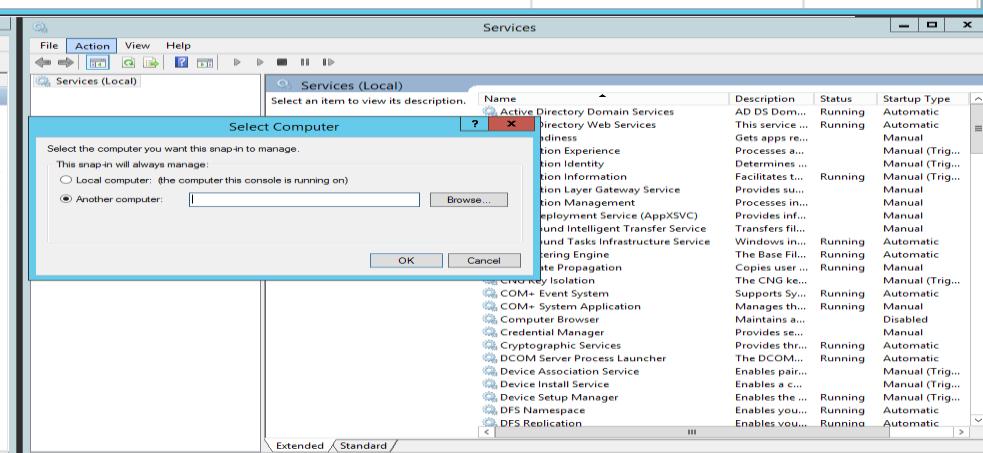
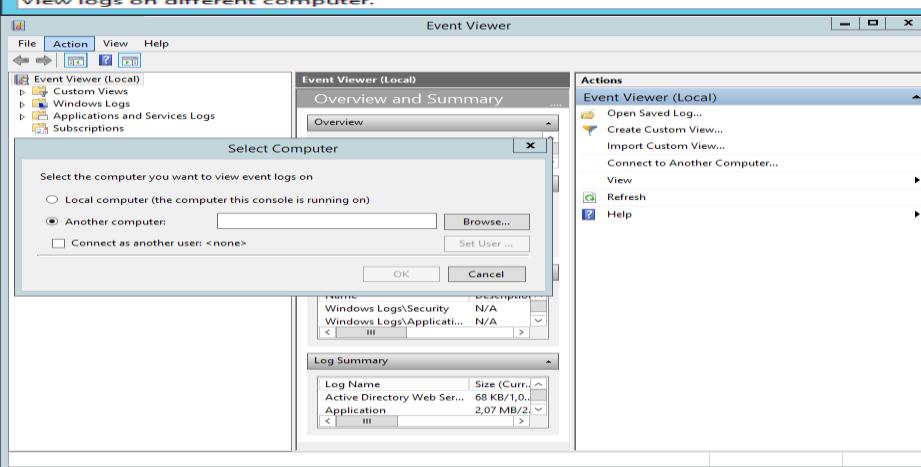
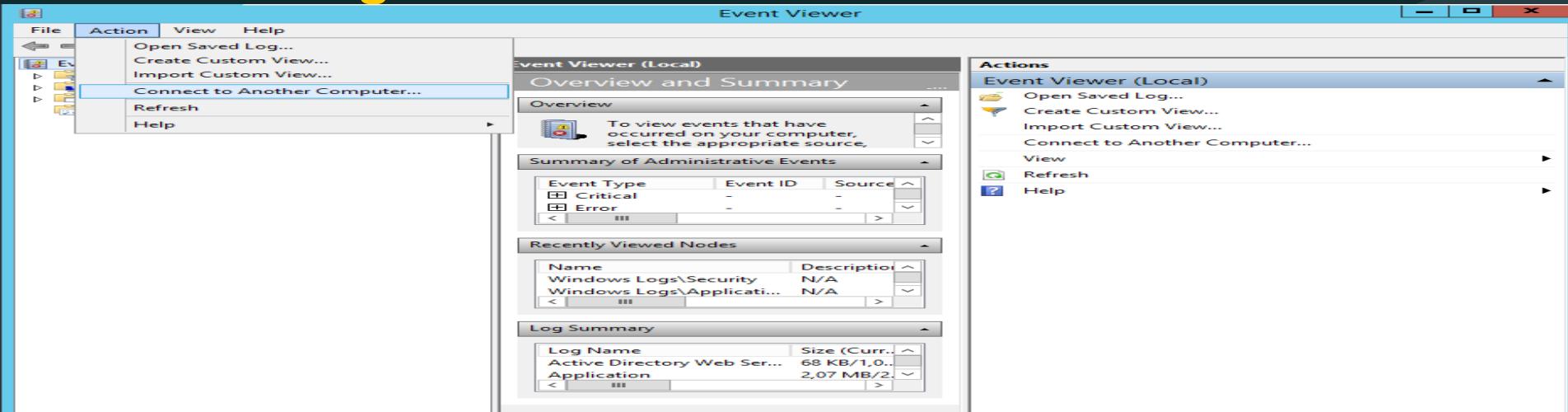
Cenário 5 – Logon powershell session

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)											
File	Options	View	Process	Find	Users	Help	Process	CPU	Privat...	Workin...	PID
							Company Name	User Name	Session	Command Line	
System Idle Process							NT AUTHORITY\SYSTEM				
System	< 0.01	104 K	280 K	4			NT AUTHORITY\SYSTEM		0		
Interrupts	< 0.01	0 K	n/a	Hardware Interrupts and DPCs							
smss.exe		288 K	1.092 K	216 Windows Session Manager	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 \SystemRoot\System32\smss.exe				
csrss.exe		1.560 K	3.680 K	308 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 %SystemRoot%\System32\cssrs.exe ObjectDirectory=\\Windows SharedSection=1024.20480.768 Windows=On SubSystemType=Windows ServerDl=basesrv.1 ServerDl=winsrv:User				
winit.exe		720 K	3.580 K	428 Windows Start-Up Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 wininit.exe				
services.exe	3.096 K	7.352 K	500 Services and Controller app	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\services.exe					
svchost.exe	3.868 K	10.888 K	564 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\svchost.exe -k DcomLaunch					
unsecapp.exe	944 K	4.156 K	1560 Sink to receive asynchronous callbacks from...	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\wben\unsecapp.exe -Embedding					
WmPrvSE.exe	8.332 K	12.968 K	180 WMI Provider Host	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\system32\wben\wmprvse.exe					
wsmprovhost.exe	52.212 K	65.428 K	293 Host process for WinRM plug-ins	Microsoft Corporation	MV-CLIENT\Administrator	0 C:\Windows\system32\wsmprovhost.exe -Embedding					
wsmprovhost.exe	46.556 K	58.908 K	2732 Host process for WinRM plug-ins	Microsoft Corporation	MV\mv	0 C:\Windows\system32\wsmprovhost.exe -Embedding					
wsmprovhost.exe	46.464 K	58.524 K	64 Host process for WinRM plug-ins	Microsoft Corporation	MV\mv	0 C:\Windows\system32\wsmprovhost.exe -Embedding					
wsmprovhost.exe	46.564 K	58.712 K	1652 Host process for WinRM plug-ins	Microsoft Corporation	MV\mv	0 C:\Windows\system32\wsmprovhost.exe -Embedding					
svchost.exe	3.089 K	6.952 K	592 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\system32\svchost.exe -k RPCSS					
vm3dservice.exe	940 K	3.544 K	720 VMware SVGA Helper Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\vm3dservice.exe					
svchost.exe	15.561 K	19.544 K	764 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0 C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted					
svchost.exe	17.648 K	31.404 K	808 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\svchost.exe -k netsvcs					
taskhost.exe	1.500 K	5.948 K	1424 Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	0 taskhost.exe					
svchost.exe	6.249 K	12.008 K	828 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0 C:\Windows\system32\svchost.exe -k LocalService					
svchost.exe	10.712 K	20.300 K	908 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\system32\svchost.exe -k NetworkService					
svchost.exe	6.188 K	10.336 K	280 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\LOCAL SERVICE	0 C:\Windows\system32\svchost.exe -k LocalServiceNoNetwork					
spoolsv.exe	3.732 K	11.072 K	204 Spooler Sub-System App	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\System32\spoolsv.exe					
Symon64.exe	4.946 K	10.196 K	1088 System activity monitor	Syntemate - www.s...	NT AUTHORITY\SYSTEM	0 C:\Windows\Syntemate - www.s...					
svchost.exe	7.440 K	11.184 K	1160 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\System32\svchost.exe -k LocalSystemNetworkRestricted					
VGAuth Service.exe	2.724 K	8.304 K	1188 VMware Guest Authentication Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0 C:\Program Files\VMware\VMware Tools\VMware VGAuth\VGAuth Service.exe"					
vmtoolsd.exe	< 0.01	8.252 K	17.848 K	1220 VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM	0 C:\Program Files\VMware\VMware Tools\vmtoolsd.exe"				
wlms.exe		484 K	2.612 K	1256 Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\system32\wlms\wlms.exe				
svchost.exe		6.352 K	11.884 K	1960 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\System32\svchost.exe -k tempsvc				
svchost.exe		1.064 K	2.944 K	1928 Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\system32\svchost.exe -k NetworkServiceNetworkRestricted				
dlhost.exe		3.116 K	6.344 K	1072 COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\WINDOWS\SYSTEM32\DLLHOST.EXE /PROCESSID:02D4B3F1-FD88-11D1-960D-00805FC79235				
msdtc.exe		2.336 K	4.904 K	1812 Microsoft Distributed Transaction Coordination	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE	0 C:\Windows\System32\msdtc.exe				
lsass.exe		4.908 K	12.752 K	500 Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	0 C:\Windows\System32\lsass.exe				
cssrs.exe	< 0.01	1.904 K	33.096 K	3064 Client Server Runtime Process	Microsoft Corporation	NT AUTHORITY\SYSTEM	1 %SystemRoot%\System32\cssrs.exe ObjectDirectory=\\Windows SharedSection=1024.20480.768 Windows=On SubSystemType=Windows ServerDl=basesrv.1 ServerDl=winsrv:User				
winlogon.exe		1.132 K	5.204 K	2704 Windows Logon Application	Microsoft Corporation	NT AUTHORITY\SYSTEM	1 winlogon.exe				
dwm.exe	< 0.01	34.708 K	67.552 K	164 Desktop Window Manager	Microsoft Corporation	Window Manager\DWIM-1	1 dwm.exe"				
explorer.exe	< 0.01	36.328 K	91.416 K	684 Windows Explorer	Microsoft Corporation	MV-CLIENT\Administrator	1 C:\Windows\Explorer.EXE				
vmtoolsd.exe	< 0.01	8.000 K	17.768 K	2852 VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator	1 "C:\Program Files\VMware\VMware Tools\vmtoolsd.exe" -n vmusr				
vm3dservice.exe		1.024 K	4.356 K	1472 VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator	1 "C:\Windows\System32\vm3dservice.exe" -u				
procexp64.exe	< 0.01	17.288 K	36.796 K	2472 Syntemate Process Explorer	Syntemate - www.s...	MV-CLIENT\Administrator	1 "C:\Users\Administrator\Desktop\Syntemate Suite\procexp64.exe"				

Cenário 5 – Logon powershell session



Cenário 6 – Logon services ou eventviewer



Cenário 6 – Logon services ou eventviewer

The screenshot displays six separate windows of the Windows Event Viewer, all showing the properties of Event ID 4624 (Microsoft Windows security auditing). Each window provides detailed information about a successful logon attempt.

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: Kerberos; Authentication Package: Kerberos; Transited Services: -; Package Name (NTLM only): -; Key Length: 0.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:04
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: Kerberos; Authentication Package: Kerberos; Transited Services: -; Package Name (NTLM only): -; Key Length: 0.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:04
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: NTLMSP; Authentication Package: NTLM; Transited Services: -; Package Name (NTLM only): -; Key Length: 128.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:08
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: Kerberos; Authentication Package: Kerberos; Transited Services: -; Package Name (NTLM only): -; Key Length: 0.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:08
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: Kerberos; Authentication Package: Kerberos; Transited Services: -; Package Name (NTLM only): -; Key Length: 0.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:08
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Event Properties - Event 4624, Microsoft Windows security auditing:

- General:** An account was successfully logged on.
- Subject:** Security ID: NULL SID; Account Name: -; Account Domain: -; Logon ID: 0x0.
- Logon Type:** 3 (Interactive).
- Impersonation Level:** Impersonation.
- New Logon:** Security ID: MV\mv; Account Name: mv; Account Domain: MV; Logon ID: 0x156056; Logon GUID: {ca04bf-0aee-1b4c-9cb8-0d4f3e0c5e03}.
- Process Information:** Process ID: 0x0; Process Name: -.
- Network Information:** Workstation Name: -; Source Network Address: 192.168.157.131; Source Port: 59161.
- Detailed Authentication Information:** Logon Process: Kerberos; Authentication Package: Kerberos; Transited Services: -; Package Name (NTLM only): -; Key Length: 0.

This event is generated when a logon session is created. It is generated on the computer that was accessed.

The subject fields indicate the account on the local system which requested the logon. This is most commonly a service such as the Server service, or a local process such as Winlogon.exe or Services.exe.

The logon type field indicates the kind of logon that occurred. The most common types are 2 (interactive) and 3 (network).

The New Logon fields indicate the account for whom the new logon was created, i.e. the account that was logged on.

Log Name: Security
Source: Microsoft Windows security
Logged: 27/06/2022 22:12:08
Event ID: 4624
Task Category: Logon
Level: Information
Keywords: Audit Success
User: N/A
Computer: MV-Client.mv.local
OpCode: Info
More Information: [Event Log Online Help](#)

Copy **Close**

Cenário 6 – Logon services ou eventviewer

Process Explorer - Sysinternals: www.sysinternals.com [MV-CLIENT\Administrator] (Administrator)								
File	Options	View	Process	Find	Users	Help		<Filter by name>
Process	CPU	Private	Workin...	PID	Description	Company Name	User Name	Session Command Line
System Idle Process	96.64	0 K	4 K	0		NT AUTHORITY\SYSTEM	NT AUTHORITY\SYSTEM	0
System	< 0.01	104 K	272 K	4	n/a Hardware Interrupts and DPCs			
Interrupts								
smss.exe								
carss.exe								
wininit.exe								
services.exe								
svchost.exe								
Unsecapp.exe								
wmiPrvSE.exe								
svchost.exe								
vm3dservice.exe								
svchost.exe								
svchost.exe								
taskhost.exe								
svchost.exe								
svchost.exe								
svchost.exe								
spoolsv.exe								
symsym64.exe								
svchost.exe								
VGAuthService.exe								
vmtoolsd.exe	1.51	5.596 K	1536 K	1536	Host Process for Windows Tasks	Microsoft Corporation	MV-CLIENT\Administrator	1 taskhost.exe
svchost.exe								
svchost.exe								
svchost.exe								
svchost.exe								
spoolsv.exe								
2.912 K	8.70 K	1068 K	Spooler SubSystem App	Microsoft Corporation	NT AUTHORITY\SYSTEM			
4.928 K	11.256 K	1124 K	System activity monitor	Sysinternals - www.s...	NT AUTHORITY\SYSTEM			
8.116 K	10.340 K	1148 K	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\SYSTEM			
2.752 K	8.344 K	1200 K	VMware Guest Authentication Service	VMware, Inc.	NT AUTHORITY\SYSTEM			
1.848 K	17.500 K	1260 K	VMware Tools Core Service	VMware, Inc.	NT AUTHORITY\SYSTEM			
4.76 K	2.604 K	1300 K	Windows License Monitoring Service	Microsoft Corporation	NT AUTHORITY\SYSTEM			
3.576 K	7.924 K	1688 K	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE			
1.016 K	4.332 K	1788 K	Host Process for Windows Services	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE			
3.128 K	9.972 K	1092 K	COM Surrogate	Microsoft Corporation	NT AUTHORITY\SYSTEM			
2.268 K	6.764 K	2132 K	Microsoft Distributed Transaction Coordinator	Microsoft Corporation	NT AUTHORITY\NETWORK SERVICE			
4.080 K	11.272 K	520 K	Local Security Authority Process	Microsoft Corporation	NT AUTHORITY\SYSTEM			
svchost.exe								
dflhost.exe								
msdc.exe								
lsass.exe								
carss.exe								
winlogon.exe								
dwm.exe								
explorer.exe								
vmtoolsd.exe								
vm3dservice.exe								
procexp64.exe	3.02	17.360 K	37.228 K	700 Systeminternals Process Explorer	Sysinternals - www.s...	MV-CLIENT\Administrator		
45.108 K	109.368 K	2960 K	VMware Tools Core Service	VMware, Inc.	MV-CLIENT\Administrator			
1.028 K	4.368 K	3004 K	VMware SVGA Helper Service	VMware, Inc.	MV-CLIENT\Administrator			

Cenário 6 – Logon services ou eventviewer

E agora o que fazer?

Os processos não mudaram e o log de logon não diz que recurso foi acessado

Cenário 6 – Logon services ou eventviewer

TCPView - Sysinternals: www.sysinternals.com

File	Edit	View	Process	Connection	Options	Help	4 TCP v4	6 TCP v6	4 UDP v4	6 UDP v6	Search		
Process Name	Process ID	Protocol	State	Local Address	Local Port	Remote Address	Remote Port	Create Time	Module Name	Sent Packets	Recv Packets	Sent Bytes	Recv Bytes
svchost.exe	592	TCP	Listen	0.0.0.0	135	0.0.0.0	0		RpcSs				
svchost.exe	592	TCP	Established	192.168.157.132	135	192.168.157.131	59162	27/06/2022 22:12:08	RpcSs	2	2	280	328
System	4	TCP	Listen	192.168.157.132	139	0.0.0.0	0		System				
svchost.exe	1784	TCP	Listen	0.0.0.0	3389	0.0.0.0	0		TermService				
wininit.exe	404	TCP	Listen	0.0.0.0	49152	0.0.0.0	0		wininit.exe				
svchost.exe	828	TCP	Listen	0.0.0.0	49153	0.0.0.0	0		EventLog				
svchost.exe	828	TCP	Established	192.168.157.132	49154	192.168.157.131	59165	27/06/2022 22:12:29	EventLog	4	6	3.074	2.059
svchost.exe	856	TCP	Listen	0.0.0.0	49154	0.0.0.0	0		Schedule				
lsass.exe	492	TCP	Listen	0.0.0.0	49155	0.0.0.0	0		Netlogon				
spoolsv.exe	1048	TCP	Listen	0.0.0.0	49156	0.0.0.0	0		Spooler				
lsass.exe	492	TCP	Listen	0.0.0.0	49181	0.0.0.0	0		lsass.exe				
services.exe	484	TCP	Listen	0.0.0.0	49182	0.0.0.0	0		services.exe				
services.exe	484	TCP	Established	192.168.157.132	49182	192.168.157.131	59163	27/06/2022 22:12:08	services.exe	803	801	703.606	69.198
svchost.exe	1864	TCP	Listen	0.0.0.0	49183	0.0.0.0	0		PolicyAgent				
[Time Wait]		TCP	Time Wait	192.168.157.132	49195	192.168.157.131	135						
[Time Wait]		TCP	Time Wait	192.168.157.132	49196	192.168.157.131	49157						
System	4	TCP	Listen	0.0.0.0	445	0.0.0.0	0		System				
System	4	TCP	Listen	0.0.0.0	5985	0.0.0.0	0		System				
System	4	TCP	Listen	0.0.0.0	47001	0.0.0.0	0		System				
svchost.exe	592	TCPv6	Listen	::	135	::	0		RpcSs				
System	4	TCPv6	Listen	::	445	::	0		System				
svchost.exe	1784	TCPv6	Listen	::	3389	::	0		TermService				
System	4	TCPv6	Listen	::	5985	::	0		System				
System	4	TCPv6	Listen	::	47001	::	0		System				
wininit.exe	404	TCPv6	Listen	::	49152	::	0		wininit.exe				
svchost.exe	828	TCPv6	Listen	::	49153	::	0		EventLog				
svchost.exe	856	TCPv6	Listen	::	49154	::	0		Schedule				
lsass.exe	492	TCPv6	Listen	::	49155	::	0		Netlogon				
spoolsv.exe	1048	TCPv6	Listen	::	49156	::	0		Spooler				
lsass.exe	492	TCPv6	Listen	::	49181	::	0		lsass.exe				
services.exe	484	TCPv6	Listen	::	49182	::	0		services.exe				
svchost.exe	1864	TCPv6	Listen	::	49183	::	0		PolicyAgent				
svchost.exe	900	UDP	0.0.0.0		123	*		27/06/2022 22:02:34	W32Time				
System	4	UDP	192.168.157.132		137	*		27/06/2022 22:02:20	System				
System	4	UDP	192.168.157.132		138	*		27/06/2022 22:02:20	System				
svchost.exe	856	UDP	0.0.0.0		500	*		27/06/2022 22:02:24	IKEEEXT				
svchost.exe	1784	UDP	0.0.0.0		3389	*		27/06/2022 22:02:34	TermService				
svchost.exe	856	UDP	0.0.0.0		4500	*		27/06/2022 22:02:24	IKEEEXT				
svchost.exe	964	UDP	0.0.0.0		5355	*		27/06/2022 22:02:23	Dnscache				
lsass.exe	492	UDP	127.0.0.1		50313	*		27/06/2022 22:02:24	Netlogon				
Endpoints: 47	Established: 3	Listening: 27	Time Wait: 2	Close Wait:	Update: 2 sec	States: (All)							

Cenário 6 – Logon services ou eventviewer

The image displays four windows of the Event Properties - Event 3, Sysmon tool, each showing a different logon event. The windows are arranged horizontally. Each window has a red box highlighting specific fields in the details tab.

Event Properties - Event 3, Sysmon (Left):

Log Name:	Source:	Level:	Event ID:	Task Category:	Keywords:	User:	Computer:	OpCode:	More Information:
Microsoft-Windows-Sysmon/Operational	Sysmon	Information	3	Network connection detected (rule: Network)		SYSTEM	MV-Client.mv.local	Info	Event Log Online Help

Event Properties - Event 1, Sysmon (Second from Left):

Log Name:	Source:	Level:	Event ID:	Task Category:	Keywords:	User:	Computer:	OpCode:	More Information:
Microsoft-Windows-Sysmon/Operational	Sysmon	Information	1	Process Create (rule: ProcessCreate)		SYSTEM	MV-Client.mv.local	Info	Event Log Online Help

Event Properties - Event 3, Sysmon (Third from Left):

Log Name:	Source:	Level:	Event ID:	Task Category:	Keywords:	User:	Computer:	OpCode:	More Information:
Microsoft-Windows-Sysmon/Operational	Sysmon	Information	3	Network connection detected (rule: Network)		SYSTEM	MV-Client.mv.local	Info	Event Log Online Help

Event Properties - Event 1, Sysmon (Right):

Log Name:	Source:	Level:	Event ID:	Task Category:	Keywords:	User:	Computer:	OpCode:	More Information:
Microsoft-Windows-Sysmon/Operational	Sysmon	Information	1	Process Create (rule: ProcessCreate)		SYSTEM	MV-Client.mv.local	Info	Event Log Online Help

Details Tab Fields (highlighted in red boxes):

- Event 1, Sysmon (Second from Left):
 - Image: C:\Windows\System32\svchost.exe
 - User: NT AUTHORITY\SYSTEM
 - OriginalFileName: svchost.exe
 - CommandLine: C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
 - User: NT AUTHORITY\LOCAL SERVICE
 - LogonId: 0x3E5
 - TerminalSessionId: 0
 - ParentProcessId: 484
 - ParentImage: C:\Windows\System32\services.exe
 - ParentCommandLine: C:\Windows\system32\services.exe
 - ParentUser: NT AUTHORITY\SYSTEM
- Event 3, Sysmon (Left):
 - Image: C:\Windows\System32\svchost.exe
 - User: NT AUTHORITY\LOCAL SERVICE
 - OriginalFileName: svchost.exe
 - CommandLine: C:\Windows\System32\svchost.exe -k LocalServiceNetworkRestricted
 - User: NT AUTHORITY\LOCAL SERVICE
 - LogonId: 0x3E5
 - TerminalSessionId: 0
 - ParentProcessId: 484
 - ParentImage: C:\Windows\System32\services.exe
 - ParentCommandLine: C:\Windows\system32\services.exe
 - ParentUser: NT AUTHORITY\SYSTEM
- Event 3, Sysmon (Third from Left):
 - Image: C:\Windows\System32\services.exe
 - User: NT AUTHORITY\SYSTEM
 - OriginalFileName: services.exe
 - CommandLine: C:\Windows\System32\services.exe
 - User: NT AUTHORITY\SYSTEM
 - LogonId: 0x3E7
 - TerminalSessionId: 0
 - ParentProcessId: 404
 - ParentImage: C:\Windows\System32\wininit.exe
 - ParentCommandLine: wininit.exe
 - ParentUser: NT AUTHORITY\SYSTEM
- Event 1, Sysmon (Right):
 - Image: C:\Windows\System32\services.exe
 - User: NT AUTHORITY\SYSTEM
 - OriginalFileName: services.exe
 - CommandLine: C:\Windows\System32\services.exe
 - User: NT AUTHORITY\SYSTEM
 - LogonId: 0x3E7
 - TerminalSessionId: 0
 - ParentProcessId: 404
 - ParentImage: C:\Windows\System32\wininit.exe
 - ParentCommandLine: wininit.exe
 - ParentUser: NT AUTHORITY\SYSTEM

Conclusão



Conclusão

- **TENHA LOGS;**
- Os logs se complementam;
- Dependendo do cenário a telemetria de processos pode substituir o log de acesso;
- Os logs de telemetria de rede são úteis, desde que tenha os logs de telemetria de processos para correlacionar;
- Sempre consulte/correlacione/use mais de uma fonte de logs;
- Entender o “**porque das coisas**” pode te salvar da dependência de um log específico e ajuda a extrair o máximo de informações;
- Façam testes e laboratórios para entender o “**porque das coisas**”.

Referências



Referências

- <https://www.alteredsecurity.com/post/fantastic-windows-logon-types-and-where-to-find-credentials-in-them#viewer-f74bo>
- <https://techcommunity.microsoft.com/t5/itops-talk-blog/deep-dive-logging-on-to-windows/ba-p/2420705>
- <https://techcommunity.microsoft.com/t5/ask-the-performance-team/sessions-desktops-and-windows-stations/ba-p/372473>
- <https://www.ultimatewindowssecurity.com/securitylog/book/default.aspx>
- <https://www.sans.org/posters/hunt-evil/>
- Mais referências estarão no github, junto com essa apresentação.

Dúvidas?



Dúvidas?



- Não tenham medo de mim haha
- Vejo vocês no QA



Obrigado!

MAIS UM EVENTO:



REALIZAÇÃO:



telegram/mvvamo
linkedin/mvmoliveira



twitter/Marcus_mcs
github/mwamo

roadsec.com.br | @roadsec | #dontstophacking