Log Number	1
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Variable" is Started. Details: ProviderName=Variable NewProviderState=Started SequenceNumber=11 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4095
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.674531Z
TimeWritten	2022-10-04T08:06:11.674531Z
Type	Information
User	N/A

Log Number	2

Category	4
CategoryString	Engine Lifecycle
ComputerName	sandbox
EventCode	400
EventIdentifier	400
EventType	3
Logfile	Windows PowerShell
Message	Engine state is changed from None to Available. Details: NewEngineState=Available PreviousEngineState=None SequenceNumber=13 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=5.1.22621.169 RunspaceId=294ed587-7265-4bfa-bcf7-ba74259544cd PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4096
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:12.232165Z
TimeWritten	2022-10-04T08:06:12.232165Z
Type	Information
User	N/A

Log Number	**3**
Category	12548

CategoryString	Special Logon
ComputerName	sandbox
EventCode	4672
EventIdentifier	4672
EventType	4
Logfile	Security
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
RecordNumber	17079
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.702543Z
TimeWritten	2022-10-05T02:53:54.702543Z
Type	Audit Success
User	N/A

Log Number	**4**
Category	0
CategoryString	N/A
ComputerName	sandbox

EventCode	16394
EventIdentifier	-1073725430
EventType	3
Logfile	Application
Message	Offline downlevel migration succeeded.
RecordNumber	7422
SourceName	Microsoft-Windows-Security-SPP
TimeGenerated	2022-10-05T02:53:56.774261Z
TimeWritten	2022-10-05T02:53:56.774261Z
Type	Information
User	N/A

Log Number	**5**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Registry" is Started. Details: ProviderName=Registry NewProviderState=Started SequenceNumber=1 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId=

	CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4246
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.588841Z
TimeWritten	2022-10-05T02:54:37.588841Z
Type	Information
User	N/A

Log Number	**6**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName=

	CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4250
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.599284Z
TimeWritten	2022-10-05T02:54:37.599284Z
Type	Information
User	N/A

Log Number	**7**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Registry" is Started. Details: ProviderName=Registry NewProviderState=Started SequenceNumber=1 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType=

	ScriptName= CommandPath= CommandLine=
RecordNumber	4253
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.36052Z
TimeWritten	2022-10-05T02:58:07.36052Z
Type	Information
User	N/A

Log Number	**8**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Alias" is Started. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName=

	CommandPath= CommandLine=
RecordNumber	4254
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.361018Z
TimeWritten	2022-10-05T02:58:07.361018Z
Type	Information
User	N/A

Log Number	**9**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Function" is Started. Details: ProviderName=Function NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath=

	CommandLine=
RecordNumber	4257
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.401071Z
TimeWritten	2022-10-05T02:58:07.401071Z
Type	Information
User	N/A

Log Number	**10**
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SANDBOX$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18

Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x304
Process Name: C:\Windows\System32\services.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. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
RecordNumber	17318
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T15:57:05.586776Z
TimeWritten	2022-10-05T15:57:05.586776Z
Type	Audit Success
User	N/A

Log Number	**11**
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	10016
EventIdentifier	10016
EventType	2
Logfile	System
Message	The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID

	{2593F8B9-4EAF-457C-B68A-50F6B8EA6B54} and APPID {15C20B67-12E7-4BB6-92BB-7AFF07997402} to the user sandbox\guru SID (S-1-5-21-3249831223-3918070856-2126610958-1001) from address LocalHost (Using LRPC) running in the application container Unavailable SID (Unavailable). This security permission can be modified using the Component Services administrative tool.
RecordNumber	7205
SourceName	Microsoft-Windows-DistributedCOM
TimeGenerated	2022-10-05T16:38:37.724846Z
TimeWritten	2022-10-05T16:38:37.724846Z
Type	Warning
User	sandbox\guru

Log Number	**12**
Category	12292
CategoryString	Other System Events
ComputerName	sandbox
EventCode	5058
EventIdentifier	5058
EventType	4
Logfile	Security
Message	Key file operation. Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox Logon ID: 0xC7B7D6A Process Information: Process ID: 14592 Process Creation Time: ?2022?-?10?-?05T11:08:37.273091600Z Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider

	Algorithm Name: ECDSA_P256 Key Name: Microsoft-Edge-TB-test-key Key Type: User key. Key File Operation Information: File Path: C:\Users\guru\AppData\Roaming\Microsoft\Crypto\Keys\53caafca80232173a709de019a f770-4829-8e8b-55f975dac4a9 Operation: Delete key file. Return Code: 0x0
RecordNumber	17335
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T16:38:40.787809Z
TimeWritten	2022-10-05T16:38:40.787809Z
Type	Audit Success
User	N/A

Log Number	**13**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Alias" is Started. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22621.169

	HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4091
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.653928Z
TimeWritten	2022-10-04T08:06:11.653928Z
Type	Information
User	N/A

Log Number	**14**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Environment" is Started. Details: ProviderName=Environment NewProviderState=Started SequenceNumber=5 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161

	HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4092
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.655681Z
TimeWritten	2022-10-04T08:06:11.655681Z
Type	Information
User	N/A

Log Number	**15**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "FileSystem" is Started. Details: ProviderName=FileSystem NewProviderState=Started SequenceNumber=7 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe

	EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4093
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.671192Z
TimeWritten	2022-10-04T08:06:11.671192Z
Type	Information
User	N/A

Log Number	**16**
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SANDBOX$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes

Impersonation Level: Impersonation

New Logon:
Security ID: S-1-5-18
Account Name: SYSTEM
Account Domain: NT AUTHORITY
Logon ID: 0x3E7
Linked Logon ID: 0x0
Network Account Name: -
Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x304
Process Name: C:\Windows\System32\services.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. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
RecordNumber	17080
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.924526Z
TimeWritten	2022-10-05T02:53:54.924526Z
Type	Audit Success
User	N/A

Log Number	**17**
Category	12548
CategoryString	Special Logon
ComputerName	sandbox

EventCode	4672
EventIdentifier	4672
EventType	4
Logfile	Security
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
RecordNumber	17081
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.924539Z
TimeWritten	2022-10-05T02:53:54.924539Z
Type	Audit Success
User	N/A

Log Number	**18**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600

EventType	3
Logfile	Windows PowerShell
Message	Provider "Alias" is Started. Details: ProviderName=Alias NewProviderState=Started SequenceNumber=3 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4247
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.58953Z
TimeWritten	2022-10-05T02:54:37.58953Z
Type	Information
User	N/A

Log Number	**19**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3

Logfile	Windows PowerShell
Message	Provider "Variable" is Started. Details: ProviderName=Variable NewProviderState=Started SequenceNumber=11 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4251
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.600602Z
TimeWritten	2022-10-05T02:54:37.600602Z
Type	Information
User	N/A

Log Number	**20**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell

Message	Provider "Environment" is Started. Details: ProviderName=Environment NewProviderState=Started SequenceNumber=5 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4255
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.361271Z
TimeWritten	2022-10-05T02:58:07.361271Z
Type	Information
User	N/A

Log Number	**21**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Variable" is Started.

	Details: ProviderName=Variable NewProviderState=Started SequenceNumber=11 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4258
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.403133Z
TimeWritten	2022-10-05T02:58:07.403133Z
Type	Information
User	N/A

Log Number	**22**
Category	4
CategoryString	Engine Lifecycle
ComputerName	sandbox
EventCode	400
EventIdentifier	400
EventType	3
Logfile	Windows PowerShell
Message	Engine state is changed from None to Available.

	Details: NewEngineState=Available PreviousEngineState=None SequenceNumber=13 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=5.1.22621.169 RunspaceId=40acef8c-09e8-431e-be19-d3ee00dd6498 PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4259
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.922265Z
TimeWritten	2022-10-05T02:58:07.922265Z
Type	Information
User	N/A

Log Number	**23**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Registry" is Started.

	Details: ProviderName=Registry NewProviderState=Started SequenceNumber=1 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4090
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.649372Z
TimeWritten	2022-10-04T08:06:11.649372Z
Type	Information
User	N/A

Log Number	**24**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Function" is Started. Details:

	ProviderName=Function NewProviderState=Started SequenceNumber=9 HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=0ed7b684-e68a-45c6-bc00-6b6d9f8a7161 HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4094
SourceName	PowerShell
TimeGenerated	2022-10-04T08:06:11.672918Z
TimeWritten	2022-10-04T08:06:11.672918Z
Type	Information
User	N/A

Log Number	**25**
Category	100
CategoryString	N/A
ComputerName	sandbox
EventCode	105
EventIdentifier	105
EventType	3
Logfile	System
Message	Power source change.
RecordNumber	7112
SourceName	Microsoft-Windows-Kernel-Power
TimeGenerated	2022-10-05T02:53:53.526809Z

TimeWritten	2022-10-05T02:53:53.526809Z
Type	Information
User	NT AUTHORITY\SYSTEM

Log Number	**26**
Category	12544
CategoryString	Logon
ComputerName	sandbox
EventCode	4624
EventIdentifier	4624
EventType	4
Logfile	Security
Message	An account was successfully logged on. Subject: Security ID: S-1-5-18 Account Name: SANDBOX$ Account Domain: WORKGROUP Logon ID: 0x3E7 Logon Information: Logon Type: 5 Restricted Admin Mode: - Remote Credential Guard: - Virtual Account: No Elevated Token: Yes Impersonation Level: Impersonation New Logon: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Linked Logon ID: 0x0 Network Account Name: -

Network Account Domain: -
Logon GUID: {00000000-0000-0000-0000-000000000000}

Process Information:
Process ID: 0x304
Process Name: C:\Windows\System32\services.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. The impersonation level field indicates the extent to which a process in the logon session can impersonate. The authentication information fields provide detailed information about this specific logon request. - Logon GUID is a unique identifier that can be used to correlate this event with a KDC event. - Transited services indicate which intermediate services have participated in this logon request. - Package name indicates which sub-protocol was used among the NTLM protocols. - Key length indicates the length of the generated session key. This will be 0 if no session key was requested.
RecordNumber	17078
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T02:53:54.702531Z
TimeWritten	2022-10-05T02:53:54.702531Z
Type	Audit Success
User	N/A

Log Number	**27**
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	15
EventIdentifier	15
EventType	3
Logfile	Application
Message	Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.
RecordNumber	7421
SourceName	SecurityCenter
TimeGenerated	2022-10-05T02:53:55.800172Z
TimeWritten	2022-10-05T02:53:55.800172Z

Type	Information
User	N/A

Log Number	**28**
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	16384
EventIdentifier	1073758208
EventType	3
Logfile	Application
Message	Successfully scheduled Software Protection service for re-start at 2122-09-10T21:24:34Z. Reason: RulesEngine.
RecordNumber	7423
SourceName	Microsoft-Windows-Security-SPP
TimeGenerated	2022-10-05T02:54:34.880793Z
TimeWritten	2022-10-05T02:54:34.880793Z
Type	Information
User	N/A

Log Number	**29**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "Environment" is Started. Details: ProviderName=Environment NewProviderState=Started SequenceNumber=5

	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4248
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.589936Z
TimeWritten	2022-10-05T02:54:37.589936Z
Type	Information
User	N/A

Log Number	**30**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "FileSystem" is Started. Details: ProviderName=FileSystem NewProviderState=Started SequenceNumber=7

	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4249
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.59774Z
TimeWritten	2022-10-05T02:54:37.59774Z
Type	Information
User	N/A

Log Number	**31**
Category	4
CategoryString	Engine Lifecycle
ComputerName	sandbox
EventCode	400
EventIdentifier	400
EventType	3
Logfile	Windows PowerShell
Message	Engine state is changed from None to Available. Details: NewEngineState=Available PreviousEngineState=None SequenceNumber=13

	HostName=ConsoleHost HostVersion=5.1.22621.169 HostId=4cea8f63-8b91-448c-b01c-64f1cdac22da HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion=5.1.22621.169 RunspaceId=67503dfb-db10-4832-a25a-86a1f432a8e3 PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4252
SourceName	PowerShell
TimeGenerated	2022-10-05T02:54:37.973293Z
TimeWritten	2022-10-05T02:54:37.973293Z
Type	Information
User	N/A

Log Number	**32**
Category	6
CategoryString	Provider Lifecycle
ComputerName	sandbox
EventCode	600
EventIdentifier	600
EventType	3
Logfile	Windows PowerShell
Message	Provider "FileSystem" is Started. Details: ProviderName=FileSystem NewProviderState=Started SequenceNumber=7 HostName=ConsoleHost

	HostVersion=5.1.22621.169 HostId=cd635701-06a7-4607-8626-f422cd2a174b HostApplication=C:\WINDOWS\System32\WindowsPowerShell\v1.0\powershell.exe EngineVersion= RunspaceId= PipelineId= CommandName= CommandType= ScriptName= CommandPath= CommandLine=
RecordNumber	4256
SourceName	PowerShell
TimeGenerated	2022-10-05T02:58:07.3984Z
TimeWritten	2022-10-05T02:58:07.3984Z
Type	Information
User	N/A

Log Number	**33**
Category	12548
CategoryString	Special Logon
ComputerName	sandbox
EventCode	4672
EventIdentifier	4672
EventType	4
Logfile	Security
Message	Special privileges assigned to new logon. Subject: Security ID: S-1-5-18 Account Name: SYSTEM Account Domain: NT AUTHORITY Logon ID: 0x3E7 Privileges: SeAssignPrimaryTokenPrivilege SeTcbPrivilege SeSecurityPrivilege

	SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege
RecordNumber	17319
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T15:57:05.586789Z
TimeWritten	2022-10-05T15:57:05.586789Z
Type	Audit Success
User	N/A

Log Number	**34**
Category	12292
CategoryString	Other System Events
ComputerName	sandbox
EventCode	5058
EventIdentifier	5058
EventType	4
Logfile	Security
Message	Key file operation. Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox Logon ID: 0xC7B7D6A Process Information: Process ID: 14592 Process Creation Time: ?2022?-?10?-?05T11:08:37.273091600Z

	Cryptographic Parameters: Provider Name: Microsoft Software Key Storage Provider Algorithm Name: ECDSA_P256 Key Name: Microsoft-Edge-TB-test-key Key Type: User key. Key File Operation Information: File Path: C:\Users\guru\AppData\Roaming\Microsoft\Crypto\Keys\53caafca80232173a709de019a f770-4829-8e8b-55f975dac4a9 Operation: Write persisted key to file. Return Code: 0x0
RecordNumber	17333
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T16:38:40.785665Z
TimeWritten	2022-10-05T16:38:40.785665Z
Type	Audit Success
User	N/A

Log Number	**35**
Category	12290
CategoryString	System Integrity
ComputerName	sandbox
EventCode	5061
EventIdentifier	5061
EventType	4
Logfile	Security
Message	Cryptographic operation. Subject: Security ID: S-1-5-21-3249831223-3918070856-2126610958-1001 Account Name: guru Account Domain: sandbox Logon ID: 0xC7B7D6A Cryptographic Parameters:

	Provider Name: Microsoft Software Key Storage Provider Algorithm Name: ECDSA_P256 Key Name: Microsoft-Edge-TB-test-key Key Type: User key. Cryptographic Operation: Operation: Create Key. Return Code: 0x0
RecordNumber	17334
SourceName	Microsoft-Windows-Security-Auditing
TimeGenerated	2022-10-05T16:38:40.786997Z
TimeWritten	2022-10-05T16:38:40.786997Z
Type	Audit Success
User	N/A

Log Number	**36**
Category	0
CategoryString	N/A
ComputerName	sandbox
EventCode	16
EventIdentifier	16
EventType	3
Logfile	System
Message	The access history in hive \??\C:\Users\guru\AppData\Local\Packages\Microsoft.ScreenSketch_8wekyb3d8bbwe\S was cleared updating 2 keys and creating 1 modified pages.
RecordNumber	7206
SourceName	Microsoft-Windows-Kernel-General
TimeGenerated	2022-10-05T16:39:07.931254Z
TimeWritten	2022-10-05T16:39:07.931254Z
Type	Information
User	NT AUTHORITY\SYSTEM