Time	Event

2024-04-30T12:47:55+0530	04/30/2024 12:47:55 PM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18820
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is
	not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments.
	This may be the expected behavior for the current provider in the current operating environment as well.

2024-04-30T12:40:52+0530	04/30/2024 12:40:52 PM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18819
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	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 DESKTOP-LU7VRCG\admin SID (S-1-5-21-1102696979-4129790392-413580853-1001) 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.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67747
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67746
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67745
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67744
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67743
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67742
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67741
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67740
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67739
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67738
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67737
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67736
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67735 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:40:49+0530	04/30/2024 12:40:49 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67734 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:30:51+0530	04/30/2024 12:30:51 PM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18818
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments. This may be the expected behavior for the current provider in the current operating environment as well.

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67733
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67732
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67731
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67730
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67729
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67728
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:27:23+0530	04/30/2024 12:27:23 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67727 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                       Event
2024-04-30T12:27:23+0530   04/30/2024 12:27:23 PM
                           LogName=Security
                           EventCode=4624
                           EventType=0
                           ComputerName=DESKTOP-LU7VRCG
                           SourceName=Microsoft Windows security auditing.
                           Type=Information
                           RecordNumber=67726
                           Keywords=Audit Success
                           TaskCategory=Logon
                           OpCode=Info
                           Message=An account was successfully logged on.

                           Subject:
                           Security ID:S-1-5-18
                           Account Name:DESKTOP-LU7VRCG$
                           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:0x404
                           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.
```

Time	Event
2024-04-30T12:22:45+0530	04/30/2024 12:22:45 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67725 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:22:45+0530	04/30/2024 12:22:45 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67724 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T12:22:44+0530	04/30/2024 12:22:44 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67723 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe
2024-04-30T12:22:36+0530	04/30/2024 12:22:36 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67722 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:22:36+0530	04/30/2024 12:22:36 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67721 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:19:23+0530	04/30/2024 12:19:23 PM
	LogName=System
	EventCode=114
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18817
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=RemUrl
	Message=Removed URL (http://*:2869/upnp/eventing/) from URL group (0xFC0000042000000F). Process Id 0x1BD4 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

2024-04-30T12:19:23+0530	04/30/2024 12:19:23 PM
	LogName=System
	EventCode=7040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18816
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.

2024-04-30T12:17:03+0530	04/30/2024 12:17:03 PM
	LogName=System
	EventCode=113
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18815
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=AddUrl
	Message=Attempted to add URL (http://*:2869/upnp/eventing/) to URL group (0xFC0000042000000F). Status: 0x0. Process Id 0x1BD4 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

2024-04-30T12:17:03+0530	04/30/2024 12:17:03 PM
	LogName=System
	EventCode=114
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18814
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=RemUrl
	Message=Removed URL (http://*:2869/upnp/eventing/) from URL group (0xFD00000120000003). Process Id 0x1BD4 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

Time	Event

2024-04-30T12:16:59+0530	04/30/2024 12:16:59 PM
	LogName=System
	EventCode=113
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18813
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=AddUrl
	Message=Attempted to add URL (http://*:2869/upnp/eventing/) to URL group (0xFD00000120000003). Status: 0x0. Process Id 0x1BD4 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

2024-04-30T12:16:59+0530	04/30/2024 12:16:59 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67720 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:16:59+0530	04/30/2024 12:16:59 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67719 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T12:16:59+0530	04/30/2024 12:16:59 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67718 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-551 Group Name:Backup Operators Group Domain:Builtin Process Information: Process ID:0xaac Process Name:C:\Windows\System32\svchost.exe
2024-04-30T12:16:59+0530	04/30/2024 12:16:59 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67717 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0xaac Process Name:C:\Windows\System32\svchost.exe

2024-04-30T12:16:54+0530	04/30/2024 12:16:54 PM
	LogName=System
	EventCode=7040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18812
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.

Time	Event
2024-04-30T12:16:54+0530	04/30/2024 12:16:54 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67716 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:16:54+0530	04/30/2024 12:16:54 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67715 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:13:47+0530	04/30/2024 12:13:47 PM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18811
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments. This may be the expected behavior for the current provider in the current operating environment as well.

2024-04-30T12:11:56+0530	04/30/2024 12:11:56 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67714 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:11:56+0530	04/30/2024 12:11:56 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67713 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67712
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67711
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67710
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67709
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67708
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67707
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67706 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:11:06+0530	04/30/2024 12:11:06 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67705 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:10:57+0530	04/30/2024 12:10:57 PM
	LogName=Application
	EventCode=1042
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5659
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Ending a Windows Installer transaction: {8198477F-198B-49C1-97C1-C745C376BE4F}. Client Process Id: 14276.

2024-04-30T12:10:56+0530	04/30/2024 12:10:56 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67704 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

2024-04-30T12:10:56+0530	04/30/2024 12:10:56 PM
	LogName=Application
	EventCode=1035
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5658
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Windows Installer reconfigured the product. Product Name: Splunk Enterprise. Product Version: 9.2.1.0. Product Language: 1033. Manufacturer: Splunk, Inc.. Reconfiguration success or error status: 0.

2024-04-30T12:10:56+0530	04/30/2024 12:10:56 PM
	LogName=Application
	EventCode=11728
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5657
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Product: Splunk Enterprise -- Configuration completed successfully.

Time	Event
2024-04-30T12:10:46+0530	04/30/2024 12:10:46 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67703 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:46+0530	04/30/2024 12:10:46 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67702 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:46+0530	04/30/2024 12:10:46 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67701 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:46+0530	04/30/2024 12:10:46 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67700 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67699 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67698 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67697 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67696 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67695 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67694 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67693 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67692 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67691 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67690 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67689 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67688 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67687 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:44+0530	04/30/2024 12:10:44 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67686 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:43+0530	04/30/2024 12:10:43 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67685 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:43+0530	04/30/2024 12:10:43 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67684 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:43+0530	04/30/2024 12:10:43 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67683 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:43+0530	04/30/2024 12:10:43 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67682 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67681 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67680 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67679 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67678 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67677 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67676 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67675 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67674 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67673 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67672 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67671 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:42+0530	04/30/2024 12:10:42 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67670 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:41+0530	04/30/2024 12:10:41 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67669 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:41+0530	04/30/2024 12:10:41 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67668 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1624 Process Creation Time:2024-04-30T06:40:39.709731600Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:10:01+0530	04/30/2024 12:10:01 PM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67667 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T12:10:01+0530	04/30/2024 12:10:01 PM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67666 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:11648 Process Creation Time:2024-04-30T06:39:57.423603300Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T12:09:48+0530	04/30/2024 12:09:48 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67665 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

2024-04-30T12:09:47+0530	04/30/2024 12:09:47 PM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18810
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: SplunkMonitorNoHandle
	Service File Name: system32\DRIVERS\SplunkMonitorNoHandleDrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

2024-04-30T12:09:47+0530	04/30/2024 12:09:47 PM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18809
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: splknetdrv
	Service File Name: \SystemRoot\system32\DRIVERS\splknetdrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

Time	Event
2024-04-30T12:09:47+0530	04/30/2024 12:09:47 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67664 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

2024-04-30T12:09:46+0530	04/30/2024 12:09:46 PM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18808
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: Splunk Trace Kernel Mode Driver
	Service File Name: \SystemRoot\system32\DRIVERS\splunkdrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

2024-04-30T12:09:46+0530	04/30/2024 12:09:46 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67663 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T12:09:20+0530	04/30/2024 12:09:20 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67662 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe
2024-04-30T12:09:20+0530	04/30/2024 12:09:20 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67661 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T12:09:19+0530	04/30/2024 12:09:19 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67660 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe
2024-04-30T12:08:56+0530	04/30/2024 12:08:56 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67659 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:08:56+0530	04/30/2024 12:08:56 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67658 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T12:07:09+0530	04/30/2024 12:07:09 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67657 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:07:09+0530	04/30/2024 12:07:09 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67656 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:04:53+0530	04/30/2024 12:04:53 PM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18807
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T12:04:18+0530	04/30/2024 12:04:18 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18806
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:04:18+0530	04/30/2024 12:04:18 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18805
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:04:18+0530	04/30/2024 12:04:18 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18804
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:03:53+0530	04/30/2024 12:03:53 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18803
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:03:53+0530	04/30/2024 12:03:53 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18802
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

Time	Event

2024-04-30T12:03:53+0530	04/30/2024 12:03:53 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18801
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:03:32+0530	04/30/2024 12:03:32 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67655 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:03:32+0530	04/30/2024 12:03:32 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67654 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:03:32+0530	04/30/2024 12:03:32 PM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5656
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Beginning a Windows Installer transaction: {8198477F-198B-49C1-97C1-C745C376BE4F}. Client Process Id: 14276.

2024-04-30T12:03:27+0530	04/30/2024 12:03:27 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18800
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:03:27+0530	04/30/2024 12:03:27 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18799
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:03:27+0530	04/30/2024 12:03:27 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18798
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:02:50+0530	04/30/2024 12:02:50 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18797
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:02:50+0530	04/30/2024 12:02:50 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18796
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

Time	Event

2024-04-30T12:02:50+0530	04/30/2024 12:02:50 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18795
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:02:41+0530	04/30/2024 12:02:41 PM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18794
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{C2F03A33-21F5-47FA-B4BB-156362A2F239}
	 and APPID
	{316CDED5-E4AE-4B15-9113-7055D84DCC97}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T12:02:41+0530	04/30/2024 12:02:41 PM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18793
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T12:02:41+0530	04/30/2024 12:02:41 PM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18792
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{C2F03A33-21F5-47FA-B4BB-156362A2F239}
	 and APPID
	{316CDED5-E4AE-4B15-9113-7055D84DCC97}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

Time	Event

2024-04-30T12:02:41+0530	04/30/2024 12:02:41 PM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18791
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T12:02:41+0530	04/30/2024 12:02:41 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67653 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T12:02:41+0530  04/30/2024 12:02:41 PM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67652
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event

2024-04-30T12:02:09+0530	04/30/2024 12:02:09 PM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67651
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-80-3589385106-520469509-3569633472-84460881-2732306008
	Account Name:ksnproxy
	Account Domain:NT SERVICE
	Logon ID:0x296E62
	
	Logon Type:5
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T12:01:56+0530	04/30/2024 12:01:56 PM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67650 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T12:01:56+0530	04/30/2024 12:01:56 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67649 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T12:01:35+0530	04/30/2024 12:01:35 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18790
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:01:35+0530	04/30/2024 12:01:35 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18789
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:01:35+0530	04/30/2024 12:01:35 PM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18788
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T12:01:16+0530	04/30/2024 12:01:16 PM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67648 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T12:00:01+0530	04/30/2024 12:00:01 PM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67647 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0x688 Process Name:C:\Windows\System32\svchost.exe

2024-04-30T12:00:01+0530	04/30/2024 12:00:01 PM
	LogName=Security
	EventCode=4672
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67646
	Keywords=Audit Success
	TaskCategory=Special Logon
	OpCode=Info
	Message=Special privileges assigned to new logon.
	
	Subject:
	Security ID:S-1-5-80-3589385106-520469509-3569633472-84460881-2732306008
	Account Name:ksnproxy
	Account Domain:NT SERVICE
	Logon ID:0x296E62
	
	Privileges:SeImpersonatePrivilege

Time	Event
2024-04-30T12:00:01+0530	04/30/2024 12:00:01 PM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67645 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:5 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:Yes Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-80-3589385106-520469509-3569633472-84460881-2732306008 Account Name:ksnproxy Account Domain:NT SERVICE Logon ID:0x296E62 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x404 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.

Time	Event
2024-04-30T12:00:01+0530	04/30/2024 12:00:01 PM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67644 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:ksnproxy Account Domain:NT SERVICE Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x404 Process Name:C:\Windows\System32\services.exe Network Information: Network Address:- Port:- 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.

2024-04-30T12:00:00+0530	04/30/2024 12:00:00 PM
	LogName=System
	EventCode=6013
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=EventLog
	Type=Information
	RecordNumber=18787
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The system uptime is 516 seconds.

2024-04-30T11:59:47+0530	04/30/2024 11:59:47 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18786
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

Time	Event

2024-04-30T11:59:47+0530	04/30/2024 11:59:47 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18785
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:59:46+0530	04/30/2024 11:59:46 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18784
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:59:31+0530	04/30/2024 11:59:31 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67643 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T11:59:28+0530	04/30/2024 11:59:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67642 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe
2024-04-30T11:59:01+0530	04/30/2024 11:59:01 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67641 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:59:01+0530	04/30/2024 11:59:01 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67640 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:58:55+0530	04/30/2024 11:58:55 AM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18783
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T11:58:55+0530	04/30/2024 11:58:55 AM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18782
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T11:58:55+0530	04/30/2024 11:58:55 AM
	LogName=System
	EventCode=7003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18781
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7003 - Roam Complete

2024-04-30T11:58:49+0530	04/30/2024 11:58:49 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67639 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T11:58:46+0530	04/30/2024 11:58:46 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5655 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket 55769560, type 5 Event Name: ShellBrowserCancel Response: Not available Cab Id: 0 Problem signature: P1: {F3364BA0-65B9-11CE-A9BA-00AA004AE837} P2: Local P3: P4: P5: P6: P7: P8: P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.24f248ae-dc0e-47b0-b6dd-68a44a241215.tmp.WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cab_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995\WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e19af637-088b-40c4-b4a6-49dc4f07336f.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cab_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995\WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.a298c6ed-dc86-41f6-b539-1b8c308db93b.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.63ce4331-c5ff-423d-b785-2f05d6f242ae.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.b17d0162-8fec-49b2-adba-245545a67951.tmp.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.054e6139-91b1-410a-841d-6225b23d5d11.tmp.xml These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995 Analysis symbol: Rechecking for solution: 0 Report Id: cfb6270b-cfb9-4e42-8e51-a8c6a15bf995 Report Status: 268435456 Hashed bucket: 43f5d71c104cc5b12195cd010f50564d Cab Guid: 0

2024-04-30T11:58:42+0530	04/30/2024 11:58:42 AM
	LogName=System
	EventCode=7040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18780
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The start type of the Background Intelligent Transfer Service service was changed from auto start to demand start.

Time	Event

2024-04-30T11:58:42+0530	04/30/2024 11:58:42 AM
	LogName=System
	EventCode=10010
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Error
	RecordNumber=18779
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The server {8CFC164F-4BE5-4FDD-94E9-E2AF73ED4A19} did not register with DCOM within the required timeout.

2024-04-30T11:58:33+0530	04/30/2024 11:58:33 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-21-1102696979-4129790392-413580853-1001 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5654 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: ShellBrowserCancel Response: Not available Cab Id: 0 Problem signature: P1: {F3364BA0-65B9-11CE-A9BA-00AA004AE837} P2: Local P3: P4: P5: P6: P7: P8: P9: P10: Attached files: These files may be available here: NULL Analysis symbol: Rechecking for solution: 0 Report Id: cfb6270b-cfb9-4e42-8e51-a8c6a15bf995 Report Status: 262148 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:58:33+0530	04/30/2024 11:58:33 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-21-1102696979-4129790392-413580853-1001 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5653 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: ShellBrowserCancel Response: Not available Cab Id: 0 Problem signature: P1: {F3364BA0-65B9-11CE-A9BA-00AA004AE837} P2: Local P3: P4: P5: P6: P7: P8: P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.24f248ae-dc0e-47b0-b6dd-68a44a241215.tmp.WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cab_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995\WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e19af637-088b-40c4-b4a6-49dc4f07336f.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cab_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995\WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.a298c6ed-dc86-41f6-b539-1b8c308db93b.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.63ce4331-c5ff-423d-b785-2f05d6f242ae.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.b17d0162-8fec-49b2-adba-245545a67951.tmp.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.054e6139-91b1-410a-841d-6225b23d5d11.tmp.xml These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_{F3364BA0-65B9-1_03f722b1c3a9f7342b324b90c4342939636d4_00000000_cab_cfb6270b-cfb9-4e42-8e51-a8c6a15bf995 Analysis symbol: Rechecking for solution: 0 Report Id: cfb6270b-cfb9-4e42-8e51-a8c6a15bf995 Report Status: 4 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:58:14+0530	04/30/2024 11:58:14 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67638 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:58:14+0530	04/30/2024 11:58:14 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67637 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:57:50+0530	04/30/2024 11:57:50 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=224
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Network Agent 13.2.0.1511 has started.

2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18778
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{C2F03A33-21F5-47FA-B4BB-156362A2F239}
	 and APPID
	{316CDED5-E4AE-4B15-9113-7055D84DCC97}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18777
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18776
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The machine-default permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{C2F03A33-21F5-47FA-B4BB-156362A2F239}
	 and APPID
	{316CDED5-E4AE-4B15-9113-7055D84DCC97}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

Time	Event

2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18775
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67636 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:57:48+0530	04/30/2024 11:57:48 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67635 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:57:47+0530	04/30/2024 11:57:47 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=223
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Windows Update Agent is ready.

2024-04-30T11:57:46+0530	04/30/2024 11:57:46 AM
	LogName=System
	EventCode=113
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18774
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=AddUrl
	Message=Attempted to add URL (https://+:26770/) to URL group (0xFF00000720000005). Status: 0x0. Process Id 0x30C4 Executable path \Device\HarddiskVolume3\Program Files (x86)\eMudhra\emBridge\emBridge.exe, User S-1-5-21-1102696979-4129790392-413580853-1001

2024-04-30T11:57:46+0530	04/30/2024 11:57:46 AM
	LogName=System
	EventCode=111
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18773
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=CreateUrlGroup
	Message=Create URL group 0xFF00000720000005. Status 0x0. Process Id 0x30C4 Executable path \Device\HarddiskVolume3\Program Files (x86)\eMudhra\emBridge\emBridge.exe, User S-1-5-21-1102696979-4129790392-413580853-1001

2024-04-30T11:57:37+0530	04/30/2024 11:57:37 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67634
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Read Credential
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:57:37+0530	04/30/2024 11:57:37 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67633
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Read Credential
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:57:37+0530	04/30/2024 11:57:37 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67632
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Read Credential
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:57:37+0530	04/30/2024 11:57:37 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67631
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Read Credential
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:57:16+0530	04/30/2024 11:57:16 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18772
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	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 DESKTOP-LU7VRCG\admin SID (S-1-5-21-1102696979-4129790392-413580853-1001) from address
	LocalHost (Using LRPC) running in the application container Microsoft.SkypeApp_15.118.3205.0_x64__kzf8qxf38zg5c SID
	 (Unavailable). This security permission can be modified using the Component Services administrative tool.

2024-04-30T11:57:10+0530	04/30/2024 11:57:10 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67630 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:57:10+0530	04/30/2024 11:57:10 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67629 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:57:07+0530	04/30/2024 11:57:07 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=222
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Network Agent data backup completed successfully

2024-04-30T11:57:06+0530	04/30/2024 11:57:06 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=221
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Network Agent data backup.

2024-04-30T11:57:02+0530	04/30/2024 11:57:02 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67628 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe

2024-04-30T11:56:58+0530	04/30/2024 11:56:58 AM
	LogName=Application
	EventCode=903
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5652
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Software Protection service has stopped.

2024-04-30T11:56:58+0530	04/30/2024 11:56:58 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5651
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T06:26:58Z. Reason: RulesEngine.

Time	Event
2024-04-30T11:56:55+0530	04/30/2024 11:56:55 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5650 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket 2002510863698662189, type 5 Event Name: AppHangB1 Response: Not available Cab Id: 0 Problem signature: P1: explorer.exe P2: 10.0.22621.3527 P3: 00c8ba7a P4: 1054 P5: 33554432 P6: P7: P8: P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.185508be-8143-41f5-aec5-d584d9b7aa52.tmp.WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\ WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.69f50058-026f-4b20-83d6-050ce0e3511c.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\ WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.6a178c01-52ce-4842-9f21-99b9579de961.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.71b09bc8-7f77-4db5-9e46-fe87de971915.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.f1f9b3c0-3fc9-4897-b429-6e6498f05b73.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.bb8df6d4-903b-4901-88ed-5b5011191f54.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.a20c288d-8cef-4792-a9da-453b0675c5f1.tmp.xml \\?\C:\Users\admin\AppData\Local\Temp\WER.c93c276f-2b0a-4dcc-97bf-87c1f052ce6f.tmp.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\minidump.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\memory.hdmp These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_d468a11d-286a-41a3-bc42-bcb421f0b21c Analysis symbol: Rechecking for solution: 0 Report Id: e2b433a6-f5ca-49a7-88b1-8a492eacc534 Report Status: 268435456 Hashed bucket: 5e730c08569828873bca5905519e932d Cab Guid: 0

Time	Event

2024-04-30T11:56:52+0530	04/30/2024 11:56:52 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67627
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:52+0530	04/30/2024 11:56:52 AM
	LogName=Application
	EventCode=1002
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Application Hang
	Type=Error
	RecordNumber=5649
	Keywords=None
	TaskCategory=Hanging Events
	OpCode=Info
	Message=The program explorer.exe version 10.0.22621.3527 stopped interacting with Windows and was closed. To see if more information about the problem is available, check the problem history in the Security and Maintenance control panel.

Time	Event
2024-04-30T11:56:52+0530	04/30/2024 11:56:52 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-21-1102696979-4129790392-413580853-1001 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5648 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: AppHangB1 Response: Not available Cab Id: 0 Problem signature: P1: explorer.exe P2: 10.0.22621.3527 P3: 00c8ba7a P4: 1054 P5: 33554432 P6: P7: P8: P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.185508be-8143-41f5-aec5-d584d9b7aa52.tmp.WERInternalMetadata.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\ WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.69f50058-026f-4b20-83d6-050ce0e3511c.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\ WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.6a178c01-52ce-4842-9f21-99b9579de961.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.71b09bc8-7f77-4db5-9e46-fe87de971915.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.f1f9b3c0-3fc9-4897-b429-6e6498f05b73.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.bb8df6d4-903b-4901-88ed-5b5011191f54.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.a20c288d-8cef-4792-a9da-453b0675c5f1.tmp.xml \\?\C:\Users\admin\AppData\Local\Temp\WER.c93c276f-2b0a-4dcc-97bf-87c1f052ce6f.tmp.xml \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\minidump.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c\memory.hdmp These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppHang_explorer. exe_b1c815da8e87fba88f84c61e1c7457aaf9f96eb_ef3cf867_cab_d468a11d-286a-41a3-bc42-bcb421f0b21c Analysis symbol: Rechecking for solution: 0 Report Id: e2b433a6-f5ca-49a7-88b1-8a492eacc534 Report Status: 4 Hashed bucket: Cab Guid: 0

Time	Event

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67626
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67625
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67624
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67623
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67622
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67621
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67620 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67619 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:56:48+0530	04/30/2024 11:56:48 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67618
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x686C2
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:56:35+0530	04/30/2024 11:56:35 AM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18771
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: MpKsla5f046dc
	Service File Name: C:\ProgramData\Microsoft\Windows Defender\Definition Updates\{2A4C7F88-994F-43E2-94C6-39902986EA4A}\MpKslDrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

2024-04-30T11:56:35+0530	04/30/2024 11:56:35 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18770
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:56:30+0530	04/30/2024 11:56:30 AM
	LogName=Application
	EventCode=15
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=SecurityCenter
	Type=Information
	RecordNumber=5647
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Updated Windows Defender status successfully to SECURITY_PRODUCT_STATE_ON.

Time	Event

2024-04-30T11:56:28+0530	04/30/2024 11:56:28 AM
	LogName=Application
	EventCode=1
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=SecurityCenter
	Type=Information
	RecordNumber=5646
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The Windows Security Center Service has started.

2024-04-30T11:56:28+0530	04/30/2024 11:56:28 AM
	LogName=Application
	EventCode=902
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5645
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Software Protection service has started.
	10.0.22621.3527

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18769
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID
	Windows.SecurityCenter.WscDataProtection
	 and APPID
	Unavailable
	 to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) 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.

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18768
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID
	Windows.SecurityCenter.SecurityAppBroker
	 and APPID
	Unavailable
	 to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) 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.

Time	Event

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18767
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Launch permission for the COM Server application with CLSID
	Windows.SecurityCenter.WscBrokerManager
	and APPID
	Unavailable
	to the user NT AUTHORITY\SYSTEM SID (S-1-5-18) 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.

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18766
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is
	not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments.
	This may be the expected behavior for the current provider in the current operating environment as well.

Time	Event
2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM LogName=Application EventCode=1003 EventType=4 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft-Windows-Security-SPP Type=Information RecordNumber=5644 Keywords=Classic TaskCategory=None OpCode=None Message=The Software Protection service has completed licensing status check. Application Id=55c92734-d682-4d71-983e-d6ec3f16059f Licensing Status= 1: 040fa323-92b1-4baf-97a2-5b67feaefddb, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 2: 0724cb7d-3437-4cb7-93cb-830375d0079d, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 3: 0ad2ac98-7bb9-4201-8d92-312299201369, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 4: 1a9a717a-cf13-4ba5-83c3-0fe25fa868d5, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 5: 221a02da-e2a1-4b75-864c-0a4410a33fdf, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 6: 291ece0e-9c38-40ca-a9e1-32cc7ec19507, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 7: 2936d1d2-913a-4542-b54e-ce5a602a2a38, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 8: 2c293c26-a45a-4a2a-a350-c69a67097529, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 9: 2de67392-b7a7-462a-b1ca-108dd189f588, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 10: 2ffd8952-423e-4903-b993-72a1aa44cf82, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 11: 30a42c86-b7a0-4a34-8c90-ff177cb2acb7, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 12: 345a5db0-d94f-4e3b-a0c0-7c42f7bc3ebf, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 13: 3502365a-f88a-4ba4-822a-5769d3073b65, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 14: 377333b1-8b5d-48d6-9679-1225c872d37c, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 15: 3df374ef-d444-4494-a5a1-4b0d9fd0e203, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 16: 3f1afc82-f8ac-4f6c-8005-1d233e606eee, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 17: 49cd895b-53b2-4dc4-a5f7-b18aa019ad37, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 18: 4de7cb65-cdf1-4de9-8ae8-e3cce27b9f2c, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 19: 4f3da0d2-271d-4508-ae81-626b60809a38, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 20: 5d78c4e9-aeb3-4b40-8ac2-6a6005e0ad6d, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 21: 60b3ec1b-9545-4921-821f-311b129dd6f6, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 22: 613d217f-7f13-4268-9907-1662339531cd, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 23: 62f0c100-9c53-4e02-b886-a3528ddfe7f6, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 24: 6365275e-368d-46ca-a0ef-fc0404119333, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 25: 721f9237-9341-4453-a661-09e8baa6cca5, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 26: 73111121-5638-40f6-bc11-f1d7b0d64300, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 27: 7a802526-4c94-4bd1-ba14-835a1aca2120, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 28: 7cb546c0-c7d5-44d8-9a5c-69ecdd782b69, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 29: 82bbc092-bc50-4e16-8e18-b74fc486aec3, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 30: 8ab9bdd1-1f67-4997-82d9-8878520837d9, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 31: 8b351c9c-f398-4515-9900-09df49427262, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 32: 90da7373-1c51-430b-bf26-c97e9c5cdc31, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 33: 92fb8726-92a8-4ffc-94ce-f82e07444653, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 34: 95dca82f-385d-4d39-b85b-5c73fa285d6f, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 35: a48938aa-62fa-4966-9d44-9f04da3f72f2, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 36: b0773a15-df3a-4312-9ad2-83d69648e356, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 37: b4bfe195-541e-4e64-ad23-6177f19e395e, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 38: b68e61d2-68ca-4757-be45-0cc2f3e68eee, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 39: bd3762d7-270d-4760-8fb3-d829ca45278a, 1, 1 [(0 [0x00000000, 1, 0], [(?)(1 0x00000000)(?)(2 0x00000000 0 0 msft:rm/algorithm/hwid/4.0 0x00000000 0)(?)(?)(10 0x00000000 msft:rm/algorithm/flags/1. 0)(?)])(1)(2)(3)] 40: c86d5194-4840-4dae-9c1c-0301003a5ab0, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 41: ca7df2e3-5ea0-47b8-9ac1-b1be4d8edd69, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 42: d552befb-48cc-4327-8f39-47d2d94f987c, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 43: d6eadb3b-5ca8-4a6b-986e-35b550756111, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 44: df96023b-dcd9-4be2-afa0-c6c871159ebe, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 45: e0c42288-980c-4788-a014-c080d2e1926e, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 46: e4db50ea-bda1-4566-b047-0ca50abc6f07, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 47: e558417a-5123-4f6f-91e7-385c1c7ca9d4, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 48: e7a950a2-e548-4f10-bf16-02ec848e0643, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 49: eb6d346f-1c60-4643-b960-40ec31596c45, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 50: ec868e65-fadf-4759-b23e-93fe37f2cc29, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 51: ef51e000-2659-4f25-8345-3de70a9cf4c4, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 52: f7af7d09-40e4-419c-a49b-eae366689ebd, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 53: fa755fe6-6739-40b9-8d84-6d0ea3b6d1ab, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)] 54: fe74f55b-0338-41d6-b267-4a201abe7285, 1, 0 [(0 [0xC004F014, 0, 0], [(?)(?)(?)(?)(?)(?)(?)(?)])(1)(2)(3)]

Time	Event
2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM LogName=Application EventCode=1066 EventType=4 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft-Windows-Security-SPP Type=Information RecordNumber=5643 Keywords=Classic TaskCategory=None OpCode=None Message=Initialization status for service objects. C:\WINDOWS\system32\sppwinob.dll, msft:spp/windowsfunctionality/agent/7.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:rm/algorithm/inherited/1.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:rm/algorithm/phone/1.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:rm/algorithm/pkey/detect, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:spp/ActionScheduler/1.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:spp/TaskScheduler/1.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:spp/statecollector/pkey, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:spp/volume/services/kms/1.0, 0x00000000, 0x00000000 C:\WINDOWS\system32\sppobjs.dll, msft:spp/volume/services/kms/activationinfo/1.0, 0x00000000, 0x00000000

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5642
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

2024-04-30T11:56:27+0530	04/30/2024 11:56:27 AM
	LogName=Application
	EventCode=900
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5641
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Software Protection service is starting.
	Parameters:<explicit>

2024-04-30T11:56:26+0530	04/30/2024 11:56:26 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67617 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-551 Group Name:Backup Operators Group Domain:Builtin Process Information: Process ID:0x296c Process Name:C:\Windows\System32\svchost.exe

Time	Event
2024-04-30T11:56:26+0530	04/30/2024 11:56:26 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67616 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0x296c Process Name:C:\Windows\System32\svchost.exe
2024-04-30T11:56:24+0530	04/30/2024 11:56:24 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67615 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:56:24+0530	04/30/2024 11:56:24 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67614 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:56:24+0530	04/30/2024 11:56:24 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67613 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                       Event
2024-04-30T11:56:24+0530   04/30/2024 11:56:24 AM
                           LogName=Security
                           EventCode=4624
                           EventType=0
                           ComputerName=DESKTOP-LU7VRCG
                           SourceName=Microsoft Windows security auditing.
                           Type=Information
                           RecordNumber=67612
                           Keywords=Audit Success
                           TaskCategory=Logon
                           OpCode=Info
                           Message=An account was successfully logged on.

                           Subject:
                           Security ID:S-1-5-18
                           Account Name:DESKTOP-LU7VRCG$
                           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:0x404
                           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.
```

Time	Event

2024-04-30T11:56:24+0530	04/30/2024 11:56:24 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=gupdate
	Type=Information
	RecordNumber=5640
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:56:24+0530	04/30/2024 11:56:24 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=edgeupdate
	Type=Information
	RecordNumber=5639
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service stopped.

2024-04-30T11:56:22+0530	04/30/2024 11:56:22 AM
	LogName=System
	EventCode=7040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18765
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The start type of the Background Intelligent Transfer Service service was changed from demand start to auto start.

2024-04-30T11:56:22+0530	04/30/2024 11:56:22 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67611 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:56:22+0530	04/30/2024 11:56:22 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67610 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:56:22+0530	04/30/2024 11:56:22 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=AESMService
	Type=Information
	RecordNumber=5638
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=AESMService: Service started/resumed

2024-04-30T11:55:58+0530	04/30/2024 11:55:58 AM
	LogName=Application
	EventCode=1003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Search
	Type=Information
	RecordNumber=5637
	Keywords=Classic
	TaskCategory=Search service
	OpCode=NOTE: This dummy error message is necessary to force MC to output the above defines inside the FACILITY_WINDOWS guard instead of leaving it empty.
	Message=The Windows Search Service started.

2024-04-30T11:55:57+0530	04/30/2024 11:55:57 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67609 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-551 Group Name:Backup Operators Group Domain:Builtin Process Information: Process ID:0xe44 Process Name:C:\Windows\System32\SearchIndexer.exe

Time	Event
2024-04-30T11:55:57+0530	04/30/2024 11:55:57 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67608 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0xe44 Process Name:C:\Windows\System32\SearchIndexer.exe
2024-04-30T11:55:55+0530	04/30/2024 11:55:55 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67607 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:55:55+0530	04/30/2024 11:55:55 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67606 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:55:49+0530	04/30/2024 11:55:49 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18764
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:55:49+0530	04/30/2024 11:55:49 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18763
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:55:48+0530	04/30/2024 11:55:48 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18762
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:55:42+0530	04/30/2024 11:55:42 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67605 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:55:42+0530	04/30/2024 11:55:42 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67604 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:55:40+0530	04/30/2024 11:55:40 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67603 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:55:40+0530  04/30/2024 11:55:40 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67602
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:55:39+0530	04/30/2024 11:55:39 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67601 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:55:39+0530  04/30/2024 11:55:39 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67600
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:55:36+0530	04/30/2024 11:55:36 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67599 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:55:36+0530	04/30/2024 11:55:36 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67598 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:54:58+0530	04/30/2024 11:54:58 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67597 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:54:58+0530	04/30/2024 11:54:58 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67596 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:54:34+0530	04/30/2024 11:54:34 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67595 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1580 Process Name:C:\Windows\explorer.exe
2024-04-30T11:54:27+0530	04/30/2024 11:54:27 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67594 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:54:27+0530  04/30/2024 11:54:27 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67593
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:54:18+0530	04/30/2024 11:54:18 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67592 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:54:18+0530	04/30/2024 11:54:18 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67591 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:54:16+0530	04/30/2024 11:54:16 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67590 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:54:16+0530	04/30/2024 11:54:16 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67589 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:53:34+0530	04/30/2024 11:53:34 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67588 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:53:34+0530	04/30/2024 11:53:34 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67587 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67586
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0xC319E
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67585 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67584 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67583
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0xC31C6
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67582 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0xC319E Privileges:SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

```
Time                      Event
2024-04-30T11:53:32+0530  04/30/2024 11:53:32 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67581
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Logon Information:
                          Logon Type:2
                          Restricted Admin Mode:-
                          Remote Credential Guard:-
                          Virtual Account:No
                          Elevated Token:No

                          Impersonation Level:Impersonation

                          New Logon:
                          Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
                          Account Name:admin
                          Account Domain:DESKTOP-LU7VRCG
                          Logon ID:0xC31C6
                          Linked Logon ID:0xC319E
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x9fc
                          Process Name:C:\Windows\System32\svchost.exe

                          Network Information:
                          Workstation Name:DESKTOP-LU7VRCG
                          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 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.
```

Time	Event
2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67580 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0xC319E Linked Logon ID:0xC31C6 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x9fc Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:DESKTOP-LU7VRCG 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 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.

Time	Event
2024-04-30T11:53:32+0530	04/30/2024 11:53:32 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67579 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x9fc Process Name:C:\Windows\System32\svchost.exe Network Information: Network Address:127.0.0.1 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.

2024-04-30T11:53:31+0530	04/30/2024 11:53:31 AM
	LogName=System
	EventCode=113
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18761
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=AddUrl
	Message=Attempted to add URL (https://+:26769/) to URL group (0xFE00000320000001). Status: 0x0.
	Process Id 0x1234 Executable path \Device\HarddiskVolume3\Program Files (x86)\eMudhra\emBridge\emBridge.exe, User S-1-5-18

2024-04-30T11:53:31+0530	04/30/2024 11:53:31 AM
	LogName=System
	EventCode=111
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18760
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=CreateUrlGroup
	Message=Create URL group 0xFE00000320000001. Status 0x0. Process Id 0x1234 Executable path \Device\HarddiskVolume3\Program Files (x86)\eMudhra\emBridge\emBridge.exe, User S-1-5-18

Time	Event
2024-04-30T11:53:26+0530	04/30/2024 11:53:26 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67578 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x1340 Process Name:C:\Windows\explorer.exe

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM
	LogName=System
	EventCode=15301
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-HttpEvent
	Type=Warning
	RecordNumber=18759
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=SSL Certificate Settings created by an admin process for endpoint : 0.0.0.0:26770 .

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM
	LogName=System
	EventCode=120
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18758
	Keywords=Flagged on all HTTP events handling SSL interactions
	TaskCategory=HTTP SSL Trace Task
	OpCode=SslCertSettingsCreated
	Message=SSL Certificate Settings created by an admin process for endpoint : 0.0.0.0:26770. Status 0x0. Process Id 0x1A84 Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM
	LogName=System
	EventCode=15300
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-HttpEvent
	Type=Warning
	RecordNumber=18757
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=SSL Certificate Settings deleted for endpoint : 0.0.0.0:26770 .

Time	Event

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM
	LogName=System
	EventCode=119
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18756
	Keywords=Flagged on all HTTP events handling SSL interactions
	TaskCategory=HTTP SSL Trace Task
	OpCode=SslCertSettingsDeleted
	Message=SSL Certificate Settings deleted for endpoint : 0.0.0.0:26770. Status 0x0. Process Id 0xC48 Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18755
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:26770/. Status 0xC0000035. Process Id 0x1708 Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:24+0530	04/30/2024 11:53:24 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67577 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{6527011C-6439-49F5-9C53-5930EB9A70B4} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

2024-04-30T11:53:22+0530	04/30/2024 11:53:22 AM
	LogName=System
	EventCode=15301
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-HttpEvent
	Type=Warning
	RecordNumber=18754
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=SSL Certificate Settings created by an admin process for endpoint : 0.0.0.0:26769 .

Time	Event

2024-04-30T11:53:22+0530	04/30/2024 11:53:22 AM
	LogName=System
	EventCode=120
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18753
	Keywords=Flagged on all HTTP events handling SSL interactions
	TaskCategory=HTTP SSL Trace Task
	OpCode=SslCertSettingsCreated
	Message=SSL Certificate Settings created by an admin process for endpoint : 0.0.0.0:26769. Status 0x0. Process Id 0x12FC Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:22+0530	04/30/2024 11:53:22 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67576 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{6527011C-6439-49F5-9C53-5930EB9A70B4} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

2024-04-30T11:53:21+0530	04/30/2024 11:53:21 AM
	LogName=System
	EventCode=119
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18752
	Keywords=Flagged on all HTTP events handling SSL interactions
	TaskCategory=HTTP SSL Trace Task
	OpCode=SslCertSettingsDeleted
	Message=SSL Certificate Settings deleted for endpoint : 0.0.0.0:26769. Status 0x0. Process Id 0x1DBC Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:21+0530	04/30/2024 11:53:21 AM
	LogName=System
	EventCode=15300
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-HttpEvent
	Type=Warning
	RecordNumber=18751
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=SSL Certificate Settings deleted for endpoint : 0.0.0.0:26769 .

Time	Event

2024-04-30T11:53:19+0530	04/30/2024 11:53:19 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18750
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:26769/. Status 0xC0000035. Process Id 0x1878 Executable path \Device\HarddiskVolume3\Windows\SysWOW64\netsh.exe, User S-1-5-18

2024-04-30T11:53:15+0530	04/30/2024 11:53:15 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67575 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:53:15+0530	04/30/2024 11:53:15 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67574 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:53:14+0530	04/30/2024 11:53:14 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67573 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x664 Process Name:C:\Windows\System32\LogonUI.exe

2024-04-30T11:53:09+0530	04/30/2024 11:53:09 AM
	LogName=System
	EventCode=1025
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-TPM-WMI
	Type=Information
	RecordNumber=18749
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The TPM was successfully provisioned and is now ready for use.

2024-04-30T11:53:08+0530	04/30/2024 11:53:08 AM
	LogName=System
	EventCode=1282
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-TPM-WMI
	Type=Information
	RecordNumber=18748
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The TBS device identifier has been generated.

Time	Event
2024-04-30T11:53:07+0530	04/30/2024 11:53:07 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67572 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:53:07+0530	04/30/2024 11:53:07 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67571 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:58+0530	04/30/2024 11:52:58 AM
	LogName=System
	EventCode=18
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18747
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=This event triggers the Trusted Platform Module (TPM) provisioning/status check to run.

2024-04-30T11:52:58+0530	04/30/2024 11:52:58 AM
	LogName=System
	EventCode=7026
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18746
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The following boot-start or system-start driver(s) did not load:
	dam
	WinSetupMon

2024-04-30T11:52:58+0530	04/30/2024 11:52:58 AM
	LogName=System
	EventCode=7000
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Error
	RecordNumber=18745
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The Splunkd service failed to start due to the following error:
	The service did not respond to the start or control request in a timely fashion.

2024-04-30T11:52:58+0530	04/30/2024 11:52:58 AM
	LogName=System
	EventCode=7009
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Error
	RecordNumber=18744
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A timeout was reached (45000 milliseconds) while waiting for the Splunkd service to connect.

2024-04-30T11:52:52+0530	04/30/2024 11:52:52 AM
	LogName=System
	EventCode=1014
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-20
	SidType=0
	SourceName=Microsoft-Windows-DNS Client Events
	Type=Warning
	RecordNumber=18743
	Keywords=None
	TaskCategory=1014
	OpCode=Info
	Message=Name resolution for the name resources.emudhra.com timed out after none of the configured DNS servers responded. Client PID 4660.

Time	Event

2024-04-30T11:52:48+0530	04/30/2024 11:52:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18742
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T11:52:48+0530	04/30/2024 11:52:48 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18741
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The application-specific permission settings do not grant Local Activation permission for the COM Server application with CLSID
	{6B3B8D23-FA8D-40B9-8DBD-B950333E2C52}
	 and APPID
	{4839DDB7-58C2-48F5-8283-E1D1807D0D7D}
	 to the user NT AUTHORITY\LOCAL SERVICE SID (S-1-5-19) 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.

2024-04-30T11:52:47+0530	04/30/2024 11:52:47 AM LogName=Security EventCode=5059 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67570 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key migration operation. Subject: Security ID:S-1-5-19 Account Name:LOCAL SERVICE Account Domain:NT AUTHORITY Logon ID:0x3E5 Process Information: Process ID:8784 Process Creation Time:2024-04-30T06:22:45.412718900Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:ECDSA_P256 Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Additional Information: Operation:Export of persistent cryptographic key. Return Code:0x0

Time	Event
2024-04-30T11:52:47+0530	04/30/2024 11:52:47 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67569 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-19 Account Name:LOCAL SERVICE Account Domain:NT AUTHORITY Logon ID:0x3E5 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:ECDSA_P256 Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:52:47+0530	04/30/2024 11:52:47 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67568 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-19 Account Name:LOCAL SERVICE Account Domain:NT AUTHORITY Logon ID:0x3E5 Process Information: Process ID:8784 Process Creation Time:2024-04-30T06:22:45.412718900Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Key File Operation Information: File Path: C:\WINDOWS\ServiceProfiles\LocalService\AppData\Roaming\Microsoft\Crypto\Keys\ de7cf8a7901d2ad13e5c67c29e5d1662_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

2024-04-30T11:52:47+0530	04/30/2024 11:52:47 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5636
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service started successfully.

Time	Event
2024-04-30T11:52:45+0530	04/30/2024 11:52:45 AM LogName=Security EventCode=5059 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67567 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key migration operation. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 Process Information: Process ID:5996 Process Creation Time:2024-04-30T06:22:39.511146700Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:ECDSA_P256 Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Additional Information: Operation:Export of persistent cryptographic key. Return Code:0x0
2024-04-30T11:52:45+0530	04/30/2024 11:52:45 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67566 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:ECDSA_P256 Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:52:45+0530	04/30/2024 11:52:45 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67565 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 Process Information: Process ID:5996 Process Creation Time:2024-04-30T06:22:39.511146700Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:Microsoft Connected Devices Platform device certificate Key Type:User key. Key File Operation Information: File Path: C:\Users\admin\AppData\Roaming\Microsoft\Crypto\Keys\de7cf8a7901d2ad13e5c67c29e5d1662_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

2024-04-30T11:52:40+0530	04/30/2024 11:52:40 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igfxCUIService2.0.0.0
	Type=Information
	RecordNumber=5635
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:52:40+0530	04/30/2024 11:52:40 AM
	LogName=Application
	EventCode=6000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=5634
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The winlogon notification subscriber <SessionEnv> was unavailable to handle a notification event.

2024-04-30T11:52:39+0530	04/30/2024 11:52:39 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igfxCUIService2.0.0.0
	Type=Information
	RecordNumber=5633
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

Time	Event

2024-04-30T11:52:39+0530	04/30/2024 11:52:39 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igfxCUIService2.0.0.0
	Type=Information
	RecordNumber=5632
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:52:38+0530	04/30/2024 11:52:38 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67564 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:38+0530  04/30/2024 11:52:38 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67563
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:38+0530	04/30/2024 11:52:38 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67562 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:38+0530	04/30/2024 11:52:38 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67561 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:38+0530	04/30/2024 11:52:38 AM
	LogName=Application
	EventCode=2
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=WMIRegistrationService
	Type=Information
	RecordNumber=5631
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) WMI Registration Service has successfully finished WMI Registration.

2024-04-30T11:52:37+0530	04/30/2024 11:52:37 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67560 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0x688 Process Name:C:\Windows\System32\svchost.exe

2024-04-30T11:52:37+0530	04/30/2024 11:52:37 AM
	LogName=Application
	EventCode=63
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WMI
	Type=Warning
	RecordNumber=5630
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=A provider, IntelMEProv, has been registered in the Windows Management Instrumentation namespace root\Intel_ME to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.

2024-04-30T11:52:37+0530	04/30/2024 11:52:37 AM
	LogName=Application
	EventCode=63
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WMI
	Type=Warning
	RecordNumber=5629
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=A provider, IntelMEProv, has been registered in the Windows Management Instrumentation namespace root\Intel_ME to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.

Time	Event

2024-04-30T11:52:37+0530	04/30/2024 11:52:37 AM
	LogName=Application
	EventCode=63
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WMI
	Type=Warning
	RecordNumber=5628
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=A provider, IntelMEProv, has been registered in the Windows Management Instrumentation namespace root\Intel_ME to use the LocalSystem account. This account is privileged and the provider may cause a security violation if it does not correctly impersonate user requests.

2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM
	LogName=System
	EventCode=7001
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=18740
	Keywords=None
	TaskCategory=1101
	OpCode=Info
	Message=User Logon Notification for Customer Experience Improvement Program

2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM
	LogName=System
	EventCode=113
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18739
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=AddUrl
	Message=Attempted to add URL (http://*:5357/bd55c2c6-03b7-4c4f-9696-8861d56332c0/) to URL group (0xFE00000420000001). Status: 0x0. Process Id 0x1954 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM
	LogName=System
	EventCode=111
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18738
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=CreateUrlGroup
	Message=Create URL group 0xFE00000420000001. Status 0x0. Process Id 0x1954 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

Time	Event
2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67559 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x68686 Privileges:SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

Time	Event
2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67558 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x686C2 Linked Logon ID:0x68686 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x9fc Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:DESKTOP-LU7VRCG 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 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.

Time	Event
2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67557 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x68686 Linked Logon ID:0x686C2 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x9fc Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:DESKTOP-LU7VRCG 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 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.

Time	Event
2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67556 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x9fc Process Name:C:\Windows\System32\svchost.exe Network Information: Network Address:127.0.0.1 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.

2024-04-30T11:52:33+0530	04/30/2024 11:52:33 AM
	LogName=Application
	EventCode=6003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=5627
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The winlogon notification subscriber <SessionEnv> was unavailable to handle a critical notification event.

2024-04-30T11:52:32+0530	04/30/2024 11:52:32 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=jenkins
	Type=Information
	RecordNumber=5626
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service started successfully.

2024-04-30T11:52:31+0530	04/30/2024 11:52:31 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=emBridge
	Type=Information
	RecordNumber=5625
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service started successfully.

Time	Event

2024-04-30T11:52:31+0530	04/30/2024 11:52:31 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=jenkins
	Type=Information
	RecordNumber=5624
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Starting C:\Program Files\Java\jdk-17\bin\java.exe -Xrs -Xmx256m -Dhudson.lifecycle=hudson.lifecycle.WindowsServiceLifecycle -jar "C:\Program Files\Jenkins\jenkins.war" --httpPort=8080 --webroot="C:\ProgramData\Jenkins\war"

2024-04-30T11:52:30+0530	04/30/2024 11:52:30 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18737
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:52:29+0530	04/30/2024 11:52:29 AM
	LogName=System
	EventCode=7023
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Error
	RecordNumber=18736
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=The ZeroConfigService service terminated with the following error:
	%%2147770990

2024-04-30T11:52:27+0530	04/30/2024 11:52:27 AM
	LogName=Application
	EventCode=5617
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WMI
	Type=Information
	RecordNumber=5623
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Windows Management Instrumentation Service subsystems initialized successfully

Time	Event
2024-04-30T11:52:24+0530	04/30/2024 11:52:24 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67555 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:24+0530	04/30/2024 11:52:24 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67554 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:23+0530	04/30/2024 11:52:23 AM
	LogName=Security
	EventCode=5024
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67553
	Keywords=Audit Success
	TaskCategory=Other System Events
	OpCode=Info
	Message=The Windows Firewall service started successfully.

2024-04-30T11:52:21+0530	04/30/2024 11:52:21 AM
	LogName=System
	EventCode=10002
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WLAN-AutoConfig
	Type=Warning
	RecordNumber=18735
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=WLAN Extensibility Module has stopped.
	
	Module Path: C:\\WINDOWS\system32\IntelIHVRouter06.dll

2024-04-30T11:52:21+0530	04/30/2024 11:52:21 AM
	LogName=System
	EventCode=10001
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WLAN-AutoConfig
	Type=Information
	RecordNumber=18734
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=WLAN Extensibility Module has successfully started.
	
	Module Path: C:\\WINDOWS\system32\IntelIHVRouter06.dll

2024-04-30T11:52:20+0530	04/30/2024 11:52:20 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67552 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:20+0530	04/30/2024 11:52:20 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67551 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:19+0530	04/30/2024 11:52:19 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5622
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service Started.

2024-04-30T11:52:19+0530	04/30/2024 11:52:19 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5621
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=VMAuthdRunService: WSCSetApplicationCategory succeeded: 0x80000000

2024-04-30T11:52:19+0530	04/30/2024 11:52:19 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5620
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=W32Util_IsDirectorySafe: Failed DACL num entries check, "C:\WINDOWS\TEMP\vmware-SYSTEM"

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5619
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Msg_SetLocaleEx: HostLocale=windows-1252 UserLocale=NULL

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5618
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=LOCALE windows-1252 -> NULL User=4009 System=409

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5617
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=lib/ssl: curves list prime256v1:secp384r1:secp521r1

Time	Event

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5616
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=lib/ssl: cipher list ECDHE+AESGCM:RSA+AESGCM:ECDHE+AES:RSA+AES

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5615
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=lib/ssl: protocol list tls1.2 (openssl flags 0x36000000)

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5614
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=lib/ssl: protocol list tls1.2

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5613
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=lib/ssl: OpenSSL using RAND_OpenSSL for RAND

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5612
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PREF Optional preferences file not found at C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\preferences.ini. Using default values.

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5611
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=[msg.dictionary.load.openFailed] Cannot open file "C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\preferences.ini": The system cannot find the file specified.

Time	Event

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5610
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=DictionaryLoad: Cannot open file "C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\preferences.ini": The system cannot find the file specified.

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5609
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PREF Optional preferences file not found at C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\config.ini. Using default values.

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5608
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=[msg.dictionary.load.openFailed] Cannot open file "C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\config.ini": The system cannot find the file specified.

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5607
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=DictionaryLoad: Cannot open file "C:\WINDOWS\system32\config\systemprofile\AppData\Roaming\VMware\config.ini": The system cannot find the file specified.

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmauthd
	Type=Information
	RecordNumber=5606
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Log for vmauthd version=17.0.0 build=build-20800274 option=Release

2024-04-30T11:52:18+0530	04/30/2024 11:52:18 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=LMS
	Type=Information
	RecordNumber=5605
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service started/resumed

Time	Event
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67550 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-20 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E4 Group: Security ID:S-1-5-32-551 Group Name:Backup Operators Group Domain:Builtin Process Information: Process ID:0x12bc Process Name:C:\Windows\System32\svchost.exe
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67549 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-551 Group Name:Backup Operators Group Domain:Builtin Process Information: Process ID:0x1358 Process Name:C:\Windows\System32\svchost.exe

Time	Event
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67548 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-20 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E4 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0x12bc Process Name:C:\Windows\System32\svchost.exe
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4799 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67547 Keywords=Audit Success TaskCategory=Security Group Management OpCode=Info Message=A security-enabled local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Group: Security ID:S-1-5-32-544 Group Name:Administrators Group Domain:Builtin Process Information: Process ID:0x1358 Process Name:C:\Windows\System32\svchost.exe

Time	Event
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67546 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:17+0530	04/30/2024 11:52:17 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67545 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:16+0530	04/30/2024 11:52:16 AM
	LogName=System
	EventCode=4000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WLAN-AutoConfig
	Type=Information
	RecordNumber=18733
	Keywords=None
	TaskCategory=None
	OpCode=Start
	Message=WLAN AutoConfig service has successfully started.

2024-04-30T11:52:16+0530	04/30/2024 11:52:16 AM
	LogName=Application
	EventCode=2000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=LMS
	Type=Information
	RecordNumber=5604
	Keywords=Classic
	TaskCategory=LMS
	OpCode=%1
	Message=Local Management Service started.

2024-04-30T11:52:16+0530	04/30/2024 11:52:16 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=AdobeARMservice
	Type=Information
	RecordNumber=5603
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:52:15+0530	04/30/2024 11:52:15 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=VMware NAT Service
	Type=Information
	RecordNumber=5602
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Using configuration file: C:\ProgramData\VMware\vmnetnat.conf.
	IP address: 192.168.138.2
	 Subnet: 255.255.255.0
	External IP address: 0.0.0.0
	Device: VMnet8.
	MAC address: 00:50:56:ED:05:47.
	Ignoring host MAC address: 00:50:56:C0:00:08.

2024-04-30T11:52:15+0530	04/30/2024 11:52:15 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=WMIRegistrationService
	Type=Information
	RecordNumber=5601
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) WMI Registration Service started.

Time	Event

2024-04-30T11:52:15+0530	04/30/2024 11:52:15 AM
	LogName=Application
	EventCode=1000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=VMware NAT Service
	Type=Information
	RecordNumber=5600
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Service started

2024-04-30T11:52:15+0530	04/30/2024 11:52:15 AM
	LogName=Application
	EventCode=1008
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5599
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Started C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\influxdb\influxd.exe for service LoadRunner Data Service in C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\influxdb.

2024-04-30T11:52:15+0530	04/30/2024 11:52:15 AM
	LogName=Application
	EventCode=1008
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5598
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Started C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\Dashboard\Service\DashboardService.exe for service LoadRunner Dashboard Service in C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\Dashboard\Service.

2024-04-30T11:52:14+0530	04/30/2024 11:52:14 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=IntelDalJhi
	Type=Information
	RecordNumber=5597
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) Dynamic Application Loader Host Interface Service started.

2024-04-30T11:52:13+0530	04/30/2024 11:52:13 AM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5595
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Dashboard Service received START control, which will be handled.

2024-04-30T11:52:13+0530	04/30/2024 11:52:13 AM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5594
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Data Service received START control, which will be handled.

Time	Event

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=System
	EventCode=12
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-UserModePowerService
	Type=Information
	RecordNumber=18732
	Keywords=None
	TaskCategory=10
	OpCode=Info
	Message=Process C:\Windows\System32\Intel\DPTF\esif_uf.exe (process ID:4744) reset policy scheme from {381b4222-f694-41f0-9685-ff5bb260df2e} to {381b4222-f694-41f0-9685-ff5bb260df2e}

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=System
	EventCode=12
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-UserModePowerService
	Type=Information
	RecordNumber=18731
	Keywords=None
	TaskCategory=10
	OpCode=Info
	Message=Process C:\Windows\System32\Intel\DPTF\esif_uf.exe (process ID:4744) reset policy scheme from {381b4222-f694-41f0-9685-ff5bb260df2e} to {381b4222-f694-41f0-9685-ff5bb260df2e}

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=System
	EventCode=12
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-UserModePowerService
	Type=Information
	RecordNumber=18730
	Keywords=None
	TaskCategory=10
	OpCode=Info
	Message=Process C:\Windows\System32\Intel\DPTF\esif_uf.exe (process ID:4744) reset policy scheme from {381b4222-f694-41f0-9685-ff5bb260df2e} to {381b4222-f694-41f0-9685-ff5bb260df2e}

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=System
	EventCode=34
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=vmx86
	Type=Information
	RecordNumber=18729
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=
	VMX86.SYS: begin DriverEntry

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67544 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67543 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67542 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                        Event
2024-04-30T11:52:12+0530    04/30/2024 11:52:12 AM
                            LogName=Security
                            EventCode=4624
                            EventType=0
                            ComputerName=DESKTOP-LU7VRCG
                            SourceName=Microsoft Windows security auditing.
                            Type=Information
                            RecordNumber=67541
                            Keywords=Audit Success
                            TaskCategory=Logon
                            OpCode=Info
                            Message=An account was successfully logged on.

                            Subject:
                            Security ID:S-1-5-18
                            Account Name:DESKTOP-LU7VRCG$
                            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:0x404
                            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.
```

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67540 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:12+0530  04/30/2024 11:52:12 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67539
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67538 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67537 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67536 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67535 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67534 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67533 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67532 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:12+0530  04/30/2024 11:52:12 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67531
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67530 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67529 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=Application
	EventCode=5615
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WMI
	Type=Information
	RecordNumber=5596
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Windows Management Instrumentation Service started sucessfully

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=RtkAudioUniversalService
	Type=Information
	RecordNumber=5593
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:52:12+0530	04/30/2024 11:52:12 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=FMAPOService
	Type=Information
	RecordNumber=5592
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:52:11+0530	04/30/2024 11:52:11 AM
	LogName=Security
	EventCode=5033
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67528
	Keywords=Audit Success
	TaskCategory=Other System Events
	OpCode=Info
	Message=The Windows Firewall Driver started successfully.

2024-04-30T11:52:10+0530	04/30/2024 11:52:10 AM
	LogName=System
	EventCode=267
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Win32k
	Type=Information
	RecordNumber=18728
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Touch/Touchpad Hardware Quality Assurance verification succeeded.

Time	Event
2024-04-30T11:52:09+0530	04/30/2024 11:52:09 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67527 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:09+0530	04/30/2024 11:52:09 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67526 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18727
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:10246/MDEServer/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18726
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:10247/apps/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18725
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:3387/rdp/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18724
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:3392/rdp/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18723
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8090:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18722
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8089:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18721
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8088:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18720
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8087:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18719
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8086:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18718
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8085:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18717
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8084:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18716
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8083:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18715
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8082:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18714
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8081:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18713
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://127.0.0.1:8080:127.0.0.1/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18712
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:26770/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18711
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:26769/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18710
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:10243/WMPNSSv4/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18709
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:10245/WMPNSSv4/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18708
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:443/sra_{BA195980-CD49-458b-9E23-C84EE0ADCD75}/. Status 0x0
	. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18707
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:80/116B50EB-ECE2-41ac-8429-9F9E963361B7/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18706
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:443/C574AC30-5794-4AEE-B1BB-6651C5315029/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18705
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:80/0131501b-d67f-491b-9a40-c4bf27bcb4d4/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18704
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://*:2869/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18703
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:5985/wsman/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18702
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:47001/wsman/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18701
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://+:5986/wsman/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18700
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL https://*:5358/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18699
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://+:80/Temporary_Listen_Addresses/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

Time	Event

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM
	LogName=System
	EventCode=112
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18698
	Keywords=Flagged on all HTTP events dealing with service setup
	TaskCategory=HTTP Setup Trace Task
	OpCode=ResvUrlV2
	Message=Attempted to reserve URL http://*:5357/. Status 0x0. Process Id 0x4 Executable path , User S-1-5-18

2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67525 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67524 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67523 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67522 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67521 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:08+0530  04/30/2024 11:52:08 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67520
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67519 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:08+0530	04/30/2024 11:52:08 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67518 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:06+0530	04/30/2024 11:52:06 AM
	LogName=System
	EventCode=51046
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18697
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStart
	Message=DHCPv6 client service is started

2024-04-30T11:52:06+0530	04/30/2024 11:52:06 AM
	LogName=System
	EventCode=50036
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18696
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStart
	Message=DHCPv4 client service is started

2024-04-30T11:52:06+0530	04/30/2024 11:52:06 AM
	LogName=System
	EventCode=50103
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18695
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceShutdown
	Message=DHCPv4 client registered for shutdown notification

2024-04-30T11:52:06+0530	04/30/2024 11:52:06 AM
	LogName=System
	EventCode=50036
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18694
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStart
	Message=DHCPv4 client service is started

2024-04-30T11:52:05+0530	04/30/2024 11:52:05 AM
	LogName=System
	EventCode=1
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=VMnetuserif
	Type=Information
	RecordNumber=18693
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=() Starting up the User Interface Driver for VMware Virtual Networks.

Time	Event
2024-04-30T11:52:05+0530	04/30/2024 11:52:05 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67517 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:05+0530  04/30/2024 11:52:05 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67516
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event

2024-04-30T11:52:04+0530	04/30/2024 11:52:04 AM
	LogName=System
	EventCode=10
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=VMnetBridge
	Type=Information
	RecordNumber=18692
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=() Starting up the Bridge Driver for VMware Virtual Networks.

2024-04-30T11:52:04+0530	04/30/2024 11:52:04 AM
	LogName=System
	EventCode=6013
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=EventLog
	Type=Information
	RecordNumber=18614
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The system uptime is 40 seconds.

2024-04-30T11:52:04+0530	04/30/2024 11:52:04 AM
	LogName=System
	EventCode=6005
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=EventLog
	Type=Information
	RecordNumber=18613
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Event log service was started.

2024-04-30T11:52:04+0530	04/30/2024 11:52:04 AM
	LogName=System
	EventCode=6009
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=EventLog
	Type=Information
	RecordNumber=18612
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Microsoft (R) Windows (R) 10.00. 22631 Multiprocessor Free.

Time	Event
2024-04-30T11:52:04+0530	04/30/2024 11:52:04 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67515 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:04+0530  04/30/2024 11:52:04 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67514
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event

2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM
	LogName=System
	EventCode=22
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Eventlog
	Type=Error
	RecordNumber=18691
	Keywords=Service availability
	TaskCategory=Service startup
	OpCode=Info
	Message=The event logging service encountered an error while initializing publishing resources for channel Microsoft-RMS-MSIPC/Debug. If channel type is Analytic or Debug, then this could mean there was an error initializing logging resources as well.

2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM
	LogName=System
	EventCode=22
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Eventlog
	Type=Error
	RecordNumber=18690
	Keywords=Service availability
	TaskCategory=Service startup
	OpCode=Info
	Message=The event logging service encountered an error while initializing publishing resources for channel DebugChannel. If channel type is Analytic or Debug, then this could mean there was an error initializing logging resources as well.

2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM
	LogName=System
	EventCode=22
	EventType=2
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Eventlog
	Type=Error
	RecordNumber=18689
	Keywords=Service availability
	TaskCategory=Service startup
	OpCode=Info
	Message=The event logging service encountered an error while initializing publishing resources for channel AirSpaceChannel. If channel type is Analytic or Debug, then this could mean there was an error initializing logging resources as well.

Time	Event
2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67513 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:03+0530  04/30/2024 11:52:03 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67512
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67511 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67510 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:03+0530	04/30/2024 11:52:03 AM
	LogName=Application
	EventCode=9027
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Desktop Window Manager
	Type=Information
	RecordNumber=5590
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Desktop Window Manager has registered the session port.

2024-04-30T11:52:02+0530	04/30/2024 11:52:02 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67509 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:02+0530	04/30/2024 11:52:02 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67508 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:02+0530	04/30/2024 11:52:02 AM
	LogName=Application
	EventCode=1531
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-User Profile Service
	Type=Information
	RecordNumber=5591
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The User Profile Service has started successfully.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18688
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'bindflt' (10.0, 2032-10-20T06:52:30.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18687
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'storqosflt' (10.0, 2039-04-22T07:06:38.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18686
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'CldFlt' (10.0, 2097-10-23T01:54:28.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=1
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18685
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'CldFlt' (Version 10.0, 2097-10-23T01:54:28.000000000Z) unloaded successfully.

Time	Event

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18684
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'CldFlt' (10.0, 2097-10-23T01:54:28.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18683
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'luafv' (10.0, 2059-02-13T14:58:11.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18682
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'wcifs' (10.0, 2065-03-02T12:24:53.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18681
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'bfs' (10.0, 1970-07-19T17:06:58.000000000Z) has successfully loaded and registered with Filter Manager.

Time	Event
2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67507 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67506 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67505 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:01+0530	04/30/2024 11:52:01 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67504 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67503 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:00+0530  04/30/2024 11:52:00 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67502
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67501 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67500 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67499 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:52:00+0530  04/30/2024 11:52:00 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67498
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x404
                          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.
```

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67497 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67496 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67495 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67494 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67493 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67492 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM
	LogName=Security
	EventCode=4672
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67491
	Keywords=Audit Success
	TaskCategory=Special Logon
	OpCode=Info
	Message=Special privileges assigned to new logon.
	
	Subject:
	Security ID:S-1-5-90-0-1
	Account Name:DWM-1
	Account Domain:Window Manager
	Logon ID:0x1C114
	
	Privileges:SeAssignPrimaryTokenPrivilege
	SeAuditPrivilege

2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM
	LogName=Security
	EventCode=4672
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67490
	Keywords=Audit Success
	TaskCategory=Special Logon
	OpCode=Info
	Message=Special privileges assigned to new logon.
	
	Subject:
	Security ID:S-1-5-90-0-1
	Account Name:DWM-1
	Account Domain:Window Manager
	Logon ID:0x1BFEF
	
	Privileges:SeAssignPrimaryTokenPrivilege
	SeAuditPrivilege
	SeImpersonatePrivilege

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67489 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:Yes Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-90-0-1 Account Name:DWM-1 Account Domain:Window Manager Logon ID:0x1C114 Linked Logon ID:0x1BFEF Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x464 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. 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.

```
Time                      Event
2024-04-30T11:52:00+0530  04/30/2024 11:52:00 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67488
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Logon Information:
                          Logon Type:2
                          Restricted Admin Mode:-
                          Remote Credential Guard:-
                          Virtual Account:Yes
                          Elevated Token:Yes

                          Impersonation Level:Impersonation

                          New Logon:
                          Security ID:S-1-5-90-0-1
                          Account Name:DWM-1
                          Account Domain:Window Manager
                          Logon ID:0x1BFEF
                          Linked Logon ID:0x1C114
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x464
                          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.

                          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.
```

Time	Event
2024-04-30T11:52:00+0530	04/30/2024 11:52:00 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67487 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:DWM-1 Account Domain:Window Manager Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x464 Process Name:C:\Windows\System32\winlogon.exe Network Information: Network Address:- Port:- 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.
2024-04-30T11:51:59+0530	04/30/2024 11:51:59 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67486 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:51:59+0530	04/30/2024 11:51:59 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67485 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM
	LogName=System
	EventCode=16983
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Directory-Services-SAM
	Type=Information
	RecordNumber=18680
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The security account manager is now logging periodic summary events for remote clients that call legacy
	password change or set RPC methods.
	
	For more information please see https://go.microsoft.com/fwlink/?linkid=2150956.

2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM
	LogName=System
	EventCode=16977
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Directory-Services-SAM
	Type=Information
	RecordNumber=18679
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The domain is configured with the following minimum password length-related settings.
	
	MinimumPasswordLength: 0
	
	RelaxMinimumPasswordLengthLimits: 0
	
	MinimumPasswordLengthAudit: -1
	
	For more information see https://go.microsoft.com/fwlink/?LinkId=2097191.

2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM
	LogName=System
	EventCode=16962
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Directory-Services-SAM
	Type=Information
	RecordNumber=18678
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Remote calls to the SAM database are being restricted using the default security descriptor: O:SYG:SYD:(A;;RC;;;BA).
	For more information please see http://go.microsoft.com/fwlink/?LinkId=787651.

Time	Event

2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM
	LogName=Security
	EventCode=4672
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67484
	Keywords=Audit Success
	TaskCategory=Special Logon
	OpCode=Info
	Message=Special privileges assigned to new logon.
	
	Subject:
	Security ID:S-1-5-20
	Account Name:NETWORK SERVICE
	Account Domain:NT AUTHORITY
	Logon ID:0x3E4
	
	Privileges:SeAssignPrimaryTokenPrivilege
	SeAuditPrivilege
	SeImpersonatePrivilege

```
Time                      Event
2024-04-30T11:51:58+0530  04/30/2024 11:51:58 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67483
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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-1-5-20
                          Account Name:NETWORK SERVICE
                          Account Domain:NT AUTHORITY
                          Logon ID:0x3E4
                          Linked Logon ID:0x0
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x404
                          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.
```

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67482 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:Yes Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-96-0-1 Account Name:UMFD-1 Account Domain:Font Driver Host Logon ID:0x138D1 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x464 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. 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.

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67481 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:Yes Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-96-0-0 Account Name:UMFD-0 Account Domain:Font Driver Host Logon ID:0x13900 Linked Logon ID:0x0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x390 Process Name:C:\Windows\System32\wininit.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.

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67480 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:UMFD-1 Account Domain:Font Driver Host Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x464 Process Name:C:\Windows\System32\winlogon.exe Network Information: Network Address:- Port:- 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.

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67479 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:UMFD-0 Account Domain:Font Driver Host Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x390 Process Name:C:\Windows\System32\wininit.exe Network Information: Network Address:- Port:- 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.

2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM
	LogName=Security
	EventCode=4672
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67478
	Keywords=Audit Success
	TaskCategory=Special Logon
	OpCode=Info
	Message=Special privileges assigned to new logon.
	
	Subject:
	Security ID:S-1-5-19
	Account Name:LOCAL SERVICE
	Account Domain:NT AUTHORITY
	Logon ID:0x3E5
	
	Privileges:SeAssignPrimaryTokenPrivilege
	SeAuditPrivilege
	SeImpersonatePrivilege

```
Time                      Event
2024-04-30T11:51:58+0530  04/30/2024 11:51:58 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67477
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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-1-5-19
                          Account Name:LOCAL SERVICE
                          Account Domain:NT AUTHORITY
                          Logon ID:0x3E5
                          Linked Logon ID:0x0
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x404
                          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.
```

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67476 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:51:58+0530	04/30/2024 11:51:58 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67475 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x404 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.

Time	Event

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18677
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: msv1_0

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18676
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: sfapm

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18675
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: schannel

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18674
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: wdigest

Time	Event

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18673
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: cloudap

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18672
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: pku2u

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18671
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: tspkg

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18670
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: msv1_0

Time	Event

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=267
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Win32k
	Type=Information
	RecordNumber=18669
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Touch/Touchpad Hardware Quality Assurance verification succeeded.

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18668
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: kerberos

2024-04-30T11:51:57+0530	04/30/2024 11:51:57 AM
	LogName=Security
	EventCode=4902
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67474
	Keywords=Audit Success
	TaskCategory=Audit Policy Change
	OpCode=Info
	Message=The Per-user audit policy table was created.
	
	Number of Elements:0
	Policy ID:0x132C6

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=System
	EventCode=6155
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Warning
	RecordNumber=18667
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=LSA package is not signed as expected. This can cause unexpected behavior with Credential Guard.
	
	PackageName: negoexts

Time	Event

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=System
	EventCode=6156
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-LSA
	Type=Information
	RecordNumber=18666
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Virtualization Based Security for Credential Guard auto enablement status.
	
	Hardware Requirements:1
	Domain Joined:0
	Azure AD Joined:0

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=System
	EventCode=15
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Wininit
	Type=Warning
	RecordNumber=18665
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Credential Guard and/or VBS Key Isolation are configured but the secure kernel is not running; continuing without them.

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=System
	EventCode=14
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Wininit
	Type=Information
	RecordNumber=18664
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Credential Guard configuration:
	
	Registry Configuration: 0x2
	Test Configuration: 0
	Auto Enablement: 1

Time	Event
2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67473 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Logon Information: Logon Type:0 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:Yes Impersonation Level:- 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:0x4 Process Name: Network Information: Workstation Name:- Source Network Address:- Source Port:- Detailed Authentication Information: Logon Process:- Authentication Package:- 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.

Time	Event

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=Security
	EventCode=4608
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67472
	Keywords=Audit Success
	TaskCategory=Security State Change
	OpCode=Info
	Message=Windows is starting up.
	
	This event is logged when LSASS.EXE starts and the auditing subsystem is initialized.

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM
	LogName=Security
	EventCode=6417
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67471
	Keywords=Audit Success
	TaskCategory=System Integrity
	OpCode=Info
	Message=The FIPS mode crypto selftests succeeded.
	
	Process ID:0x41c
	Process Name:C:\Windows\System32\lsass.exe

2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67470 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x41c New Process Name:C:\Windows\System32\lsass.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x390 Creator Process Name:C:\Windows\System32\wininit.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2024-04-30T11:51:56+0530	04/30/2024 11:51:56 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67469 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x404 New Process Name:C:\Windows\System32\services.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x390 Creator Process Name:C:\Windows\System32\wininit.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

```
Time                      Event
2024-04-30T11:51:55+0530  04/30/2024 11:51:55 AM
                          LogName=Security
                          EventCode=4688
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67468
                          Keywords=Audit Success
                          TaskCategory=Process Creation
                          OpCode=Info
                          Message=A new process has been created.

                          Creator Subject:
                          Security ID:S-1-5-18
                          Account Name:-
                          Account Domain:-
                          Logon ID:0x3E7

                          Target Subject:
                          Security ID:S-1-0-0
                          Account Name:-
                          Account Domain:-
                          Logon ID:0x0

                          Process Information:
                          New Process ID:0x390
                          New Process Name:C:\Windows\System32\wininit.exe
                          Token Elevation Type:TokenElevationTypeDefault (1)
                          Mandatory Label:S-1-16-16384
                          Creator Process ID:0x3b4
                          Creator Process Name:C:\Windows\System32\smss.exe
                          Process Command Line:

                          Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy.

                          Type 1 is a full token with no privileges removed or groups disabled.  A full token is only used if User Account
                          Control is disabled or if the user is the built-in Administrator account or a service account.

                          Type 2 is an elevated token with no privileges removed or groups disabled.  An elevated token is used when User
                          Account Control is enabled and the user chooses to start the program using Run as administrator.  An elevated token
                           is also used when an application is configured to always require administrative privilege or to always require maximum
                          privilege, and the user is a member of the Administrators group.

                          Type 3 is a limited token with administrative privileges removed and administrative groups disabled.  The limited token
                          is used when User Account Control is enabled, the application does not require administrative privilege, and the user
                          does not choose to start the program using Run as administrator.
```

Time	Event
2024-04-30T11:51:55+0530	04/30/2024 11:51:55 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67467 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x360 New Process Name:C:\Windows\System32\csrss.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x348 Creator Process Name:C:\Windows\System32\smss.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2024-04-30T11:51:55+0530	04/30/2024 11:51:55 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67466 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x348 New Process Name:C:\Windows\System32\smss.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x2ac Creator Process Name:C:\Windows\System32\smss.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2024-04-30T11:51:54+0530	04/30/2024 11:51:54 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67465 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x3c4 New Process Name:C:\Windows\System32\csrss.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x3b4 Creator Process Name:C:\Windows\System32\smss.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2024-04-30T11:51:54+0530	04/30/2024 11:51:54 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67464 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x3b4 New Process Name:C:\Windows\System32\smss.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x2ac Creator Process Name:C:\Windows\System32\smss.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

2024-04-30T11:51:53+0530	04/30/2024 11:51:53 AM
	LogName=System
	EventCode=24
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-General
	Type=Information
	RecordNumber=18663
	Keywords=Time
	TaskCategory=11
	OpCode=Info
	Message=The time zone information was refreshed with exit reason 0. Current time zone bias is -330.

2024-04-30T11:51:51+0530	04/30/2024 11:51:51 AM
	LogName=System
	EventCode=98
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Ntfs
	Type=Information
	RecordNumber=18662
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Volume \\?\Volume{d6a4eca2-c474-4f2e-926b-4789c15ec43a} (\Device\HarddiskVolume4) is healthy. No action is needed.

Time	Event
2024-04-30T11:51:51+0530	04/30/2024 11:51:51 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67463 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x35c New Process Name:C:\Windows\System32\autochk.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x2ac Creator Process Name:C:\Windows\System32\smss.exe Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

2024-04-30T11:51:45+0530	04/30/2024 11:51:45 AM
	LogName=System
	EventCode=27
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=e1i68x64
	Type=Warning
	RecordNumber=18661
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) Ethernet Connection (4) I219-V
	 Network link is disconnected.

2024-04-30T11:51:44+0530	04/30/2024 11:51:44 AM
	LogName=System
	EventCode=219
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-PnP
	Type=Warning
	RecordNumber=18660
	Keywords=None
	TaskCategory=212
	OpCode=Info
	Message=The driver \Driver\WUDFRd failed to load for the device USB\VID_06CB&PID_009A\9c44b486162f.

Time	Event

2024-04-30T11:51:44+0530	04/30/2024 11:51:44 AM
	LogName=System
	EventCode=10118
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DriverFrameworks-UserMode
	Type=Information
	RecordNumber=18659
	Keywords=None
	TaskCategory=Startup of the UMDF reflector
	OpCode=Info
	Message=UMDF reflector is unable to connect to service control manager (SCM). This is expected during boot, when SCM has not started yet. Will retry when it starts.

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=7017
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18658
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7017 - secure boot (SB) configuration

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=7010
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18657
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7010 - driver enabled (miniport init)

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=7002
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18656
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7002 - CTDP power limit value (SPLC)

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=7005
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18655
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7005 - SAR value max TX power (WRDS)

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=7036
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18654
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The \Device\NDMP6 service entered the Intel(R) Dual Band Wireless-AC 8265 state.

Time	Event

2024-04-30T11:51:41+0530	04/30/2024 11:51:41 AM
	LogName=System
	EventCode=2
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=MEIx64
	Type=Information
	RecordNumber=18653
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) Management Engine Interface driver has started successfully.

2024-04-30T11:51:39+0530	04/30/2024 11:51:39 AM
	LogName=System
	EventCode=521
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18652
	Keywords=None
	TaskCategory=220
	OpCode=Info
	Message=Active battery count change.

2024-04-30T11:51:39+0530	04/30/2024 11:51:39 AM
	LogName=System
	EventCode=521
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18651
	Keywords=None
	TaskCategory=220
	OpCode=Info
	Message=Active battery count change.

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18650
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 7 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

Time	Event

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18649
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 5 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18648
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 3 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18647
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 1 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

Time	Event

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18646
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 6 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18645
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 4 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18644
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 2 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

Time	Event

2024-04-30T11:51:38+0530	04/30/2024 11:51:38 AM
	LogName=System
	EventCode=55
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Information
	RecordNumber=18643
	Keywords=None
	TaskCategory=47
	OpCode=Info
	Message=Processor 0 in group 0 exposes the following power management capabilities:
	
	Idle state type: ACPI Idle (C) States (3 state(s))
	
	Performance state type: ACPI Performance (P) / Throttle (T) States
	Nominal Frequency (MHz): 1801
	Maximum performance percentage: 100
	Minimum performance percentage: 22
	Minimum throttle percentage: 2

2024-04-30T11:51:35+0530	04/30/2024 11:51:35 AM
	LogName=System
	EventCode=219
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-PnP
	Type=Warning
	RecordNumber=18642
	Keywords=None
	TaskCategory=212
	OpCode=Info
	Message=The driver \Driver\WUDFRd failed to load for the device PCI\VEN_8086&DEV_1903&SUBSYS_506A17AA&REV_08\3&11583659&0&20.

2024-04-30T11:51:35+0530	04/30/2024 11:51:35 AM
	LogName=System
	EventCode=10118
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DriverFrameworks-UserMode
	Type=Information
	RecordNumber=18641
	Keywords=None
	TaskCategory=Startup of the UMDF reflector
	OpCode=Info
	Message=UMDF reflector is unable to connect to service control manager (SCM). This is expected during boot, when SCM has not started yet. Will retry when it starts.

2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM
	LogName=System
	EventCode=172
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18640
	Keywords=None
	TaskCategory=203
	OpCode=Info
	Message=Connectivity state in standby: Disconnected, Reason: NIC compliance

Time	Event

2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM
	LogName=System
	EventCode=125
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18639
	Keywords=None
	TaskCategory=86
	OpCode=Info
	Message=ACPI thermal zone _TZ.THM0 has been enumerated.
	_PSV = 0K
	_TC1 = 0
	_TC2 = 0
	_TSP = 0ms
	_AC0 = 0K
	_AC1 = 0K
	_AC2 = 0K
	_AC3 = 0K
	_AC4 = 0K
	_AC5 = 0K
	_AC6 = 0K
	_AC7 = 0K
	_AC8 = 0K
	_AC9 = 0K
	_CRT = 400K
	_HOT = 0K
	minimum throttle = 0
	_CR3 = 0K

2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM
	LogName=System
	EventCode=36
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=VMnetAdapter
	Type=Information
	RecordNumber=18638
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=() Starting up the Adapter Driver for VMware Virtual Networks.

Time	Event
2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67462 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x2ac New Process Name:C:\Windows\System32\smss.exe Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x4 Creator Process Name: Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

Time	Event
2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM LogName=Security EventCode=4826 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67461 Keywords=Audit Success TaskCategory=Other Policy Change Events OpCode=Info Message=Boot Configuration Data loaded. Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 General Settings: Load Options:- Advanced Options:No Configuration Access Policy:Default System Event Logging:No Kernel Debugging:No VSM Launch Type:Off Signature Settings: Test Signing:No Flight Signing:No Disable Integrity Checks:No HyperVisor Settings: HyperVisor Load Options:- HyperVisor Launch Type:Off HyperVisor Debugging:No
2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM LogName=Security EventCode=4696 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67460 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A primary token was assigned to process. Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Process Information: Process ID:0x4 Process Name: Target Process: Target Process ID:0x9c Target Process Name:Registry New Token Information: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x3E7

Time	Event
2024-04-30T11:51:34+0530	04/30/2024 11:51:34 AM LogName=Security EventCode=4688 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67459 Keywords=Audit Success TaskCategory=Process Creation OpCode=Info Message=A new process has been created. Creator Subject: Security ID:S-1-5-18 Account Name:- Account Domain:- Logon ID:0x3E7 Target Subject: Security ID:S-1-0-0 Account Name:- Account Domain:- Logon ID:0x0 Process Information: New Process ID:0x9c New Process Name:Registry Token Elevation Type:TokenElevationTypeDefault (1) Mandatory Label:S-1-16-16384 Creator Process ID:0x4 Creator Process Name: Process Command Line: Token Elevation Type indicates the type of token that was assigned to the new process in accordance with User Account Control policy. Type 1 is a full token with no privileges removed or groups disabled. A full token is only used if User Account Control is disabled or if the user is the built-in Administrator account or a service account. Type 2 is an elevated token with no privileges removed or groups disabled. An elevated token is used when User Account Control is enabled and the user chooses to start the program using Run as administrator. An elevated token is also used when an application is configured to always require administrative privilege or to always require maximum privilege, and the user is a member of the Administrators group. Type 3 is a limited token with administrative privileges removed and administrative groups disabled. The limited token is used when User Account Control is enabled, the application does not require administrative privilege, and the user does not choose to start the program using Run as administrator.

2024-04-30T11:51:33+0530	04/30/2024 11:51:33 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18637
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'npsvctrig' (10.0, 1979-12-19T21:42:41.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:51:31+0530	04/30/2024 11:51:31 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18636
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'UCPD' (10.0, 2053-03-18T16:47:45.000000000Z) has successfully loaded and registered with Filter Manager.

Time	Event

2024-04-30T11:51:31+0530	04/30/2024 11:51:31 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18635
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'FileCrypt' (10.0, 1983-08-19T08:28:35.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:51:27+0530	04/30/2024 11:51:27 AM
	LogName=System
	EventCode=98
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Ntfs
	Type=Information
	RecordNumber=18634
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Volume C: (\Device\HarddiskVolume3) is healthy. No action is needed.

2024-04-30T11:51:26+0530	04/30/2024 11:51:26 AM
	LogName=System
	EventCode=98
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Ntfs
	Type=Information
	RecordNumber=18633
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=Volume E: (\Device\HarddiskVolume5) is healthy. No action is needed.

2024-04-30T11:51:25+0530	04/30/2024 11:51:25 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18632
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'WdFilter' (10.0, 1985-01-06T00:23:45.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:51:25+0530	04/30/2024 11:51:25 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18631
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'Wof' (10.0, 2086-08-04T16:50:16.000000000Z) has successfully loaded and registered with Filter Manager.

Time	Event

2024-04-30T11:51:25+0530	04/30/2024 11:51:25 AM
	LogName=System
	EventCode=6
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-FilterManager
	Type=Information
	RecordNumber=18630
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=File System Filter 'FileInfo' (10.0, 2079-02-27T03:33:00.000000000Z) has successfully loaded and registered with Filter Manager.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=16
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-HAL
	Type=Information
	RecordNumber=18629
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The iommu fault reporting has been initialized.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=20
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-General
	Type=Information
	RecordNumber=18628
	Keywords=Time
	TaskCategory=6
	OpCode=Info
	Message=The leap second configuration has been updated.
	Reason: Leap second data initialized from registry during boot
	Leap seconds enabled: true
	New leap second count: 0
	Old leap second count: 0

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=30
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18627
	Keywords=None
	TaskCategory=21
	OpCode=Info
	Message=The firmware reported boot metrics.

Time	Event

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=32
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18626
	Keywords=None
	TaskCategory=58
	OpCode=Info
	Message=The bootmgr spent 0 ms waiting for user input.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=18
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18625
	Keywords=None
	TaskCategory=57
	OpCode=Info
	Message=There are 0x1 boot options on this system.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=27
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18624
	Keywords=None
	TaskCategory=33
	OpCode=Info
	Message=The boot type was 0x0.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=25
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18623
	Keywords=None
	TaskCategory=32
	OpCode=Info
	Message=The boot menu policy was 0x1.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=238
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18622
	Keywords=None
	TaskCategory=101
	OpCode=Info
	Message=EFI time zone bias: 2047. Daylight flags: 0. Firmware time: 2024-04-30T11:51:22.000000000Z.

Time	Event

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=20
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18621
	Keywords=None
	TaskCategory=31
	OpCode=Info
	Message=The last shutdown's success status was true. The last boot's success status was true.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=153
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18620
	Keywords=None
	TaskCategory=62
	OpCode=Info
	Message=Virtualization-based security (policies: 0) is disabled.

2024-04-30T11:51:24+0530	04/30/2024 11:51:24 AM
	LogName=System
	EventCode=12
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-General
	Type=Information
	RecordNumber=18619
	Keywords=None
	TaskCategory=1
	OpCode=Info
	Message=The operating system started at system time 2024-04-30T06:21:23.500000000Z.

2024-04-30T11:51:08+0530	04/30/2024 11:51:08 AM
	LogName=System
	EventCode=13
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-General
	Type=Information
	RecordNumber=18618
	Keywords=None
	TaskCategory=2
	OpCode=Info
	Message=The operating system is shutting down at system time 2024-04-30T06:21:08.106147200Z.

2024-04-30T11:51:05+0530	04/30/2024 11:51:05 AM
	LogName=System
	EventCode=577
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18617
	Keywords=None
	TaskCategory=280
	OpCode=Info
	Message=The system has prepared for a system initiated reboot from Active.

Time	Event

2024-04-30T11:50:43+0530	04/30/2024 11:50:43 AM
	LogName=System
	EventCode=109
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18616
	Keywords=None
	TaskCategory=103
	OpCode=Info
	Message=The kernel power manager has initiated a shutdown transition.
	
	Action: Power Action Reboot
	Event Code: 0x0
	Reason: Kernel API

2024-04-30T11:50:40+0530	04/30/2024 11:50:40 AM
	LogName=System
	EventCode=4001
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-WLAN-AutoConfig
	Type=Information
	RecordNumber=18615
	Keywords=None
	TaskCategory=None
	OpCode=Stop
	Message=WLAN AutoConfig service has successfully stopped.

2024-04-30T11:50:37+0530	04/30/2024 11:50:37 AM
	LogName=System
	EventCode=117
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18611
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=DeleteUrlGroup
	Message=Delete URL group 0xFE00000620000001. Status 0x0. Process Id 0x2224 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

2024-04-30T11:50:37+0530	04/30/2024 11:50:37 AM
	LogName=System
	EventCode=114
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-HttpService
	Type=Information
	RecordNumber=18610
	Keywords=Flagged on all HTTP events triggered on a URL group
	TaskCategory=HTTP Configuration Property Trace Task
	OpCode=RemUrl
	Message=Removed URL (http://*:5357/bd55c2c6-03b7-4c4f-9696-8861d56332c0/) from URL group (0xFE00000620000001). Process Id 0x2224 Executable path \Device\HarddiskVolume3\Windows\System32\svchost.exe, User S-1-5-19

Time	Event

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=50037
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18609
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStop
	Message=DHCPv4 client service is stopped. ShutDown Flag value is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18608
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18607
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18606
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18605
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

Time	Event

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18604
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51057
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18603
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStopWithRefCount
	Message=DHCPv6 client service stop is almost done.DHCP Context Ref count is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=51047
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-DHCPv6-Client
	Type=Information
	RecordNumber=18602
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceStop
	Message=DHCPv6 client service is stopped. ShutDown Flag value is 1

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=50106
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18601
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceShutdown
	Message=DHCPv4 is waiting on DHCPv6 service to stop

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=50105
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18600
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceShutdown
	Message=DHCPv4 client ProcessDHCPRequestForever received TERMINATE_EVENT

Time	Event

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=50104
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Dhcp-Client
	Type=Information
	RecordNumber=18599
	Keywords=None
	TaskCategory=Service State Event
	OpCode=ServiceShutdown
	Message=DHCPv4 client received shutdown notification

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=System
	EventCode=6006
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=EventLog
	Type=Information
	RecordNumber=18598
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The Event log service was stopped.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Security
	EventCode=1100
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Eventlog
	Type=Information
	RecordNumber=67458
	Keywords=Audit Success
	TaskCategory=Service shutdown
	OpCode=Info
	Message=The event logging service has shut down.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=1532
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-User Profile Service
	Type=Information
	RecordNumber=5589
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The User Profile Service has stopped.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=1011
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5588
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Killing process C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\influxdb\influxd.exe because service LoadRunner Data Service is stopping.

Time	Event

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5587
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Data Service received SHUTDOWN control, which will be handled.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=1012
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5586
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Requested stop of service LoadRunner Dashboard Service. No action is required as program C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\Dashboard\Service\DashboardService.exe is not running.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=RtkAudioUniversalService
	Type=Information
	RecordNumber=5585
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=2000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=LMS
	Type=Information
	RecordNumber=5584
	Keywords=Classic
	TaskCategory=LMS
	OpCode=%1
	Message=Local Management Service stopped.

2024-04-30T11:50:36+0530	04/30/2024 11:50:36 AM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5583
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Dashboard Service received SHUTDOWN control, which will be handled.

2024-04-30T11:50:35+0530	04/30/2024 11:50:35 AM
	LogName=Application
	EventCode=1034
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Warning
	RecordNumber=5582
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Dashboard Service ran for less than 1500 milliseconds. Restart will be delayed by 2000 milliseconds.

Time	Event

2024-04-30T11:50:35+0530	04/30/2024 11:50:35 AM
	LogName=Application
	EventCode=1014
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5581
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Service LoadRunner Dashboard Service action for exit code 0 is Restart. Attempting to restart C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\Dashboard\Service\DashboardService.exe.

2024-04-30T11:50:35+0530	04/30/2024 11:50:35 AM
	LogName=Application
	EventCode=1027
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5580
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Killing PID 5512 in process tree of PID 5512 because service LoadRunner Dashboard Service is stopping.

2024-04-30T11:50:35+0530	04/30/2024 11:50:35 AM
	LogName=Application
	EventCode=1023
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5579
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Killing process tree of process 5512 for service LoadRunner Dashboard Service with exit code 0

2024-04-30T11:50:35+0530	04/30/2024 11:50:35 AM
	LogName=Application
	EventCode=1013
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=nssm
	Type=Information
	RecordNumber=5578
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Program C:\Program Files (x86)\OpenText\LoadRunner\dat\Setup\LoadRunner\MSBuild\..\..\..\..\bin\Dashboard\Service\DashboardService.exe for service LoadRunner Dashboard Service exited with return code 0.

2024-04-30T11:50:33+0530	04/30/2024 11:50:33 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=220
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Network Agent stopped

Time	Event

2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM
	LogName=System
	EventCode=7002
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=18597
	Keywords=None
	TaskCategory=1102
	OpCode=Info
	Message=User Logoff Notification for Customer Experience Improvement Program

2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67457 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-504 Account Name:WDAGUtilityAccount Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe
2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67456 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-501 Account Name:Guest Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe

Time	Event
2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67455 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-503 Account Name:DefaultAccount Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe
2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67454 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-500 Account Name:Administrator Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe

Time	Event
2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67453 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe

2024-04-30T11:50:28+0530	04/30/2024 11:50:28 AM
	LogName=Application
	EventCode=6000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=5577
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The winlogon notification subscriber <SessionEnv> was unavailable to handle a notification event.

2024-04-30T11:50:27+0530	04/30/2024 11:50:27 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67452 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:50:27+0530  04/30/2024 11:50:27 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67451
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T11:50:27+0530	04/30/2024 11:50:27 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67450 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:50:27+0530  04/30/2024 11:50:27 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67449
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event

2024-04-30T11:50:27+0530	04/30/2024 11:50:27 AM
	LogName=Application
	EventCode=6000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Winlogon
	Type=Information
	RecordNumber=5576
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=The winlogon notification subscriber <WSearch> was unavailable to handle a notification event.

2024-04-30T11:50:27+0530	04/30/2024 11:50:27 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igfxCUIService2.0.0.0
	Type=Information
	RecordNumber=5575
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:50:27+0530	04/30/2024 11:50:27 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igfxCUIService2.0.0.0
	Type=Information
	RecordNumber=5574
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=The operation completed successfully.

2024-04-30T11:50:26+0530	04/30/2024 11:50:26 AM
	LogName=Security
	EventCode=4647
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67448
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=User initiated logoff:
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	
	This event is generated when a logoff is initiated. No further user-initiated activity can occur. This event can be interpreted as a logoff event.

Time	Event
2024-04-30T11:50:21+0530	04/30/2024 11:50:21 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67447 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:50:21+0530	04/30/2024 11:50:21 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67446 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:50:06+0530	04/30/2024 11:50:06 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18596
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:50:06+0530	04/30/2024 11:50:06 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18595
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:50:05+0530	04/30/2024 11:50:05 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18594
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:50:05+0530	04/30/2024 11:50:05 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67445 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:50:05+0530	04/30/2024 11:50:05 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67444 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:49:49+0530	04/30/2024 11:49:49 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18593
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:49:48+0530	04/30/2024 11:49:48 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18592
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:49:47+0530	04/30/2024 11:49:47 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18591
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67443
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67442
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67441
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67440
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67439
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:49:09+0530	04/30/2024 11:49:09 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67438
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:49:08+0530	04/30/2024 11:49:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67437 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:49:08+0530	04/30/2024 11:49:08 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67436 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:46:08+0530	04/30/2024 11:46:08 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18590
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:43:38+0530	04/30/2024 11:43:38 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5573 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket 2297000818131724559, type 4 Event Name: APPCRASH Response: Not available Cab Id: 2250365392405663694 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportArchive\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 268451852 Hashed bucket: 992d5e7b570e13afbfe09612f585e90f Cab Guid: f7cbec29-f6b8-4203-8f3a-e766c52c0fce

Time	Event

2024-04-30T11:42:29+0530	04/30/2024 11:42:29 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5572
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T06:12:29Z. Reason: RulesEngine.

2024-04-30T11:42:01+0530	04/30/2024 11:42:01 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67435 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:42:01+0530	04/30/2024 11:42:01 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67434 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:41:58+0530	04/30/2024 11:41:58 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5571
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

2024-04-30T11:41:56+0530	04/30/2024 11:41:56 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67433 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:41:56+0530	04/30/2024 11:41:56 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67432 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:41:08+0530	04/30/2024 11:41:08 AM
	LogName=Application
	EventCode=1033
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5570
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Windows Installer installed the product. Product Name: Splunk Enterprise. Product Version: 9.2.1.0. Product Language: 1033. Manufacturer: Splunk, Inc.. Installation success or error status: 0.

2024-04-30T11:41:08+0530	04/30/2024 11:41:08 AM
	LogName=Application
	EventCode=11707
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5569
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Product: Splunk Enterprise -- Installation completed successfully.

2024-04-30T11:41:00+0530	04/30/2024 11:41:00 AM
	LogName=Application
	EventCode=1042
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5568
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Ending a Windows Installer transaction: C:\Users\admin\Downloads\SPLUNK\splunk-9.2.1-78803f08aabb-x64-release (1).msi. Client Process Id: 7564.

2024-04-30T11:40:58+0530	04/30/2024 11:40:58 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67431 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

Time	Event

2024-04-30T11:40:38+0530	04/30/2024 11:40:38 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5567
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T06:10:38Z. Reason: RulesEngine.

2024-04-30T11:40:07+0530	04/30/2024 11:40:07 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5566
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

2024-04-30T11:40:04+0530	04/30/2024 11:40:04 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67430
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:40:04+0530	04/30/2024 11:40:04 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67429
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:40:04+0530	04/30/2024 11:40:04 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67428
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:40:04+0530	04/30/2024 11:40:04 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67427
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:40:03+0530	04/30/2024 11:40:03 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67426
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:40:03+0530	04/30/2024 11:40:03 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67425
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:40:03+0530	04/30/2024 11:40:03 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67424
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2024-04-30T11:39:32+0530	04/30/2024 11:39:32 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-21-1102696979-4129790392-413580853-1001 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5565 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket 1686379278370546074, type 5 Event Name: RADAR_PRE_LEAK_64 Response: Not available Cab Id: 0 Problem signature: P1: splunkd.exe P2: 2306.256.26107.30017 P3: 10.0.22631.2.0.0 P4: P5: P6: P7: P8: P9: P10: Attached files: \\?\C:\Users\admin\AppData\Local\Temp\RDR95AA.tmp\empty.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.ff91d937-7ba5-4985-9edc-7f72d79b036c.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.01e466fe-b9dd-44bf-b40a-e554b9b8d667.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.94f1700d-4122-479e-8ce3-50c1585a7417.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.f8ba94a6-2947-4849-a9f4-c25635f124a5.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.8e393356-0716-4db3-aa6a-afca3290cccf.tmp.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e260c551-694f-4b92-a82d-481d7f1e920e.tmp.xml These files may be available here: NULL Analysis symbol: Rechecking for solution: 0 Report Id: 6f0c572b-f46e-4222-b65c-569849e10ce4 Report Status: 268435456 Hashed bucket: 75852a02a38e15b697673904d3db219a Cab Guid: 0

2024-04-30T11:39:30+0530	04/30/2024 11:39:30 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67423
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:39:30+0530	04/30/2024 11:39:30 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67422
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:30+0530	04/30/2024 11:39:30 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67421
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:30+0530	04/30/2024 11:39:30 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67420
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:39:27+0530	04/30/2024 11:39:27 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67419
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:27+0530	04/30/2024 11:39:27 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67418
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:27+0530	04/30/2024 11:39:27 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67417
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:39:27+0530	04/30/2024 11:39:27 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67416
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:27+0530	04/30/2024 11:39:27 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67415
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67414
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67413
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67412
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67411
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C5F4
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67410
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67409
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67408
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67407 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:39:26+0530	04/30/2024 11:39:26 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67406 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:39:14+0530	04/30/2024 11:39:14 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67405 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:39:14+0530	04/30/2024 11:39:14 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67404 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:38:26+0530	04/30/2024 11:38:26 AM
	LogName=Kaspersky Event Log
	EventCode=3
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=klnagent
	Type=Information
	RecordNumber=219
	Keywords=Classic
	TaskCategory=General
	OpCode=Info
	Message=Compute-intensive operations are available again since the system awoke from Sleep mode.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18589
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 0 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18588
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 2 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18587
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 6 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18586
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 4 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

Time	Event

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18585
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 3 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18584
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 1 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18583
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 7 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=System
	EventCode=37
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Processor-Power
	Type=Warning
	RecordNumber=18582
	Keywords=None
	TaskCategory=7
	OpCode=Info
	Message=The speed of processor 5 in group 0 is being limited by system firmware. The processor has been in this reduced performance state for 110 seconds since the last report.

Time	Event
2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67403 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67402 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67401
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0xC03C5B
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67400
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0xC03C97
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67399 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0xC03C5B Privileges:SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

```
Time                      Event
2024-04-30T11:37:49+0530  04/30/2024 11:37:49 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67398
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Logon Information:
                          Logon Type:2
                          Restricted Admin Mode:-
                          Remote Credential Guard:-
                          Virtual Account:No
                          Elevated Token:No

                          Impersonation Level:Impersonation

                          New Logon:
                          Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
                          Account Name:admin
                          Account Domain:DESKTOP-LU7VRCG
                          Logon ID:0xC03C97
                          Linked Logon ID:0xC03C5B
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x90c
                          Process Name:C:\Windows\System32\svchost.exe

                          Network Information:
                          Workstation Name:DESKTOP-LU7VRCG
                          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 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.
```

```
Time                      Event
2024-04-30T11:37:49+0530  04/30/2024 11:37:49 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67397
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Logon Information:
                          Logon Type:2
                          Restricted Admin Mode:-
                          Remote Credential Guard:-
                          Virtual Account:No
                          Elevated Token:Yes

                          Impersonation Level:Impersonation

                          New Logon:
                          Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
                          Account Name:admin
                          Account Domain:DESKTOP-LU7VRCG
                          Logon ID:0xC03C5B
                          Linked Logon ID:0xC03C97
                          Network Account Name:-
                          Network Account Domain:-
                          Logon GUID:{00000000-0000-0000-0000-000000000000}

                          Process Information:
                          Process ID:0x90c
                          Process Name:C:\Windows\System32\svchost.exe

                          Network Information:
                          Workstation Name:DESKTOP-LU7VRCG
                          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 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.
```

Time	Event
2024-04-30T11:37:49+0530	04/30/2024 11:37:49 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67396 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe Network Information: Network Address:127.0.0.1 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.
2024-04-30T11:37:45+0530	04/30/2024 11:37:45 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67395 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:37:45+0530	04/30/2024 11:37:45 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67394 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0
2024-04-30T11:37:43+0530	04/30/2024 11:37:43 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67393 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

```
Time                      Event
2024-04-30T11:37:43+0530  04/30/2024 11:37:43 AM
                          LogName=Security
                          EventCode=5058
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67392
                          Keywords=Audit Success
                          TaskCategory=Other System Events
                          OpCode=Info
                          Message=Key file operation.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Process Information:
                          Process ID:1828
                          Process Creation Time:2024-04-30T06:05:53.200612800Z

                          Cryptographic Parameters:
                          Provider Name:Microsoft Software Key Storage Provider
                          Algorithm Name:UNKNOWN
                          Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD}
                          Key Type:Machine key.

                          Key File Operation Information:
                           File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f
                          -9696-8861d56332c0
                          Operation:Read persisted key from file.
                          Return Code:0x0
2024-04-30T11:37:42+0530  04/30/2024 11:37:42 AM
                          LogName=Security
                          EventCode=5061
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67391
                          Keywords=Audit Success
                          TaskCategory=System Integrity
                          OpCode=Info
                          Message=Cryptographic operation.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          Account Domain:WORKGROUP
                          Logon ID:0x3E7

                          Cryptographic Parameters:
                          Provider Name:Microsoft Software Key Storage Provider
                          Algorithm Name:RSA
                          Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD}
                          Key Type:Machine key.

                          Cryptographic Operation:
                          Operation:Open Key.
                          Return Code:0x0
```

Time	Event
2024-04-30T11:37:42+0530	04/30/2024 11:37:42 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67390 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0
2024-04-30T11:37:40+0530	04/30/2024 11:37:40 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67389 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:37:40+0530	04/30/2024 11:37:40 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67388 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0
2024-04-30T11:37:34+0530	04/30/2024 11:37:34 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67387 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x23b0 Process Name:C:\Windows\System32\LogonUI.exe

Time	Event
2024-04-30T11:37:34+0530	04/30/2024 11:37:34 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67386 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:34+0530	04/30/2024 11:37:34 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67385 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:29+0530	04/30/2024 11:37:29 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67384 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:29+0530	04/30/2024 11:37:29 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67383 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:27+0530	04/30/2024 11:37:27 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67382 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:27+0530	04/30/2024 11:37:27 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67381 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:24+0530	04/30/2024 11:37:24 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67380 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:24+0530	04/30/2024 11:37:24 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67379 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:18+0530	04/30/2024 11:37:18 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67378 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:18+0530	04/30/2024 11:37:18 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67377 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:12+0530	04/30/2024 11:37:12 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67376 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:12+0530	04/30/2024 11:37:12 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67375 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:09+0530	04/30/2024 11:37:09 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67374 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:37:09+0530	04/30/2024 11:37:09 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67373 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:37:06+0530	04/30/2024 11:37:06 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67372 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:06+0530	04/30/2024 11:37:06 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67371 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event

2024-04-30T11:37:03+0530	04/30/2024 11:37:03 AM
	LogName=System
	EventCode=1
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Power-Troubleshooter
	Type=Information
	RecordNumber=18581
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The system has returned from a low power state.
	
	Sleep Time: 2024-04-30T06:05:58.742329600Z
	Wake Time: 2024-04-30T06:06:56.466924100Z
	
	Wake Source: Unknown

2024-04-30T11:37:02+0530	04/30/2024 11:37:02 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67370 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:37:02+0530	04/30/2024 11:37:02 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67369 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

2024-04-30T11:37:02+0530	04/30/2024 11:37:02 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5564
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

2024-04-30T11:37:02+0530	04/30/2024 11:37:02 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5563
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

Time	Event
2024-04-30T11:37:00+0530	04/30/2024 11:37:00 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67368 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:00+0530	04/30/2024 11:37:00 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67367 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:37:00+0530	04/30/2024 11:37:00 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67366 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:37:00+0530	04/30/2024 11:37:00 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67365 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event

2024-04-30T11:36:58+0530	04/30/2024 11:36:58 AM
	LogName=System
	EventCode=566
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18580
	Keywords=None
	TaskCategory=268
	OpCode=Info
	Message=The system session has transitioned from 6 to 8.
	
	Reason WinRT
	
	BootId: 19

2024-04-30T11:36:57+0530	04/30/2024 11:36:57 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67364 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:36:57+0530	04/30/2024 11:36:57 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67363 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

2024-04-30T11:36:57+0530	04/30/2024 11:36:57 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5562
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=105
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18579
	Keywords=None
	TaskCategory=100
	OpCode=Info
	Message=Power source change.

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=566
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18578
	Keywords=None
	TaskCategory=268
	OpCode=Info
	Message=The system session has transitioned from 5 to 6.
	
	Reason SxTransition
	
	BootId: 19

Time	Event

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18577
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=32
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18576
	Keywords=None
	TaskCategory=58
	OpCode=Info
	Message=The bootmgr spent 0 ms waiting for user input.

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=18
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18575
	Keywords=None
	TaskCategory=57
	OpCode=Info
	Message=There are 0x1 boot options on this system.

2024-04-30T11:36:55+0530	04/30/2024 11:36:55 AM
	LogName=System
	EventCode=30
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Boot
	Type=Information
	RecordNumber=18574
	Keywords=None
	TaskCategory=21
	OpCode=Info
	Message=The firmware reported boot metrics.

2024-04-30T11:36:53+0530	04/30/2024 11:36:53 AM
	LogName=System
	EventCode=1
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-General
	Type=Information
	RecordNumber=18573
	Keywords=Time
	TaskCategory=5
	OpCode=Info
	Message=The system time has changed to 2024-04-30T06:06:53.500000000Z from 2024-04-30T06:06:13.878978600Z.
	Time Delta: 39621 ms
	
	Change Reason: System time synchronized with the hardware clock.
	Process: '' (PID 4).
	
	RTC time: 2024-04-30T11:36:53.500000000Z
	Current time zone bias: -330
	RTC time is in UTC: false
	System time was based on RTC time: false

Time	Event

2024-04-30T11:36:13+0530	04/30/2024 11:36:13 AM
	LogName=System
	EventCode=107
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18572
	Keywords=None
	TaskCategory=102
	OpCode=Info
	Message=The system has resumed from sleep.

2024-04-30T11:36:11+0530	04/30/2024 11:36:11 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67362 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:36:11+0530	04/30/2024 11:36:11 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67361 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event

2024-04-30T11:36:11+0530	04/30/2024 11:36:11 AM
	LogName=Application
	EventCode=2
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=IntelDalJhi
	Type=Information
	RecordNumber=5561
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Intel(R) Dynamic Application Loader Host Interface Service has been reset.

2024-04-30T11:36:10+0530	04/30/2024 11:36:10 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5560
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

2024-04-30T11:36:06+0530	04/30/2024 11:36:06 AM
	LogName=System
	EventCode=42
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18571
	Keywords=None
	TaskCategory=64
	OpCode=Info
	Message=The system is entering sleep.
	
	Sleep Reason: Battery

2024-04-30T11:36:05+0530	04/30/2024 11:36:05 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67360 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0

Time	Event
2024-04-30T11:36:05+0530	04/30/2024 11:36:05 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67359 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0
2024-04-30T11:36:03+0530	04/30/2024 11:36:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67358 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:36:03+0530	04/30/2024 11:36:03 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67357 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:36:03+0530	04/30/2024 11:36:03 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67356 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe
2024-04-30T11:36:03+0530	04/30/2024 11:36:03 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67355 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T11:36:03+0530	04/30/2024 11:36:03 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5559
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

Time	Event
2024-04-30T11:36:02+0530	04/30/2024 11:36:02 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67354 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:36:02+0530	04/30/2024 11:36:02 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67353 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:36:01+0530	04/30/2024 11:36:01 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67352 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:36:01+0530	04/30/2024 11:36:01 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67351 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event

2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM
	LogName=System
	EventCode=566
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18570
	Keywords=None
	TaskCategory=268
	OpCode=Info
	Message=The system session has transitioned from 4 to 5.
	
	Reason WinRT
	
	BootId: 19

2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67350 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67349 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67348 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67347 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67346 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:36:00+0530	04/30/2024 11:36:00 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67345 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67344 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67343 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67342 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67341 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67340 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67339 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67338 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67337 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67336 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67335 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

Time	Event
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5061 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67334 Keywords=Audit Success TaskCategory=System Integrity OpCode=Info Message=Cryptographic operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:RSA Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Cryptographic Operation: Operation:Open Key. Return Code:0x0
2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM LogName=Security EventCode=5058 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67333 Keywords=Audit Success TaskCategory=Other System Events OpCode=Info Message=Key file operation. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Process Information: Process ID:1828 Process Creation Time:2024-04-30T06:05:53.200612800Z Cryptographic Parameters: Provider Name:Microsoft Software Key Storage Provider Algorithm Name:UNKNOWN Key Name:{CDE7A1E7-FBDF-4164-AAD4-44B81C9990DD} Key Type:Machine key. Key File Operation Information: File Path: C:\ProgramData\Microsoft\Crypto\RSA\MachineKeys\8d4209b31650b62070ed11816e50c375_bd55c2c6-03b7-4c4f-9696-8861d56332c0 Operation:Read persisted key from file. Return Code:0x0

2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5558
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

Time	Event

2024-04-30T11:35:59+0530	04/30/2024 11:35:59 AM
	LogName=Application
	EventCode=0
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=igccservice
	Type=Information
	RecordNumber=5557
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=PowerEvent handled successfully by the service.

2024-04-30T11:35:58+0530	04/30/2024 11:35:58 AM
	LogName=System
	EventCode=524
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Kernel-Power
	Type=Information
	RecordNumber=18569
	Keywords=None
	TaskCategory=223
	OpCode=Info
	Message=Critical Battery Trigger Met

2024-04-30T11:34:20+0530	04/30/2024 11:34:20 AM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18568
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: Splunkd Service
	Service File Name: E:\Splunk\bin\splunkd.exe service
	Service Type: user mode service
	Service Start Type: auto start
	Service Account: LocalSystem

2024-04-30T11:34:06+0530	04/30/2024 11:34:06 AM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18567
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: SplunkMonitorNoHandle
	Service File Name: system32\DRIVERS\SplunkMonitorNoHandleDrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

Time	Event
2024-04-30T11:34:06+0530	04/30/2024 11:34:06 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67332 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe
2024-04-30T11:34:06+0530	04/30/2024 11:34:06 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67331 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T11:34:04+0530	04/30/2024 11:34:04 AM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18566
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: splknetdrv
	Service File Name: \SystemRoot\system32\DRIVERS\splknetdrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

Time	Event
2024-04-30T11:34:04+0530	04/30/2024 11:34:04 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67330 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T11:34:03+0530	04/30/2024 11:34:03 AM
	LogName=System
	EventCode=7045
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-Service Control Manager
	Type=Information
	RecordNumber=18565
	Keywords=Classic
	TaskCategory=None
	OpCode=The operation completed successfully.
	Message=A service was installed in the system.
	
	Service Name: Splunk Trace Kernel Mode Driver
	Service File Name: \SystemRoot\system32\DRIVERS\splunkdrv.sys
	Service Type: kernel mode driver
	Service Start Type: demand start
	Service Account:

2024-04-30T11:32:08+0530	04/30/2024 11:32:08 AM
	LogName=Application
	EventCode=1040
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=MsiInstaller
	Type=Information
	RecordNumber=5556
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	Message=Beginning a Windows Installer transaction: C:\Users\admin\Downloads\SPLUNK\splunk-9.2.1-78803f08aabb-x64-release (1).msi. Client Process Id: 7564.

2024-04-30T11:31:58+0530	04/30/2024 11:31:58 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18564
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

Time	Event

2024-04-30T11:31:58+0530	04/30/2024 11:31:58 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18563
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:58+0530	04/30/2024 11:31:58 AM
	LogName=System
	EventCode=6001
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18562
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6001 - BSS no beacon after connection. This event is info event which is used for debug purposes only.

2024-04-30T11:31:57+0530	04/30/2024 11:31:57 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18561
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:57+0530	04/30/2024 11:31:57 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18560
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:57+0530	04/30/2024 11:31:57 AM
	LogName=System
	EventCode=6001
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18559
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6001 - BSS no beacon after connection. This event is info event which is used for debug purposes only.

2024-04-30T11:31:56+0530	04/30/2024 11:31:56 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18558
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

Time	Event

2024-04-30T11:31:56+0530	04/30/2024 11:31:56 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18557
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:56+0530	04/30/2024 11:31:56 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18556
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:55+0530	04/30/2024 11:31:55 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18555
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:55+0530	04/30/2024 11:31:55 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18554
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:55+0530	04/30/2024 11:31:55 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18553
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:55+0530	04/30/2024 11:31:55 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18552
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:55+0530	04/30/2024 11:31:55 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18551
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:54+0530	04/30/2024 11:31:54 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18550
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:54+0530	04/30/2024 11:31:54 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18549
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:54+0530	04/30/2024 11:31:54 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18548
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:54+0530	04/30/2024 11:31:54 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18547
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:54+0530	04/30/2024 11:31:54 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18546
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:53+0530	04/30/2024 11:31:53 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18545
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:53+0530	04/30/2024 11:31:53 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18544
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:53+0530	04/30/2024 11:31:53 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18543
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:53+0530	04/30/2024 11:31:53 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18542
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:53+0530	04/30/2024 11:31:53 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18541
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:52+0530	04/30/2024 11:31:52 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18540
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:52+0530	04/30/2024 11:31:52 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18539
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:52+0530	04/30/2024 11:31:52 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18538
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:52+0530	04/30/2024 11:31:52 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18537
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:52+0530	04/30/2024 11:31:52 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18536
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:51+0530	04/30/2024 11:31:51 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18535
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:51+0530	04/30/2024 11:31:51 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18534
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:51+0530	04/30/2024 11:31:51 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18533
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:51+0530	04/30/2024 11:31:51 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18532
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:51+0530	04/30/2024 11:31:51 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18531
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:47+0530	04/30/2024 11:31:47 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18530
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:47+0530	04/30/2024 11:31:47 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18529
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:47+0530	04/30/2024 11:31:47 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18528
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:47+0530	04/30/2024 11:31:47 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18527
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:47+0530	04/30/2024 11:31:47 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18526
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:46+0530	04/30/2024 11:31:46 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18525
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:46+0530	04/30/2024 11:31:46 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18524
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:46+0530	04/30/2024 11:31:46 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18523
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:46+0530	04/30/2024 11:31:46 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18522
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:46+0530	04/30/2024 11:31:46 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18521
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:45+0530	04/30/2024 11:31:45 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18520
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:45+0530	04/30/2024 11:31:45 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18519
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:43+0530	04/30/2024 11:31:43 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18518
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:43+0530	04/30/2024 11:31:43 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18517
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:43+0530	04/30/2024 11:31:43 AM
	LogName=System
	EventCode=6001
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18516
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6001 - BSS no beacon after connection. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:42+0530	04/30/2024 11:31:42 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18515
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:42+0530	04/30/2024 11:31:42 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18514
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:42+0530	04/30/2024 11:31:42 AM
	LogName=System
	EventCode=6001
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18513
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6001 - BSS no beacon after connection. This event is info event which is used for debug purposes only.

2024-04-30T11:31:41+0530	04/30/2024 11:31:41 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18512
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:41+0530	04/30/2024 11:31:41 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18511
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:41+0530	04/30/2024 11:31:41 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18510
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:40+0530	04/30/2024 11:31:40 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18509
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:40+0530	04/30/2024 11:31:40 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18508
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:40+0530	04/30/2024 11:31:40 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18507
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:40+0530	04/30/2024 11:31:40 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18506
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:39+0530	04/30/2024 11:31:39 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18505
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:39+0530	04/30/2024 11:31:39 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18504
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:39+0530	04/30/2024 11:31:39 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18503
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:39+0530	04/30/2024 11:31:39 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18502
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:39+0530	04/30/2024 11:31:39 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18501
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:38+0530	04/30/2024 11:31:38 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18500
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:38+0530	04/30/2024 11:31:38 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18499
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:38+0530	04/30/2024 11:31:38 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18498
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:38+0530	04/30/2024 11:31:38 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18497
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:38+0530	04/30/2024 11:31:38 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18496
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:37+0530	04/30/2024 11:31:37 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18495
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:37+0530	04/30/2024 11:31:37 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18494
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:37+0530	04/30/2024 11:31:37 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18493
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:37+0530	04/30/2024 11:31:37 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18492
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:37+0530	04/30/2024 11:31:37 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18491
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:36+0530	04/30/2024 11:31:36 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18490
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:32+0530	04/30/2024 11:31:32 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18489
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:32+0530	04/30/2024 11:31:32 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18488
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:29+0530	04/30/2024 11:31:29 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18487
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:31:29+0530	04/30/2024 11:31:29 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18486
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

Time	Event

2024-04-30T11:31:26+0530	04/30/2024 11:31:26 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18485
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:26+0530	04/30/2024 11:31:26 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18484
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T11:31:26+0530	04/30/2024 11:31:26 AM
	LogName=System
	EventCode=6000
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Warning
	RecordNumber=18483
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=6000 - BSS missed beacons. This event is info event which is used for debug purposes only.

2024-04-30T11:30:09+0530	04/30/2024 11:30:09 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67329 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:30:09+0530	04/30/2024 11:30:09 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67328 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:30:06+0530	04/30/2024 11:30:06 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67327 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:30:06+0530	04/30/2024 11:30:06 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67326 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67325
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67324
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67323
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67322
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67321
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67320
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event
2024-04-30T11:29:53+0530	04/30/2024 11:29:53 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67319 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:29:53+0530  04/30/2024 11:29:53 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67318
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T11:26:03+0530	04/30/2024 11:26:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67317 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:26:03+0530	04/30/2024 11:26:03 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67316 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:24:11+0530	04/30/2024 11:24:11 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67315 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:24:11+0530	04/30/2024 11:24:11 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67314 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:22:03+0530	04/30/2024 11:22:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67313 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:22:03+0530	04/30/2024 11:22:03 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67312 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:22:03+0530	04/30/2024 11:22:03 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67311 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:22:03+0530	04/30/2024 11:22:03 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67310 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:19:47+0530	04/30/2024 11:19:47 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67309 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe
2024-04-30T11:19:46+0530	04/30/2024 11:19:46 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67308 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T11:19:36+0530	04/30/2024 11:19:36 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67307 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe
2024-04-30T11:19:27+0530	04/30/2024 11:19:27 AM LogName=Security EventCode=4797 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67306 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=An attempt was made to query the existence of a blank password for an account. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F Additional Information: Caller Workstation:DESKTOP-LU7VRCG Target Account Name:WDAGUtilityAccount Target Account Domain:DESKTOP-LU7VRCG
2024-04-30T11:19:27+0530	04/30/2024 11:19:27 AM LogName=Security EventCode=4797 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67305 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=An attempt was made to query the existence of a blank password for an account. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F Additional Information: Caller Workstation:DESKTOP-LU7VRCG Target Account Name:Guest Target Account Domain:DESKTOP-LU7VRCG

Time	Event
2024-04-30T11:19:27+0530	04/30/2024 11:19:27 AM LogName=Security EventCode=4797 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67304 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=An attempt was made to query the existence of a blank password for an account. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F Additional Information: Caller Workstation:DESKTOP-LU7VRCG Target Account Name:DefaultAccount Target Account Domain:DESKTOP-LU7VRCG
2024-04-30T11:19:27+0530	04/30/2024 11:19:27 AM LogName=Security EventCode=4797 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67303 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=An attempt was made to query the existence of a blank password for an account. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F Additional Information: Caller Workstation:DESKTOP-LU7VRCG Target Account Name:Administrator Target Account Domain:DESKTOP-LU7VRCG

2024-04-30T11:19:16+0530	04/30/2024 11:19:16 AM
	LogName=System
	EventCode=24579
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-WPD-ClassInstaller
	Type=Information
	RecordNumber=18479
	Keywords=Classic
	TaskCategory=Driver Post-Install Configuration
	OpCode=None
	Message=Autoplay registration was skipped for device %1.

2024-04-30T11:19:16+0530	04/30/2024 11:19:16 AM
	LogName=System
	EventCode=24577
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-WPD-ClassInstaller
	Type=Information
	RecordNumber=18478
	Keywords=Classic
	TaskCategory=Driver Post-Install Configuration
	OpCode=None
	Message=Media player and imaging program compatibility layers were successfully registered for device %1. Layer bits %2 were requested, layer bits %3 were registered.

Time	Event

2024-04-30T11:19:16+0530	04/30/2024 11:19:16 AM
	LogName=System
	EventCode=24576
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-WPD-ClassInstaller
	Type=Information
	RecordNumber=18477
	Keywords=Classic
	TaskCategory=Driver Installation
	OpCode=None
	Message=Drivers were successfully installed for device WPD Device.

2024-04-30T11:19:16+0530	04/30/2024 11:19:16 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67302 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=System
	EventCode=20003
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-UserPnp
	Type=Information
	RecordNumber=18482
	Keywords=None
	TaskCategory=7005
	OpCode=Info
	Message=Driver Management has concluded the process to add Service WUDFWpdFs for Device Instance ID SWD\WPDBUSENUM\{9EE4DBD3-062C-11EF-8C3F-E86A64BB60E3}#0000000000000400 with the following status: 0.

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=System
	EventCode=10100
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DriverFrameworks-UserMode
	Type=Information
	RecordNumber=18481
	Keywords=None
	TaskCategory=Installation or update of device drivers.
	OpCode=Stop
	Message=The driver package installation has succeeded.

Time	Event

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=System
	EventCode=10002
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DriverFrameworks-UserMode
	Type=Information
	RecordNumber=18480
	Keywords=None
	TaskCategory=Installation or update of device drivers.
	OpCode=Info
	Message=The UMDF service WpdFs (CLSID {112de495-ac4c-46f8-b663-6a4266c53313}) was upgraded. It requires framework version 2.33.0 or higher.

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=System
	EventCode=10000
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=Microsoft-Windows-DriverFrameworks-UserMode
	Type=Information
	RecordNumber=18476
	Keywords=None
	TaskCategory=Installation or update of device drivers.
	OpCode=Start
	Message=A driver package which uses user-mode driver framework version 2.33.0 is being installed on device SWD\WPDBUSENUM\{9EE4DBD3-062C-11EF-8C3F-E86A64BB60E3}#0000000000000400.

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67301 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

Time	Event
2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67300 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                       Event
2024-04-30T11:19:15+0530   04/30/2024 11:19:15 AM
                           LogName=Security
                           EventCode=4624
                           EventType=0
                           ComputerName=DESKTOP-LU7VRCG
                           SourceName=Microsoft Windows security auditing.
                           Type=Information
                           RecordNumber=67299
                           Keywords=Audit Success
                           TaskCategory=Logon
                           OpCode=Info
                           Message=An account was successfully logged on.

                           Subject:
                           Security ID:S-1-5-18
                           Account Name:DESKTOP-LU7VRCG$
                           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:0x3b8
                           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.
```

Time	Event

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67298
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x8044A0
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM
	LogName=Security
	EventCode=4634
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67297
	Keywords=Audit Success
	TaskCategory=Logoff
	OpCode=Info
	Message=An account was logged off.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x8044D3
	
	Logon Type:2
	
	This event is generated when a logon session is destroyed. It may be positively correlated with a logon event using the Logon ID value. Logon IDs are only unique between reboots on the same computer.

2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67296 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info Message=Special privileges assigned to new logon. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x8044A0 Privileges:SeSecurityPrivilege SeTakeOwnershipPrivilege SeLoadDriverPrivilege SeBackupPrivilege SeRestorePrivilege SeDebugPrivilege SeSystemEnvironmentPrivilege SeImpersonatePrivilege SeDelegateSessionUserImpersonatePrivilege

Time	Event
2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67295 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:No Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x8044D3 Linked Logon ID:0x8044A0 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:DESKTOP-LU7VRCG 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 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.

Time	Event
2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67294 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon Information: Logon Type:2 Restricted Admin Mode:- Remote Credential Guard:- Virtual Account:No Elevated Token:Yes Impersonation Level:Impersonation New Logon: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x8044A0 Linked Logon ID:0x8044D3 Network Account Name:- Network Account Domain:- Logon GUID:{00000000-0000-0000-0000-000000000000} Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe Network Information: Workstation Name:DESKTOP-LU7VRCG 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 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.

Time	Event
2024-04-30T11:19:15+0530	04/30/2024 11:19:15 AM LogName=Security EventCode=4648 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67293 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=A logon was attempted using explicit credentials. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 Logon GUID:{00000000-0000-0000-0000-000000000000} Account Whose Credentials Were Used: Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon GUID:{00000000-0000-0000-0000-000000000000} Target Server: Target Server Name:localhost Additional Information:localhost Process Information: Process ID:0x90c Process Name:C:\Windows\System32\svchost.exe Network Information: Network Address:127.0.0.1 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.
2024-04-30T11:19:14+0530	04/30/2024 11:19:14 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67292 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:19:14+0530  04/30/2024 11:19:14 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67291
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T11:19:14+0530	04/30/2024 11:19:14 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67290 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:19:14+0530	04/30/2024 11:19:14 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67289 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:19:11+0530	04/30/2024 11:19:11 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67288 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe
2024-04-30T11:19:11+0530	04/30/2024 11:19:11 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67287 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:19:11+0530	04/30/2024 11:19:11 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67286 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:16:30+0530	04/30/2024 11:16:30 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67285 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ Account Domain:WORKGROUP Logon ID:0x3E7 User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0x2f88 Process Name:C:\Windows\System32\LogonUI.exe
2024-04-30T11:16:30+0530	04/30/2024 11:16:30 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67284 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:16:30+0530  04/30/2024 11:16:30 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67283
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T11:16:28+0530	04/30/2024 11:16:28 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67282 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T11:15:01+0530	04/30/2024 11:15:01 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5555
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T05:45:00Z. Reason: RulesEngine.

2024-04-30T11:14:30+0530	04/30/2024 11:14:30 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5554
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

Time	Event
2024-04-30T11:11:25+0530	04/30/2024 11:11:25 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5553 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

2024-04-30T11:11:23+0530	04/30/2024 11:11:23 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18475
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

Time	Event
2024-04-30T11:11:16+0530	04/30/2024 11:11:16 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67281 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:11:16+0530  04/30/2024 11:11:16 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67280
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event

2024-04-30T11:10:54+0530	04/30/2024 11:10:54 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18474
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:10:54+0530	04/30/2024 11:10:54 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18473
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:10:53+0530	04/30/2024 11:10:53 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18472
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T11:10:53+0530	04/30/2024 11:10:53 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67279 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:10:53+0530	04/30/2024 11:10:53 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67278 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T11:07:40+0530	04/30/2024 11:07:40 AM
	LogName=System
	EventCode=1014
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-20
	SidType=0
	SourceName=Microsoft-Windows-DNS Client Events
	Type=Warning
	RecordNumber=18471
	Keywords=None
	TaskCategory=1014
	OpCode=Info
	Message=Name resolution for the name client.wns.windows.com timed out after none of the configured DNS servers responded. Client PID 4876.

2024-04-30T11:07:22+0530	04/30/2024 11:07:22 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5552 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat.exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:06:22+0530	04/30/2024 11:06:22 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5551 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:05:22+0530	04/30/2024 11:05:22 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5550 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:04:07+0530	04/30/2024 11:04:07 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5549 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:03:10+0530	04/30/2024 11:03:10 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67277 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T11:03:10+0530	04/30/2024 11:03:10 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67276 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T11:03:07+0530	04/30/2024 11:03:07 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5548 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

Time	Event
2024-04-30T11:02:08+0530	04/30/2024 11:02:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67275 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T11:02:08+0530  04/30/2024 11:02:08 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67274
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T11:02:08+0530	04/30/2024 11:02:08 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5547 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

2024-04-30T11:02:02+0530	04/30/2024 11:02:02 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18470
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

Time	Event

2024-04-30T11:01:50+0530	04/30/2024 11:01:50 AM
	LogName=System
	EventCode=1014
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-20
	SidType=0
	SourceName=Microsoft-Windows-DNS Client Events
	Type=Warning
	RecordNumber=18469
	Keywords=None
	TaskCategory=1014
	OpCode=Info
	Message=Name resolution for the name telemetry.influxdata.com timed out after none of the configured DNS servers responded. Client PID 5524.

2024-04-30T11:00:43+0530	04/30/2024 11:00:43 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18468
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T10:59:32+0530	04/30/2024 10:59:32 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18467
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T10:50:40+0530	04/30/2024 10:50:40 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67273 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                     Event
2024-04-30T10:50:40+0530 04/30/2024 10:50:40 AM
                         LogName=Security
                         EventCode=4624
                         EventType=0
                         ComputerName=DESKTOP-LU7VRCG
                         SourceName=Microsoft Windows security auditing.
                         Type=Information
                         RecordNumber=67272
                         Keywords=Audit Success
                         TaskCategory=Logon
                         OpCode=Info
                         Message=An account was successfully logged on.

                         Subject:
                         Security ID:S-1-5-18
                         Account Name:DESKTOP-LU7VRCG$
                         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:0x3b8
                         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.
```

Time	Event
2024-04-30T10:48:09+0530	04/30/2024 10:48:09 AM LogName=Security EventCode=4798 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67271 Keywords=Audit Success TaskCategory=User Account Management OpCode=Info Message=A user's local group membership was enumerated. Subject: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Logon ID:0x14C73F User: Security ID:S-1-5-21-1102696979-4129790392-413580853-1001 Account Name:admin Account Domain:DESKTOP-LU7VRCG Process Information: Process ID:0xba0 Process Name:C:\Windows\explorer.exe

2024-04-30T10:47:36+0530	04/30/2024 10:47:36 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5546
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T05:17:36Z. Reason: RulesEngine.

2024-04-30T10:47:06+0530	04/30/2024 10:47:06 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5545
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

2024-04-30T10:41:09+0530	04/30/2024 10:41:09 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5544
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T05:11:09Z. Reason: RulesEngine.

2024-04-30T10:40:39+0530	04/30/2024 10:40:39 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5543
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

Time	Event

2024-04-30T10:37:04+0530	04/30/2024 10:37:04 AM
	LogName=Application
	EventCode=16384
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5542
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Successfully scheduled Software Protection service for re-start at 2124-04-06T05:07:04Z. Reason: RulesEngine.

2024-04-30T10:36:22+0530	04/30/2024 10:36:22 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67270 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T10:36:22+0530  04/30/2024 10:36:22 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67269
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T10:36:19+0530	04/30/2024 10:36:19 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67268 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T10:36:19+0530	04/30/2024 10:36:19 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67267 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T10:36:14+0530	04/30/2024 10:36:14 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67266
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:14+0530	04/30/2024 10:36:14 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67265
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:14+0530	04/30/2024 10:36:14 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67264
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:14+0530	04/30/2024 10:36:14 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67263
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67262
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67261
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67260
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67259
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67258
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67257
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67256
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67255
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67254
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-21-1102696979-4129790392-413580853-1001
	Account Name:admin
	Account Domain:DESKTOP-LU7VRCG
	Logon ID:0x14C73F
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67253
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67252
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67251
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67250
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67249
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Time	Event

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM
	LogName=Security
	EventCode=5379
	EventType=0
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft Windows security auditing.
	Type=Information
	RecordNumber=67248
	Keywords=Audit Success
	TaskCategory=User Account Management
	OpCode=Info
	Message=Credential Manager credentials were read.
	
	Subject:
	Security ID:S-1-5-18
	Account Name:DESKTOP-LU7VRCG$
	Account Domain:WORKGROUP
	Logon ID:0x3E7
	Read Operation:Enumerate Credentials
	
	This event occurs when a user performs a read operation on stored credentials in Credential Manager.

2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67247 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T10:36:13+0530	04/30/2024 10:36:13 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67246 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event
2024-04-30T10:36:10+0530	04/30/2024 10:36:10 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67245 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T10:36:10+0530	04/30/2024 10:36:10 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67244 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T10:36:10+0530	04/30/2024 10:36:10 AM
	LogName=Application
	EventCode=16394
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Microsoft-Windows-Security-SPP
	Type=Information
	RecordNumber=5541
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=Offline downlevel migration succeeded.

2024-04-30T10:36:08+0530	04/30/2024 10:36:08 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67243 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

Time	Event
2024-04-30T10:36:08+0530	04/30/2024 10:36:08 AM LogName=Security EventCode=4624 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67242 Keywords=Audit Success TaskCategory=Logon OpCode=Info Message=An account was successfully logged on. Subject: Security ID:S-1-5-18 Account Name:DESKTOP-LU7VRCG$ 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:0x3b8 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.

Time	Event

2024-04-30T10:31:24+0530	04/30/2024 10:31:24 AM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18466
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments. This may be the expected behavior for the current provider in the current operating environment as well.

2024-04-30T10:30:35+0530	04/30/2024 10:30:35 AM
	LogName=System
	EventCode=7021
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	SourceName=Netwtw06
	Type=Information
	RecordNumber=18465
	Keywords=Classic
	TaskCategory=None
	OpCode=None
	Message=7021 - Connection telemetry fields and analysis usage

2024-04-30T10:28:55+0530	04/30/2024 10:28:55 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67241 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                      Event
2024-04-30T10:28:55+0530  04/30/2024 10:28:55 AM
                          LogName=Security
                          EventCode=4624
                          EventType=0
                          ComputerName=DESKTOP-LU7VRCG
                          SourceName=Microsoft Windows security auditing.
                          Type=Information
                          RecordNumber=67240
                          Keywords=Audit Success
                          TaskCategory=Logon
                          OpCode=Info
                          Message=An account was successfully logged on.

                          Subject:
                          Security ID:S-1-5-18
                          Account Name:DESKTOP-LU7VRCG$
                          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:0x3b8
                          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.
```

Time	Event
2024-04-30T10:28:49+0530	04/30/2024 10:28:49 AM LogName=Application EventCode=1001 EventType=4 ComputerName=DESKTOP-LU7VRCG User=NOT_TRANSLATED Sid=S-1-5-18 SidType=0 SourceName=Windows Error Reporting Type=Information RecordNumber=5540 Keywords=None TaskCategory=None OpCode=Info Message=Fault bucket , type 0 Event Name: APPCRASH Response: Not available Cab Id: 0 Problem signature: P1: Acrobat.exe P2: 24.2.20687.0 P3: 66172090 P4: Acrobat.dll P5: 24.2.20687.0 P6: 6617208a P7: c0000005 P8: 00000000008fd107 P9: P10: Attached files: \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.1c4def71-94f8-440d-bc73-52af65294a9e.tmp.mdmp \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e17d6ab6-b12e-4b43-b642-241c142e59d1.tmp.WERInternalMetadata.xml WPR_initiated_DiagTrackMiniLogger_OneTrace_User_Logger_20240425_1_EC_0_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.bc6968a2-cb39-4393-9de4-65f4e677419b.tmp.etl WPR_initiated_DiagTrackMiniLogger_WPR System Collector_inject.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.4ddf1e45-c3d4-45b1-97c4-bc51f64bd035.tmp.etl \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.66da97d3-cc6f-4978-b4df-6e1d59ad4ce6.tmp.csv \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.d1ca7f19-2e31-4643-8069-7c3c56a11eab.tmp.txt \\?\C:\Users\admin\AppData\Local\Temp\WER.ef2e3459-9b2d-468a-accd-e9fc992686a6.tmp.appcompat.txt \\?\C:\ProgramData\Microsoft\Windows\WER\Temp\WER.e1f1d8dc-a2ee-42b5-a7d0-1ce7ce165d70.tmp.xml \\?\C:\Windows\SystemTemp\WER.b2a3113f-339b-4b2d-ab20-6d5949678592.tmp.WERDataCollectionStatus.txt These files may be available here: \\?\C:\ProgramData\Microsoft\Windows\WER\ReportQueue\AppCrash_Acrobat. exe_61ebea3cb657c33f68faca4dacb963ec72fd933_b0da3bdd_cab_ccea5822-8bb2-4bd7-94f0-ce085bda0f4e Analysis symbol: Rechecking for solution: 0 Report Id: 6085b3e8-e6c6-4ebd-a658-e1687308219f Report Status: 16396 Hashed bucket: Cab Guid: 0

2024-04-30T10:14:20+0530	04/30/2024 10:14:20 AM
	LogName=System
	EventCode=158
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-19
	SidType=0
	SourceName=Microsoft-Windows-Time-Service
	Type=Information
	RecordNumber=18464
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The time provider 'VMICTimeProvider' has indicated that the current hardware and operating environment is not supported and has stopped. This behavior is expected for VMICTimeProvider on non-HyperV-guest environments. This may be the expected behavior for the current provider in the current operating environment as well.

Time	Event

2024-04-30T10:11:00+0530	04/30/2024 10:11:00 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18463
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T10:11:00+0530	04/30/2024 10:11:00 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18462
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T10:10:59+0530	04/30/2024 10:10:59 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18461
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T10:10:59+0530	04/30/2024 10:10:59 AM LogName=Security EventCode=4672 EventType=0 ComputerName=DESKTOP-LU7VRCG SourceName=Microsoft Windows security auditing. Type=Information RecordNumber=67239 Keywords=Audit Success TaskCategory=Special Logon OpCode=Info 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

```
Time                       Event
2024-04-30T10:10:59+0530   04/30/2024 10:10:59 AM
                           LogName=Security
                           EventCode=4624
                           EventType=0
                           ComputerName=DESKTOP-LU7VRCG
                           SourceName=Microsoft Windows security auditing.
                           Type=Information
                           RecordNumber=67238
                           Keywords=Audit Success
                           TaskCategory=Logon
                           OpCode=Info
                           Message=An account was successfully logged on.

                           Subject:
                           Security ID:S-1-5-18
                           Account Name:DESKTOP-LU7VRCG$
                           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:0x3b8
                           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.
```

Time	Event

2024-04-30T10:01:08+0530	04/30/2024 10:01:08 AM
	LogName=System
	EventCode=10016
	EventType=3
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-21-1102696979-4129790392-413580853-1001
	SidType=0
	SourceName=Microsoft-Windows-DistributedCOM
	Type=Warning
	RecordNumber=18460
	Keywords=Classic
	TaskCategory=None
	OpCode=Info
	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 DESKTOP-LU7VRCG\admin SID (S-1-5-21-1102696979-4129790392-413580853-1001) 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.

2024-04-30T10:00:30+0530	04/30/2024 10:00:30 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18459
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T10:00:30+0530	04/30/2024 10:00:30 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18458
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.

2024-04-30T10:00:29+0530	04/30/2024 10:00:29 AM
	LogName=System
	EventCode=17
	EventType=4
	ComputerName=DESKTOP-LU7VRCG
	User=NOT_TRANSLATED
	Sid=S-1-5-18
	SidType=0
	SourceName=TPM
	Type=Information
	RecordNumber=18457
	Keywords=None
	TaskCategory=None
	OpCode=Info
	Message=The Trusted Platform Module (TPM) hardware failed to execute a TPM command.