Privileged Log-Ons

Privileged Log-Ons

time	_raw
2025-07-30 02:40:18.028	14264,14264,2025-07-30 02:40:18.0283112,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816, DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData":"[""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18""),(""@Name":""SubjectUserName",""#text":""SYSTEM""),(""@Name":""SubjectLogonId"",""#text"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name":""SubjectLogonId"",""#text"":"" 0x3E7""),(""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
	14262,14262,2025-07-30 02:40:17.7983761,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760,
2025-07-30 02:40:17.798	DESKTOP-5A3QNSS,169,Administrative logon,NT AUTHORITY/LOCAL SERVICE (S-1-5-19),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E5,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0, "("EventData":",(""@Name":""SubjectUserSid",""# text":""S-1-5-19""),(""@Name"":""SubjectUserName"","#text":""LOCAL SERVICE"),(""@ Name":""SubjectDomainName",""#text":""NT AUTHORITY""},(""@Name":"SubjectLogonId"","# text":""0x3E5""),(""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege"")}})"
2005 07 20 20 40 47 702	14260,14260,2025-07-30 02:40:17.7939310,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":""S"-1-5-18""},{""@Name":""SubjectUserName"",""#text":""SYSTEM""},{""@Name":""SubjectDomainName",""#text":""SYSTEM""},{""@Name":""SubjectLogonId",""#text"":"" 0x3E7""},{""@Name",""PrivilegeList","#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
025-07-30 02:40:17.793	
2025-07-30 02:40:17.763	14258,14258,2025-07-30 02:40:17.7637053,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QNSS,169,,Administrative logon,Window ManagerDWM-1 (5-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xDA08,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1 ""},{""@Name"":""SubjectUserName"",""#text"":""SubjectUserName"",""#text":""SubjectUserName"",""#text":""SubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName"",""#text":""\$ubjectUserName",""#text":""\$ubjectUserName","#text":""\$ubjectUserName
	14257,14257,2025-07-30 02:40:17.7637041,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804,
2025-07-30 02:40:17.763	DESKTOP-5A3QN5S,169,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xD9EF,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0, "\"EventData"";\""0ata"";\""0ata"";\""0ata"";\""0ata"";\""0atame";\""1ata";\""0atame";\""1ata";\""0atame";\""1ata";\""0atame";\""1ata";\""0atame";\""1ata
2025-07-30 02:40:17.731	14253,14253,2025-07-30 02:40:17.7310828,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760, DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege*, CogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx, Audit success,0,"(""EventData":\""Data":\""@Name":\""SubjectUserSid"\"\"#text"\"\" "S-1-5-18"},\""@Name"\"\"SubjectUserName"\"\""Mtext\"\"\""SYSTEM\"\"\"\"@Name\"\\"\"" SubjectDomainName\",\"\"#text\"\\"\"\"NT AUTHORITY\"\\\"@Name\"\\"\"\"SubjectLogonId\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\



time	_raw
	14251,14251,2025-07-30 02:40:17.7309696,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"" "S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName", ""#text"":""NT AUTHORITY""], (""@Name": ""SubjectLogonId"", ""#text"": ""
	0x3E7""},{""@Name":""PrivilegeList"",""#ext":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecutifyPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeRestorePrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-30 02:40:17.	
	44040 44040 2005 OT 20 004047 4440750 4070 Landhurun Missand Windows Convits Audition Convits 700 004
	14249,14249,2025-07-30 02:40:17.4440759,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,169,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,,False,C:\Users\VM\
	Desktop\Security.evtx.Audit success,0,"=EventData":(""Data":(""@Name"::"SubjectUserSid":,""#
	text":""S-1-5-20"},(""@Name":"SubjectUserName", ""#text":""NETWORK SERVICE"",(""@
	Name":""SubjectDomainName",""#text":""NT AUTHORITY"];{"@Name":""SubjectLogonId",";"#
	text":""0x3E4"";{""@Name":""PrivilegeList"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
25-07-30 02:40:17.	
	14247,14247,2025-07-30 02:40:17.1965929,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityFivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeSebenderinger, SeAssignPrivilege, SeSebenderinger, SeAssignPrivilege, SeSebenderinger, SeAssignPrivilege, SeAssignPrivilege
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"" "S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecutifyPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeRestorePrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]]}}
25-07-30 02:40:17.	
	14106,14106,2025-07-30 02:21:43.8662566,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772,
	DESKTOP-5A3QNSS,167,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeDebugPrivilege, SeD
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name":""SubjectUserName"",""#text":""SYSTEM""),{""@Name":""
	SubjectDomainName",""#text"":"NT AUTHORITY""),{""@Name"::"SubjectLogonId",""#text"":"
	0x3E7*"];""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
25-07-30 02:21:43.	
	44404 44404 2005 OT 20 00:04 40 5004004 4070 Local June Missage Windows Copyright Audition Copyright 704 704
	14104,14104,2025-07-30 02:21:43.5864264,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764,
	DESKTOP-5A3QN5S,167,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,,False,C:\Users\VM\
	Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":[""@Name"":""SubjectUserSid"",""#
	text"":"S-1-5-19""},\f""@Name"":"SubjectUserName"",""#text"":""LOCAL SERVICE""},\f""@
	Name":""SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"::""SubjectLogonId"",""#
	text":""0x3E5""},{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
25-07-30 02:21:43.	
	14102,14102,2025-07-30 02:21:43.5847159,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,820,
	DESKTOP-5A3QN5S,167,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityFivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeSebenderinger, SeAssignPrivilege, SeSebenderinger, SeAssignPrivilege, SeSebenderinger, SeAssignPrivilege, SeAssignPrivilege
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Seimpersonaterrivilege, SebelegateSessionuserimpersonaterrivilege ;Logonid: 0x3E7,,,,,,raise,C:\users\vm\besktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	Security.evix,Audit success,u, { "EventData": { "@name": "SubjectUserSid", "#ext": "S-1-5-18""},{ ""@Name": """S+1-5-18""},{ ""@Name": """
	SubjectDomainName", ""#text"":""NT AUTHORITY""], (""@Name": ""SubjectLogonId"", ""#text"": ""
	0x3E7""},{""@Name":""PrivilegeList"',""#ext":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecutifyPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege" []]
25-07-30 02:21:43.	
	14100,14100,2025-07-30 02:21:43.5565043,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764, DESKTOP-5A3QN5S,167,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList:
	DESKTOP-SA3QNSS,167,,Administrative logon,Window Managen,DWM-1 (S-1-5-90-0-1),, PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xD837,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit
	success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1
	Succession, Leverthala . Data . Whatte . SubjectOstion , #text . 3-1-3-30-0-1
	""},{""@Name"":"SubjectUserName"",""#text"":"DWM-1""),{""@Name"":"SubjectDomainName"" ,""#text"":""Window Manager"',{""@Name"":"SubjectLogonId"",""#text"":"0xD837""},{""@



_time	_raw
025-07-30 02:21:43.556	14099,14099,2025-07-30 02:21:43.5565018,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764, DESKTOP-5A3QN5S,167,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xD827,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0."(""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text"":""S-1-5-90-0-1"],{""@Name"":""SubjectUserName"","#text"":"DWM-1""),{""@Name"" ":""SubjectDomainName"",""#text"":""Window Manager"],{""@Name":""SubjectLogonId"",""#text"" :""0xD827""),{""@Name":""FrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege"}]}}
025-07-30 02:21:43.534	14095,14095,2025-07-30 02:21:43.5348733,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,820, DESKTOP-5A3QN5S,167,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"","#text*"":" "S-1-5-18"),(""@Name"":""SubjectUserSid"","#text*":"" SubjectDomainName","#text*":""NT AUTHORITY"),(""@Name":""SubjectLogonId","#text*":"" 0x3E7""),(""@Name":""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege")]]}
	14093,14093,2025-07-30 02:21:43.5348063,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772, DESKTOP-5A3QN5S,167,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSesionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{"EventData"":{""QName"::""SubjectIoserSid"",""#text"":" "S-1-5-18""},{""@Name"::""SubjectUserName",""#text"::""SYSTEM"},{""@Name"::"" SubjectDomainName"",""#text"::""NT AUTHORITY""},{""@Name"::"SubjectLogonId"",""#text"::"" 0x3E7"*],{""@Name"::""PrivilegeList",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebugPrivilege*)}
025-07-30 02:21:43.534	14091,14091,2025-07-30 02:21:43.1807997,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772, DESKTOP-5A3QN5S,167,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0."{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text"":""S-1-5-20""},{""@Name":""SubjectUserName",""#text"":"NETWORK SERVICE"],{""@ Name"":""SubjectDomainName",""#text"":"NT AUTHORITY"],{""@Name":""SubjectLogonId"",""# text"":"0x3E4""),(""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege")]])}
025-07-30 02:21:42.899	14085,14085,2025-07-30 02:21:42.8995337,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772, DESKTOP-5A3QN5S,167,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x327,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"("EventData"":\""Data"":\""@Name":\""SubjectUserSid"",\"#text"":\" "S-1-5-18""\""@Name"\"\""SubjectUserName"\"\""#text"\"\""SYSTEM"\\\""@Name\"\\"" SubjectDomainName\"\"\"#text\"\\"\""NT AUTHORITY\"\\\\"@Name\"\\\""SubjectLogonId\"\\"\"#text\"\\\"\"" 0x327\"\\\\\\"@Name\"\\"\""Privilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
025-07-30 02:18:02.338	13996,13996,2025-07-30 02:18:02.3382074,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSider","#text"":" S-1-5-18"",{""@Name"":""SubjectUserName",""#text"":"" SubjectDomainName",""#text":""NT AUTHORITY*"),{""@Name":"SubjectLogonId","#text":"" 0x3E7""},{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]]}



_time	_raw
025-07-30 02:18:02.069	13994,13994,2025-07-30 02:18:02.0691750,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776, DESKTOP-5A3QN5S,166,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0,"\"EventData"":\""Data"":\"\"@Name":\""SubjectUserSid"",\"#text"\":\" "S-1-5-18"\",\\"@Name\"\":\"SUbjectUserName\"\"\"#text\"\\"\"SYSTEM\"\\\\"@Name\"\\\"\"\" SubjectDomainName\"\"#text\"\\"\"\"NAUTHORITY\"\\\"@Name\"\\\"\\"SubjectLogonId\"\"\"#text\"\\\"\\"\"\"\ 0x3E7\"\\\\\\"\@Name\"\\\\"\\"\"\\"\\"\\"\\"\\"\\"\\"\\\"\
025-07-30 02:18:02.047	13992,13992,2025-07-30 02:18:02.0479130,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,832, DESKTOP-5A3QN5S,166,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",Logonld: 0xDC7B,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":\"Data":\"G\Name":\"SubjectUserSid"\"#text":\"S-1-5-90-0-1 "",\"\"\\ W\Name\":\"SubjectUser\Name\"\"\",\"\\ W\Name\"\:\"\\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\
025-07-30 02:18:02.047	13991,13991,2025-07-30 02:18:02.0479116,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,832, DESKTOP-5A3QN5S,166,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xDC67,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData":"{""Data"":{""@Name":""SubjectUserSid"",""#text"":""SubjectUserSid"",""#text"":""SubjectUserSid"",""#text"":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege"]}}
025-07-30 02:18:02.022	13987,13987,2025-07-30 02:18:02.0223449,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,832, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData"":\""Data"":\""SubjectUserSid"",""# text"":\""S-1-5-19\""\"\"@Name\":\""SubjectUserName\"\",\"\"\"UNDEXTUSER\VICE\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
025-07-30 02:18:02.016	13985,13985,2025-07-30 02:18:02.0168074,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776, DESKTOP-5A3QN5S,166,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData"":\""Data"":\"@Name":\""SubjectUserSid",\""#text"\"\"""\"S-1-5-18"\),\""@Name"\"\""SUbjectUserSid"\",\""#text\"\"\""\"SUBJectUserSid"\",\""#text\"\"\"\""\"SUBJectUserSid\"\",\""#text\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
025-07-30 02:18:01.718	13983,13983,2025-07-30 02:18:01.7185812,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,832, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0."{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text"":""S-1-5-20""},{\""@Name"":""SubjectUserName"",""#text"":""NETWORK SERVICE"",{\""@Name"":""SubjectLogonId"",""# text"":""S-1-5-20""],{\""@Name"":""SubjectLogonId"",""#text"":""S-1-5-20"",{\""@Name"":""SubjectLogonId"",""#text"":""S-1-5-20"",{\""@Name"":""SubjectLogonId"",""#text"":""S-1-5-20"",{\""@Name":""SubjectLogonId"",""#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"",""#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"",""#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"",""#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"",""#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":""SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId"","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId","#text":""S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20"",{\""@Name":"SubjectLogonId","#text":"S-1-5-20",{\""#text":"SubjectLogonId","#text":"S-1-5-20",{\""#text":"SubjectLogonId","#text":"S-1-5-20",{\""#text":"SubjectLogonId","#text":"S-1-5-20",{\""#text":"SubjectLogonId",\""#text":"S-1-5-20",\""#text":"S-1-5-20",\""#text":"S-1-5-20",\""#text"
2025-07-30 02:18:01.577	13981,13981,2025-07-30 02:18:01.5779108,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData":(""Data":(""@Name":""SubjectUserSici","#text"":" S-1-5-18"),(""@Name":""SubjectUserName","#text"":""SYSTEM"),{""@Name":""SubjectUserSici","#text":"" SubjectDomainName",""#text":""NT AUTHORITY"),{""@Name":"SubjectLognId","#text":"" 0x3E7"*),{""@Name":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegerivilege")}}}



_time	_raw
025-07-30 02:16:04.502	13894,13894,2025-07-30 02:16:04.5024950,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,164,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData":"[""@Name":""SubjectUserSid"",""#text"": "S-1-5-18""),(""@Name":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":"" SubjectDomainName"",""#text":""NT AUTHORITY""),{""@Name":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
1025 07 30 02:46:04 30 0	13892,13892,2025-07-30 02:16:04.2989418,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,164,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"","#text"":" S-1-5-18""),(""@Name"":""SubjectUserName","#text":""SYSTEM""),(""@Name"":"" SubjectDomainName","#text":""NT AUTHORITY"),(""@Name":"SubjectLogonId","#text":"" 0x3E7""),(""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}}
2025-07-30 02:16:04.298 2025-07-30 02:16:04.277	"3890,13890,2025-07-30 02:16:04.2775060,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,164,,Administrative logon,Window ManagerDWM-1 (5-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xDB75,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1 ""},{""@Name"":"SubjectUserName",""#text":""DWM-1""},{""@Name"":"SubjectDomainName"",""#text":""\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-30 02:16:04.277	13889,13889,2025-07-30 02:16:04.2775048,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,164,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",Logonld: 0xDB42,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData"":{\""QName"":""SubjectUserSid"",""# text"":\"S-1-5-90-0-1"\"\{\""@Name"\":\""S-1-5-90-0-1\"\\\"\""@Name"\":\""SbjectUserSid\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-30 02:16:04.257	13885,13885,2025-07-30 02:16:04.2571627,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820, DESKTOP-5A3QN5S,164,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData"";(""@Name"";""SubjectUserSid"",""# text"":"S-1-5-19"");(""@Name":""SubjectUserName"",""#text"":""LOCAL SERVICE");(""@Name"",""#text"":""SubjectUserName"",""#text"":""SeMsbjectUserName"",""#text"":""SeMsbjectUserName"",""#text"":""SeMsbjectUserName"",""#text"":""SeMssignPrimaryTokenPrivilege, SeAuditPrivilege, SeAuditPrivilege, SeAuditPrivilege, SeImpersonatePrivilege";)]}
2025-07-30 02:16:04.246	13883,13883,2025-07-30 02:16:04.2469881,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820, DESKTOP-5A3QN5S,164,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x367,,,,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0,\"\"EventData"":\""Data"":\""@Name":\""SubjectUserSid"",\""#text"":\" "S-1-5-18"\"\""@Name"\":\"SubjectUserName"\",\"#text\"\"\"\"SYSTEM"\\"@Name\"\\"\"" SubjectDomainName\",\"#text\"\\"\"\"NT AUTHORITY\\\\\\\"\"\@Name\"\\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
	13881,13881,2025-07-30 02:16:03.7450018,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820, DESKTOP-5A3QN5S,164,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E4,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text"":""S-1-5-20""),{""@Name"":""SubjectUserName"",""#text"":"NETWORK SERVICE""},{""@Name"":""SubjectUserName"",""#text"":"NETWORK SERVICE""},""# Name"":""SubjectDomainName"","#lext":""NT AUTHORITY"],{""@Name"":"SubjectLogonId"",""# text"":""0x3E4""),{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SelmpersonatePrivilege";}})



_time	_raw
	13877,13877,2025-07-30 02:16:03.5447524,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,836, DESKTOP-5A3QN5S,164,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBentpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""SubjectUserSid"",""#text"":""SubjectDomainName",""SubjectUserName"",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}
025-07-30 02:16:03.544	" 13583,13583,2025-07-30 02:07:46.7943930,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QNSS,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":\""Datata"":\""\"@Name"":\""SubjectUserSid"\",\""#text"":\" S-1-5-18\"),\"\"@Name"\":\""SubjectUserName\",\""#text\":\"" SubjectDomainName\",\""#text\":\"\""NT AUTHORITY\"\),\(\"@Name\"\"\"\@Name\"\":\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-30 02:07:46.625	13581,13581,2025-07-30 02:07:46.6253290,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""@Name"":""SubjectUserSid"",""# text":\""S-1-5-19"{\""@Name"":\""SubjectUserName",\""#text\":\""LOCAL SERVICE\"{\""@Name\"""#text\"\":\""Cotal Service\"\""@Name\"\""#text\"\"\"\""SubjectLogonId\"\"#text\"\"\""SubjectLogonId\"\""#text\"\"\"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeAuditPrivilege, SeImpersonatePrivilege\"\;\"\"
:025-07-30 02:07:46.619	13579,13579,2025-07-30 02:07:46.6199438,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,160,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0."(""EventData":\"[""\@\Name":\"""\"""\""\""\""\""\""\""\""\""\""\""
2025-07-30 02:07:46.583	13577,13577,2025-07-30 02:07:46.5834254,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,160,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xD5FF,,,,,False,C:\Users\\W\Desktop\Security.evtx,Audit success,0,"{""EventData"::{""Okmae"::"SubjectUserSid",,"#text*":"S-1-5-90-0-1 "",,{""@Name":""SubjectUserName"",""#text*":""DWM-1""),{""@Name"::""SubjectDomainName"" ,"#text*":""Vinindow Manager"},","@Name"::"SubjectDogonId", "#text*":""VD5FF""},(""@Name":""SubjectUserName":""SubjectUserName"" ,""#text*":""VD7FF"",(""@Name":""SubjectUserNa
:025-07-30 02:07:46.583	13576,13576,2025-07-30 02:07:46.5834243,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,160,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xD541,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,""EventData"":{""Data"":{"@Name"":"SubjectUserSid"",""# text"":"S-1-5-90-0-1"],{""@Name"\"":"SubjectUserSid"",""# text"":"SubjectUserSid"",""# text"":"SubjectUserSid",""# ("@Name"\"";"SubjectUserSid",""# ("@Name"\"";"SubjectUserSid",""# ("@Name"\"";"SubjectUserSid",""# ("@Name"\"";"SubjectUserSid",""# ("@Name"\"";"SubjectUserSid",""# ("@Name"\";""SubjectUserSid","# ("@Name"\";"SubjectUserSid","# ("@Name"\";"SubjectUserSid","# ("@Name"\";"SubjectUserSid","# ("@Name"\";"SubjectUserSid","# ("@Name"\";"SubjectUserSid","# ("@Name"\";"SubjectUserSid\","# ("@Name"\";""SubjectUserSid\","# ("@Name"\";""SubjectUserSid\","# ("@Name"\";""SubjectUserSid\","# ("@Name\";""SubjectUserSid\","# ("@Name\";""Sub
2025-07-30 02:07:46.581	13572,13572,2025-07-30 02:07:46.5818100,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,804, DESKTOP-5A3QN5S,160,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3ET,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18"",{""@Name"":""SubjectUserSid",""#text":""S-1-5-18"",{""@Name"":""SubjectUserName","""SubjectUserName",""SubjectUserName",""SubjectUserName","""SubjectUserName","""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName","#text":"" SubjectUserName************************************



time	_raw
205 07 20 20 07 40 550	13570,13570,2025-07-30 02:07:46.5792616,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0.x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18"",\""@Name"*:""SubjectUserName","#text":""SYSTEM"",\""@Name"*:""SubjectUserName","#text":"" SubjectDomainName","#text":"NT AUTHORITY"",\""@Name":"SubjectLogonId","#text"::" 0x3E7"",\"@Name":"PrivilegeList"",""#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugerImpersonatePrivilege")]]}
025-07-30 02:07:46.579	
025-07-30 02:07:46.123	13568,13568,2025-07-30 02:07:46.1239345,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,800, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITYINETWORK SERVICE (5-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E4,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData"::{""Data"::{"@Name"::"SubjectUserSid"",""# text"":""St-1-5-20""),{\"@Name"::"SubjectUserName"",""#text"":""NETWORK SERVICE""),{\"@Name":"SubjectLogonId"",""# text"":""SubjectDomainName"",""#text"::"NT AUTHORITY""),{\"@Name"::"SubjectLogonId"",""# text"":"\"0x3E4""),{\"@Name"::"PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""]}}
	13562,13562,2025-07-30 02:07:45.8971359,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\"EventData"":\""Data"":\""\""SySTEM""\""\""Atae"":\""SySTEM""\""\""Atae"\":\""SySTEM"\\""\""Atae"\":\""SySTEM"\\""\""Atae\":\""\""SySTEM"\\""\""Atae\":\""\""SySTEM\"\\""\""Atae\":\""\""\""Atae\"\"\"\""\""Atae\"\"\"\""\""Atae\"\"\"\""\""Atae\"\"\"\""\""\""Atae\"\"\"\""\"\""\""\"\"\"\"\"\"\"\"\"\"\
025-07-30 02:07:45.897	•
025-07-29 18:02:45.989	14360,14360,2025-07-29 18:02:45.9899822,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QNSS,170,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSestorePrivilege, SeLoadDriverPrivilege, SeSestorePrivilege, SeSestorePrivileg
	14351,14351,2025-07-29 17:57:50.7045197,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,170,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\"EventData"":\""Data"":\""SubjectUserSid"",""#text"":\" "S-1-5-18""\""@Name"\""SubjectUserName"\"\""SYSTEM"\\""@Name\"\"\"" SubjectDomainName\"\"\"#text\"\"\"\NT AUTHORITY\"\\"\"@Name\"\\"\"SubjectLogonId\"\"\"#text\"\\"\"\" SeAscurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29 17:57:50.704	•
	14342,14342,2025-07-29 17:50:46.9257321,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,5732, DESKTOP-5A3QN5S,170,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBestorePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"("EventData":",""Data":",(""@Name"::""SubjectIoerSid("",""#text"":""""",""#text"":"""","""",""",""",""",""","","","",""



_time	_raw
	14316,14316,2025-07-29 17:42:22.0102938,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,824,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 17:42:22.010	
	44044 44044 2005 07 00 47 44 40 0704400 4670 Londhunun Microsoft Windows Copyrity Auditing Copyrity 700 700
	14314,14314,2025-07-29 17:41:42.9731489,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,796,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx, Audit success, 0,1"("EventData": (""Data": ([("@ Name": ""SubjectUserSid"", "#text"": "
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
725-07-20 47-44-42 070	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 17:41:42.97	
	14309,14309,2025-07-29 17:40:43.7276013,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text*":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 17:40:43.727	• • • • • • • • • •
	14207 14207 2025 07 20 17:40:24 1207272 4672 LagAlyaya Microsoft Windows Society Auditing Society 720 946
	14307,14307,2025-07-29 17:40:31.1297273,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTctPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"", ""#text": ""NT AUTHORITY"], {""@Name"": "SubjectLogonId"", ""#text": ""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 47:40:04 400	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 17:40:31.129	
	14305,14305,2025-07-29 17:40:28.2054421,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,824,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security evtx, Audit success, 0, "{""EventData"": {""Data"": [""@Name"": "SubjectUserSid"", ""#text"": "
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY"",{""@Name":""SubjectLogonId"",""#text":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 17:40:28.205	
	14204 44204 2025 07 20 47:40:22 7475709 4672 Landburg Missand Missand Missand Audit - County 700 042
	14291,14291,2025-07-29 17:40:23.7175788,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816,
	DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"



_time	_raw
025-07-29 17:40:23.447	14288,14288,2025-07-29 17:40:23.4478835,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,169,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*,Logonld: 0x38CE6,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData":\"\"Data":\"\"Bame":\"SubjectUserSid"\"#text":\"S-1-5-21-3151804214-3226339955-2188200191-1001\"\"\(\mathrew{\text{W}}\)\"SubjectUserSid\"\"\"#text\"\\"\"\\\"\\\"\\\"\\\"\\\"\\\"\\\"\\\
025-07-29 17:40:20.690	14279,14279,2025-07-29 17:40:20.6902073,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816, DESKTOP-5A3QN5S,169,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""@Name":.""SubjectIoserSidi"",""#text*":" "S-1-5-18"},{"@Name":""SubjectUserName",""#text*":""SYSTEM""},{""@Name"::"" SubjectDomainName",""#text*":""NT AUTHORITY""},{""@Name"::""SubjectLogonId",""#text*":"" 0x3E7""},{""@Name"::""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege ", SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
	14277 14277 2025-07-29 17:40:20 6574435 4672 onAlways Microsoft-Windows-Security-Auditing Security 720 816
025-07-29 17:40:20.657	14277,14277,2025-07-29 17:40:20.6574435,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816, DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""Data"":(""@Name":""SubjectUserSidm","#text"":" S-1-5-18""),(""@Name":""SubjectUserName"","#text"":""SvSTEM"),(""@Name":"" SubjectDomainName","#text":""NT AUTHORITY"),(""@Name":"SubjectLogonId","#text":"" 0x3E7""},(""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
025-07-29 17:40:20.645	14275,14275,2025-07-29 17:40:20.6451683,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,169,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"::""SubjectUserSid"",""#text"":" "S-1-5-18"),{""@Name"::""SubjectUserName",""#text"::"SYSTEM"'),{""@Name"::"" SubjectDomainName",""#text"::""NT AUTHORITY"'],{""@Name"::"SubjectLogonId",""#text"::"" 0x3E7"),{""@Name"::"PrivilegeList",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
025.07.20.17.40-20.060	14272,14272,2025-07-29 17:40:20.0699883,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,816, DESKTOP-5A3QN5S,169,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0.x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":" "S-1-5-18"",{""@Name":""SubjectUserName"",""#text*":""SYSTEM"],{""@Name"":""SubjectUserName",""#text*":"" SubjectDomainName"",""#text*":""NT AUTHORITY"',{""@Name":""SubjectLogonId"","#text*":"" 0x3E7""},{""@Name":""PrivilegeList*",""#text*":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebege**")]]}}
2025-07-29 17:40:20.069	14270,14270,2025-07-29 17:40:19.8684703,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,169,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSetakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{\"EventData"":\"\"0x4a"\":\"\"0x4a"\":\"\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0x4a"\":\"\"0



_time	_raw
	14218,14218,2025-07-29 17:37:57.0938636,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,5660, DESKTOP-5A3QN5S,168,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, Cogonid: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text*":""SYSTEM""},{""@Name"":""SubjectDomainName","#text*":""NAUTHORITY""},{""@Name"":""SubjectLogonid"",""#text*":"" 0x3E7""},{""@Name"":""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}}}
2025-07-29 17:37:57	7.093 "
2005 07 20 47/20 5	14172,14172,2025-07-29 17:23:50.6894195,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764, DESKTOP-5A3QN5S,168,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":" "S-1-5-18"),{""@Name":""SubjectUserName"","#text*":"SYSTEM"),{\""@Name":""SubjectDomainName","#text*":" 0x3E7""},{\""@Name":""PrivilegeList*","#text*":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}}}}
2025-07-29 17:23:50	1.689
2025-07-29 17:22:11	14151,14151,2025-07-29 17:22:11.5221156,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764, DESKTOP-5A3QN5S,168,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18"",{\""@Name"":""SubjectUserName"",""#text*":""SYSTEM""},{\""@Name":"""SubjectLogonId"",""#text*":"" SubjectDomainName",""#text*":""NT AUTHORITY""),{\""@Name":\""SubjectLogonId"",\""#text*"\"\"" 0x3E7""},{\""@Name":\""PrivilegeList"",\"\#text*"\"\""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}}
2025-07-29 17:21:58	14149,14149,2025-07-29 17:21:58.7825755,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,820, DESKTOP-5A3QN5S,168,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0.†{""EventData"":{{""@Name"":""SubjectUserSid"",""#text*":"" "S-1-5-18"",{{""@Name"":""SubjectUserName",""#text*":""SYSTEM""},{{""@Name":"" SubjectDomainName",""#text*":""NT AUTHORITY""),{{""@Name"":""SubjectLogonId"",""#text*":"" 0x3E7""},{{""@Name":""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}}
2025-07-29 17:21:58	14147,14147,2025-07-29 17:21:55.5978158,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,764, DESKTOP-5A3QN5S,168,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Loggnld: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":"" "S-1-5-18"",{""@Name"":""SubjectUserName"",""#text*":""SYSTEM""},{""@Name":""" SubjectDomainName"",""#text*":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text*":"" 0x3E7""},{""@Name":""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}}}}
2025 07 20 47:24:50	14133,14133,2025-07-29 17:21:50.4299364,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772, DESKTOP-5A3QN5S,167,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3850C,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-1001""},{""@Name"":"SubjectUserName",""#text"":"VM"),{""@Name"":"SubjectDomainName",""#text":""DESKTOP-5A3QN55""},{""@Name":"SubjectLogonId",""#text":""SubjectDomainName",""#text":""SeSecurityPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"]})}"



time	_tsw
	14128,14128,2025-07-29 17:21:50.2146700,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772, DESKTOP-5A3QN5S,167,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName": "#text": "NT AUTHORITY" \} {""@ Name": "SubjectLogonId", ""#text": ""
	0x3E7""],(""@Name"": ""PrivilegeList"", ""#text"": ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}}
25-07-29 17:21:50.	
	14121,14121,2025-07-29 17:21:46.4434194,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772,
	DESKTOP-5A3QNSS,167,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text*":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text*":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"*]]}
25-07-29 17:21:46.	443 "
	14119,14119,2025-07-29 17:21:46.3846467,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772,
	DESKTOP-5A3QN5S,167,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"::"'SubjectUserName"",""#text"":"'SYSTEM""),(""@Name"::""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
25-07-29 17:21:46.	
	14117,14117,2025-07-29 17:21:46.3789671,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,772,
	DESKTOP-5A3QNSS,167,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcDPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{*"@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"*]]}}
25-07-29 17:21:46.	378
	14114,14114,2025-07-29 17:21:45.7517160,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,820,
	DESKTOP-5A3QN5S,167,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"::"SubjectUserName"",""#text"::"SYSTEM""),{""@Name"::""
	SubjectDomainName",""#text":""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text"":""
	Ox3E7***],{***@Name***:***PrivilegeList**,***#text***:****SASsignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}]}}
25-07-29 17:21:45.	
	14112,14112,2025-07-29 17:21:45.5758868,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,820,
	DESKTOP-5A3QNSS,167,.Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text*":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"



time	_raw
	14052,14052,2025-07-29 17:18:28.7752855,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,832,
	DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7"],{""@Name"".""PrivilegeList"",""#text"".""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}
025-07-29 17:18:28.77	
025-07-25 17.10.20.77	
	14050,14050,2025-07-29 17:18:16.3181938,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776,
	DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""],{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 17:18:16.31	3 "
	14048,14048,2025-07-29 17:18:13.0692272,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,828,
	DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 47.40.40 00	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
025-07-29 17:18:13.06	9
	14042,14042,2025-07-29 17:18:10.0677322,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776,
	DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name": "PrivilegeList"", ""#text": ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeAeschupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 17:18:10.06	
	14023,14023,2025-07-29 17:18:07.9481496,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,, ,
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""]]}}
025-07-29 17:18:07.94	3 "
	14021,14021,2025-07-29 17:18:07.9415716,4672.LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776,
	DESKTOP-5A3QNSS,166,Administrative logon,NT AUTHORITY\SYSTEM (5-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{{""Data"":{{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}



_time	_raw
025-07-29 17:18:05.802	14017,14017,2025-07-29 17:18:05.8024123,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,Logonld: 0x1EE05,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{\text{\
025-07-29 17:18:05.286	14008,14008,2025-07-29 17:18:05.2867496,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{"EventData"":{""Oata"":{"@Name"::""SubjectIoerSidi",""#text*":"" "S-1-5-18""),{""@Name"":"SubjectUserName"",""#text*":""SYSTEM""),{""@Name"::"" SubjectDomainName"",""#text*":""NT AUTHORITY"",{""@Name"*:""SubjectLogonId",""#text*":"" 0x3E7""),{""@Name"*:"PrivilegeList*",""#text*":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege "")]}}
	14006,14006,2025-07-29 17:18:05.2243977,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764,
025-07-29 17:18:05.224	14006;14006;2025-07-29 17:18:05:2243977,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""0*ata"":(""0*ame":""SubjectUserSid"", ""#text*":" "5-1-5-18""),(""@Name":.""SubjectUserName":,""#text*":""SubjectUserSid"","#text*":" SubjectDomainName",","#text*":"NT AUTHORITY"),(""@Name":"SubjectLogonId"","#text*":"" 0x3E7""},\"@Name"::"PrivilegeList"",""#text*":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegeriy]]}}
025-07-29 17:18:05.205	14004,14004,2025-07-29 17:18:05.2051220,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,764, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{\"EventData"*:\"Data"*:\"GName"*:\"SubjectUserSid"*,\"#text*":\" "S-1-5-18"\"\"@Name\":\"SubjectUserSid\",\"#text*":\" "SubjectDomainName\",\"#text\":\"NT AUTHORITY\"\"\"@Name\":\"SubjectLogonId\",\"#text\":\" 0x3E7\"\\\"@Name\":\"PrivilegeList\",\"\"#text\":\"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege\", SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\"\}\}\"
	14001,14001,2025-07-29 17:18:04.6297983,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776, DESKTOP-5A3QN5S,166,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeLoadDriverPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeUndit Success,0,"(""EventData":"(""@Name":""SubjectUserSid"",""#text":"""SySTEM""),(""@Name":""SySTEM""),(""@Name":"""SySTEM""),(""@Name":"""SySTEM""),(""@Name":""""SySTEM""),(""@Name":""SySTEM""),(""@Name":""SySTEM""),(""@Name":""SySTEM""),(""@Name":""SySTEM""),(""@Name":""SySTEM""),(""@Name":""SySTEM"),(""@
2025-07-29 17:18:04.629 2025-07-29 17:18:04.509	" 13999,13999,2025-07-29 17:18:04.5098509,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,728,776, DESKTOP-5A3QN5S,166,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),{""@Name":""SubjectUserName":""text"::""SYSTEM""},{""@Name":""SUbjectUserName":""SUBjectUserSid"",""#text":"" SubjectDomainName"",""#text":""NT AUTHORITY""),{""@Name":""SubjectLogonId",""#text":"" 0x3E7""},{""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegersonatePrivilege, SeDebeger*}]]}



time	_raw
	13950,13950,2025-07-29 17:16:38.2174693,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,772,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name":""SubjectUserName"",""#text":""SYSTEM""),{""@Name":""
	SubjectDomainName", ""#text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"", ""#text"":""
	0x3E7""},{""@Name":""PrivilegeList"",""#ext":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
25-07-29 17:16:38.217	
	13948,13948,2025-07-29 17:16:25.1982067,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,836,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 17:16:25.198	
	13946,13946,2025-07-29 17:16:17.9946343,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	seAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 17:16:17.994	
	13924,13924,2025-07-29 17:16:14.8943980,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,772,
	DESKTOP-5A3QN5S,165,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191
	-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege,
	SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege,
	SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x4F2CC,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit
	success,0,"{""EventData"":[{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-21-
	3151804214-3226339955-2188200191-1001""},{""@Name"":""SubjectUserName"",""#text"":""VM""},{""
	@Name"":""SubjectDomainName"",""#text"":""DESKTOP-5A3QN5S""],{""@Name"":""SubjectLogonId"",
	""#text"":"0x4F2CC""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege,
	SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege,
025-07-29 17:16:14.894	
	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}]" 13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Qhame"":""SubjectUserSid"",""#text"":"
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3F7,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0,"(""EventData"":{\""Data"":{\""@Name"":\""SubjectUserSid\"",\""#text\":\"""\""\""@Name\"":\"""\""\""\""\""\""\""\""\""\""\""\"
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7.,"False. C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid!"",""#text:"": "S-1-5-18"],{""@Name"":""SubjectUserName"":""SubjectUserName"":""SubjectUserName"":""SubjectUserName"":""SubjectUserName"":""SubjectUserName"":""SubjectUserName":""" SubjectDomainName"",""#text:"":""NT AUTHORITY"],{""@Name":""SubjectLogonId"",""#text:"":""
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*,Logonld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":""S-1-5-18"",{""@Name"":""SySTEM"},{""@Name"":""SubjectUserSid",""#text*":""SubjectUserName",""#text*":""SubjectUserName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName**:"""SubjectUsemInName**:"""SubjectUsemInName*
	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\""EventData"":\""\"@Name"":\""SubjectUserSid"\""#text\"\:"\"" SubjectDomainName"\""#text\"\:"\""\""\""\""\""\""\""\""\""\""\""\"
125-07-20 17-18-11 000	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*,Logonld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":""S-1-5-18"",{""@Name"":""SySTEM"},{""@Name"":""SubjectUserSid",""#text*":""SubjectUserName",""#text*":""SubjectUserName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName",""#text*":""SubjectUsemInName**:"""SubjectUsemInName**:"""SubjectUsemInName*
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""@Name"":\""SubjectUserSid",\"#text\"":\""S-1-5-18\""),\""@Name\"":\""SubjectUserName\"",\""#text\"":\""SubjectUserName\"",\""#text\"":\""SubjectUserName\"",\""#text\"":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\",\"\"#text\"\":\""SubjectUogonId\"\",\"\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\""SubjectUogonId\"\",\"#text\"\"\"\"\"SubjectUogonId\"\",\"#text\"\"\"\"\"SubjectUogonId\"\",\"#text\"\"\"\"\"SubjectUogonId\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0,"("EventData":",(""@Name":.""SubjectUserSid"", ""#text"::" "S-1-5-18"",{""@Name":.""SubjectUserName"",""#text"":"SYSTEM""),{""@Name":."" "SubjectDomainName",."#text":."NT AUTHORITY"),{""@Name":.""SubjectLogonId",."#text":."" 0x3E7"",\{""@Name":.""PrivilegeList",.""#text":."SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}} " 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,False,C:Users\VM\Desktop\ Security,evtx,Audit success,0,"(""EventData"":{""Data"":{""QName"":""SubjectUserSid"",""#text"":" "S-1-5-18"",{""@Name":""SubjectUserSid"",""#text"":""SySTEM""),{""@Name":"" SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7"*],{""@Name"*:"PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}} " 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False, C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{"@Name":""SubjectUserSid"",""#text"":" "S-1-5-18"},{"@Name":""SubjectUserName"",""#text":""SySTEM"},{""@Name":""SubjectUserSid"",""#text"":"" SubjectDomainName"",""#text"":"NT AUTHORITY"],{""@Name":"SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}} 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", Logonld: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName"":""SubjectUserSiam",""#text"":""SubjectUserSiam",""#text"":""SubjectUserName":""SubjectUserSiam",""#text"":"" SubjectDomainName"",""#text"":""NT AUTHORITY"]*{""QName":""SubjectLogonld"",""#text"":"" 0x3E7""},{""QName"::"PrivilegeList"",""#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeTakeOwnershipPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}}} 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"("EventData":\""Data":\"\""\"@Name":\""SubjectUserSid"",\""#text"\":\""S-1-5-18"),\"\"@Name\":\""SubjectUserSid\"\",\"#text\"\":\""S-1-5-18"\",\"\"@Name\":\"\""\""\""\""\""\""\""\""\""\""\""\"
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0,"(""EventData"":{\"Data"":{\"@Name"":\"SubjectLoserSid\"",\"#ext*":\"SYSTEM\"),{\"@Name\":\""#ext*":\""SubjectLoserSid\"",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""SubjectLoganId\"\",\"#ext*\":\""\" ux3E7\"\{\"@Name\":\"\"Privilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeSessionUserImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\"\] 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),\"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeCauditPrivilege, SeSecurityPrivilege, SeSec
)25-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, Logonid: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName"":""SubjectUserSid"",""#text"":""SubjectUserSid"",""#text"":""SvSTEM"],{""QName":""SubjectUserSid"",""#text"":""SubjectDomainName",""#text"":""NT AUTHORITY"],{""QName"":""SubjectLogonid"",""#text"":""SubjectDomainName",""#text"":""NT AUTHORITY"],{""QName":"SubjectLogonid"",""#text"":""SubjectDomainName",""#text"":""SubjectIverPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTcbPrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEn
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName":""SubjectUserSid!"",""#text*":""SubjectUserSid!"",""#text*":""SubjectDomainName",""#text*":""NT AUTHORITY"],{""QName":""SubjectLogonId!",""#text*":""SubjectDomainName",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]}}} 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeMackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeRestorePrivilege, SeSionUserImpersonatePrivilege, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"::""Data*"::"SubjectUserSid!",""#text*":""SubjectUserSid!",""#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUser
025-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, Loganld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":[""Qhame":""SubjectUserSid"",""#text"":" "S-1-5-18"),{""@Name":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name":""SubjectUserSid"","#text"::" SubjectDomainName",""#text":""NT AUTHORITY""),{""@Name":""SubjectLogonId","#text"::" 0x3E7""],{""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SelapersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, SeAuditPrivilege, SeDelegateSessionUserImpersonatePrivilege, SeBasckupPrivilege, SeCondDriverPrivilege, SeBasckupPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeLoadDriverPrivilege, SeBasckupPrivilege, SeLoadDriverPrivilege, SeSecurityPrivilege, SeSecurity-Auditing,Security,736,816, DESKTOP-5A3QNSS,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeBasckupPrivilege, SeDelegateSessionUserImpersonatePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeCurity,evtx,Audit success,0,"("EventData"";("Data");(""@Name":""SySTEM"),""@Name":""SySTEM");"#text*":" "S-1-5-18"),(""@Name":""SubjectUserName":""#text*":""SySTEM*"),"@Name":""SySTEM*","#text*":"" SubjectDomainName","#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
)25-07-29 17:16:11.008	13916,13916,2025-07-29 17:16:11.0086269,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName":""SubjectUserSid!"",""#text*":""SubjectUserSid!"",""#text*":""SubjectDomainName",""#text*":""NT AUTHORITY"],{""QName":""SubjectLogonId!",""#text*":""SubjectDomainName",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]}}} 13914,13914,2025-07-29 17:16:10.9805275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816, DESKTOP-5A3QN5S,165,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeMackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeRestorePrivilege, SeSionUserImpersonatePrivilege, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"::""Data*"::"SubjectUserSid!",""#text*":""SubjectUserSid!",""#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUserSid!","#text*":""SubjectUser



_time	_raw
	13908,13908,2025-07-29 17:16:07.9619172,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 17:16:07.961	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
025-07-29 17.16.07.96	
	13906,13906,2025-07-29 17:16:07.8929540,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY"",/(""@Name"::"SubjectLogonId"",""#text"::""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege****]}}}
025-07-29 17:16:07.892	
	13904 13904 2025-07-29 17:16:07 8873637 4672 LogAlways Microsoft Windows Society Auditing Society 736 773
	13904,13904,2025-07-29 17:16:07.8873637,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,772, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,False,C:\Users\\M\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""Data"":{(""@Name"":""SubjectUserSid"", ""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]]}
025-07-29 17:16:07.887	
	13901,13901,2025-07-29 17:16:07.1817640,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,816,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"", ""#text": ""NT AUTHORITY""}, {""@Name"", ""SubjectLogonId"", ""#text": ""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 17:16:07.181	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
020-01-20 11.10.01.10	
	13899,13899,2025-07-29 17:16:07.0663542,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,836,
	DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":" "\$.1.5.18\"\\""@Name\"":""SubjectUserName\"\""#text\"\""@Name\"\"\""@Name\"\"""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege "** }}
025-07-29 17:16:07.066	
	13897,13897,2025-07-29 17:16:06.1891488,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,772, DESKTOP-5A3QN5S,165,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY"",/(""@Name"::"SubjectLogonId"",""#text"::""
	0x3E7""},(""@Name":"'PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
	13850,13850,2025-07-29 17:13:42.8065850,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,3768, DESKTOP-5A3QN5S,164,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"':""SubjectLogonId"",""#text"":""
	0x3E7***],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 17:13:42.80	
	13846,13846,2025-07-29 17:13:42.6739027,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,3768,
	DESKTOP-5A3QN5S,164,.Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),."PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 17:13:42.67	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]} 73 "
20 07 20 17.10.42.07	
	13698,13698,2025-07-29 17:13:24.3908112,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,3768, DESKTOP-5A3QN5S,162,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData":(""@Name"::"SubjectUserSid":,"#text":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]}}
25-07-29 17:13:24.39	0 "
	13674,13674,2025-07-29 17:10:25.0557177,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,824,
	DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege".LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],(""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege";)]}}
25-07-29 17:10:25.05	
	13640,13640,2025-07-29 17:09:51.3126369,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760,
	DESKTOP-5A3QNSS,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}
25-07-29 17:09:51.31	
555.51.51	
	13630,13630,2025-07-29 17:08:13.6304281,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760,
	DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeRackunPrivilege SeRestorePrivilege SeDebugPrivilege SeAuditPrivilege SeSystemEnvironmentPrivilege
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege".LogonId: 0x3E7False.C:\Users\VM\Desktop\
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),{(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectLogonId"",""#text"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""),{(""@Name"":"SubjectLogonId"",""#text"":""



_time	_raw
10025 OZ 20 47-09-04 2	13628,13628,2025-07-29 17:08:01.3081570,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,804, DESKTOP-5A3QN55,161,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeDestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeDestorePrivilege, SeDebugPrivilege, SeDestorePrivilege, SeSystemEnvironmentPrivilege, SeDestorePrivilege, SeDestorePrivilege
025-07-29 17:08:01.3	
	13626,13626,2025-07-29 17:07:55.2711768,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,804, DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),(""@Name"":""SubjectUserName"","#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName",""#text":""NT AUTHORITY"),{""@Name":""SubjectUsegnId"",""#text":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#ext":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege"]]]}}
025-07-29 17:07:55.2	771 "
2025-07-29 17:07:53.6	13614,13614,2025-07-29 17:07:53.6297068,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,804, DESKTOP-5A3QN5S,161,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191 -1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeSesionUserImpersonatePrivilege*,LogonId: 0x3FB99,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-1001""},{{""@Name"":""SubjectUserName"",""#text*":""VM""},{{""@Name"":""SubjectUserName"",""#text*":""VM""},{{""@Name"":""SubjectUserName",""#text*":""VM""},{""@Name"":""SubjectUserName",""#text*":""SubjectLogonId"","#text*":""SubjectLogonId"","#text*":""SubjectLogonId"","#text*":""SubjectLogonId"","#text*":""SubjectLogonId"","#text*":""SubjectLogonId",""#text*":""SubjectLogonId",""#text*":""SubjectLogonId",""#text*":""SubjectLogonId",""#text*":""SubjectLogonId",""#text*":""SubjectLogonId",""#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",","#text*":""SubjectLogonId",",","#text*":""SubjectLogonId",",","#text*":""SubjectLogonId",",,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
025-07-29 17:07:52.8	13607,13607,2025-07-29 17:07:52.8741801,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,800, DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\""EventData"":\""Data":\"\"@Name":"SubjectUserSid"","#text\"":" "S-1-5-18\""},\""@Name":\""SubjectUserName\"",\""#text\"":\""SYSTEM\""},\""@Name\":\""" SubjectDomainName\",\"\"#text\":\"\"NT AUTHORITY\"\",\"\"@Name\":\"\"SubjectLogonId\"\"\"#text\"\":\" 0x3E7\"\",\"\@Name\":\"\"PrivilegeList\"\"\"#text\"\:\"\"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege\"\]}}, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\"\]}}
	13600,13600,2025-07-29 17:07:49.5370111,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760, DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":"(""QName":""SubjectUserSid","#text"":" "S-1-5-18""),(""@Name":"SubjectUserName",""#text":""SYSTEM"),{""@Name":""""""System","#text"":"" SubjectDomainName",""#text"::""NAUTHORITY"",{""@Name":""SubjectLogonld","#text"":"" 0x3E7""),(""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugersonatePrivilege, SeDebugersonatePrivilege, SeDebugerivilege")]}}
2025-07-29 17:07:49.5	



ne	_raw
	13596,13596,2025-07-29 17:07:49.5042164,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,804,
	DESKTOP-5A3QN5S,161,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""Data"":"SubjectUserSid"","";#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"::"SYSTEM""},{""@Name"::"
	SubjectDomainName"",""#text"":""NT AUTHORITY"",\{""@Name"":""SubjectLogonId"",\""#text"":"" 0x3E7"",\{""@Name"":""PrivilegeList"",\""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
5-07-29 17:07:49.50	
	13593,13593,2025-07-29 17:07:48.9982469,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	Selmakapi minggi, Ostadari minggi, Ostad
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":" "\$.1.5.18""!(""@Name":""SubjectUserSid"",""#text"":"" "\$.1.5.18""!(""@Name":""SubjectUserSid"",""#text"":"" "\$.1.5.18""!(""@Name":""SubjectUserSid"",""#text"":"" "\$.1.5.18""!(""@Name":""SubjectUserSid"",""#text"":"" "\$.1.5.18""!(""@Name":"""") "\$.1.5.18""!(""@Name":""""") "\$.1.5.18""!(""@Name":"""""") "\$.1.5.18""!(""@Name":"""""""""""""""""""""""""""""""""""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId",""#text"":""
	0x3E7***),(***@Name***.:**PrivilegeList***, "*#text***.***"SeAssignPrimaryTokenPrivilege, SeTcDPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
07 00 47 07 40 00	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
-07-29 17:07:48.99	3 "
	13591,13591,2025-07-29 17:07:48.8370074,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{\""@Name":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}}
5-07-29 17:07:48.83	
7 07 20 17 10 10 10 10 10	
	13589,13589,2025-07-29 17:07:48.1779496,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,724,760,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}}
-07-29 17:07:48.17	7
	13543,13543,2025-07-29 17:03:02.2064390,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8536,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, Logg, Gold: 0x3E7False, C:Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"::"SYSTEM""},{""@Name"::"
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name": "PrivilegeList"",""#text": ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege [""]}}
-07-29 17:03:02.20	
-01-23 11.03.02.20	
	13535,13535,2025-07-29 17:02:59.9953508,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8536,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"","#text"":""SYSTEM""},{""@Name"":"
	SubjectDomainName"",""#text":""NT AUTHORITY""),(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text":"""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	- Coccounty Inviogo, Se rango wherein invioge, Second Invioge, Sebackup Invioge, Selectioner Invioge, Sebebug Fininge
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}



time	_raw
	13533,13533,2025-07-29 16:50:57.8706570,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4668, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""},;""@Name"":""
	SubjectDomainName"",""#text":""NT AUTHORITY""),{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""],(""@Name"::""PrivilegeList"', ""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
5-07-29 16:50:57.8	70 "
	13531,13531,2025-07-29 16:50:56.2963149,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4668,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{\""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectionmainName:","#text"::"NT AUTHORITY":\frac{1}{2}\text{@Name:":\frac{1}{2}\text{Uthording}}\text{ording}\text{":""}
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
25-07-29 16:50:56.2	96 "
	13529,13529,2025-07-29 16:48:08.6895842,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,2852,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"".""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"".""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}}
25-07-29 16:48:08.6	
	13527,13527,2025-07-29 16:48:08.5702123,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,2852, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]}}
25-07-29 16:48:08.5	70
	13525,13525,2025-07-29 16:42:45.0851757,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3068,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,1008,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"" :""S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
25-07-29 16:42:45.0	85 "
	13523,13523,2025-07-29 16:41:22.5301358,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3688,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":"
	SubjectDomainName"", "#text": ""T AUTHORITY""}, (""@Name"", ""SubjectLogonId"", ""#text"", ""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}



time	_raw
	13521,13521,2025-07-29 16:41:22.3579511,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRotorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
25-07-29 16:41:22.3	57 "
	13519,13519,2025-07-29 16:41:20.2922382,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3068,
	DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"",""NT AUTHORITY""},(""@Name"",'"SubjectLogonId"",""#text"",""
	0x3E7""],[""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeSecurityPrivilege, SeTakeOwnersnipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}}
25-07-29 16:41:20.2	
3 20 10 1. 20. 2	
	13517,13517,2025-07-29 16:39:20.4757827,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3068, DESKTOP-5A3QN5S,160,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3877False, C:\Users\VM\Desktop\
	Security.evtx, Audit success, 0, "(""EventData": (""Data": (""@ Name": ""SubjectUserSid": "#text"":
	"S-1-5-18""}{""@Name"::""SubjectUserName"",""#text"":""SYSTEM""},[""@Name"":""
	SubjectDomainName"",""#text*":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text*":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 16:39:20.4	75
	13515,13515,2025-07-29 16:39:19.2637233,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""),{""@Name"":"
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{"" @ Name"":""SubjectLogonId", ""#text"":""
	0x3E7""},{""@Name"":"PrivilegeList"","#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 16:39:19.2	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}} 33 "
0 .0.00.10.2	
	13513,13513,2025-07-29 16:22:09.9123309,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4416, DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, Logonia: 0x3E7False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"::(""Data"::(""@Name"::""SubjectUserSid"",""#text"::
	"S-1-5-18""},[""@Name"::"SubjectUserName"","#text"::"SYSTEM""},[""@Name"::"
	SubjectDomainName"",""#text"":"NT AUTHORITY""},(""@Name"":"SubjectLogonId"",""#text"":"
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 16:22:09.9	12 "
	13511,13511,2025-07-29 16:13:04.0100523,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""IT AUTHORITY""},{""@Name"";""SubjectLogonId"",""#text"";""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	10.0 % 0.0 % 0.7 %
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}}



_time	_raw
	13509,13509,2025-07-29 16:06:06.2490413,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6228,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 16:06:06.249	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
020 07 20 10:00:00:210	
	13507,13507,2025-07-29 16:06:06.0732821,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4876,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeSecuntyPrivilege, SeSestantPrivilege, SeSestantPrivilege, SeCoalDriverPrivilege, SeSestantPrivilege, SeSe
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, Logondt: 0x3E7,,False, C:\Users\VM\personatePrivilege\(\)
	Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},[*"@Name":.""SubjectUserName"", "#text*":.""SYSTEM""},[*"@Name"":""
	SubjectDomainName", "#text": ""NT AUTHORITY"), ""@Name": "SubjectLogonId", ""#text": ""
	0x3E7""},(""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 16:06:06.073	"
	13505,13505,2025-07-29 16:06:03.8430288,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4876,
	DESKTOP-5A3QNSS,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]}}
025-07-29 16:06:03.843	
	13503,13503,2025-07-29 16:00:01.6480503,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{\""Bata"":{\""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY"],{""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 16:00:01.648	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
020-01-23 10.00.01.040	
	13501,13501,2025-07-29 16:00:01.3892313,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcDPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeSecurityPrivilege, SeSecurityPrivileg
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),[*"@Name"":""
	SubjectDomainName",""#text"":"NT AUTHORITY""),(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege**** }
025-07-29 16:00:01.389	
	13499,13499,2025-07-29 15:38:16.6434316,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,1912,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY""),{""@Name"::"SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name":"PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
	13497,13497,2025-07-29 15:38:15.3242692,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,1912,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"::"SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name":"PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
025-07-29 15:38:15.3	24 "
	13495,13495,2025-07-29 15:38:15.0145347,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,1912,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 45 00 := =	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}
025-07-29 15:38:15.0	14 "
	13493,13493,2025-07-29 15:15:57.1915039,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],(""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY"",\[""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""],(""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 15:15:57.1	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
020-07-29 13.13.37.1	
	13491,13491,2025-07-29 15:11:56.2291756,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,7552,
	DESKTOP-5A3QN5S,159,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx, Audit success, 0, "(""EventData"": (""Data"": [(""@Name"": ""SubjectUserSid"", ""#text"": ""
	"S-1-5-18""},[""@Name":""SubjectUserName"",""#kext":"SYSTEM""},[""@Name":"
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7"],{""@Name"":"PfrivilegeList"",""#text":"'SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"";}]}}
025-07-29 15:11:56.2	
	13489,13489,2025-07-29 15:11:55.3940792,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,7552,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{"EventData"":{""Data"":{""@Name"::"SubjectUserSid": "#text**:":
	"S-1-5-18""),(""@Name"::"'SubjectUserName",""#text"":"'SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 15:11:55.3	94 "
	13487,13487,2025-07-29 15:08:07.3762048,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4592,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}



_time	_raw
	13485,13485,2025-07-29 15:00:06.5174751,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8236,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 15:00:06.51	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
J25-07-29 15.00.00.51	
	13483,13483,2025-07-29 15:00:06.0898485,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8236,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY"",/("@Name"::"SubjectLogonId"",""#text":""
	0x3E7"*,("@Name":"PrivilegeList",""#ext":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege***********************************
025-07-29 15:00:06.08	
	13481,13481,2025-07-29 14:00:17.6301837,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,2844, DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"
	SubjectDomainName",""#text"*:""NT AUTHORITY""),{""@Name"":"'SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 14:00:17.63) <u>"</u>
	13479,13479,2025-07-29 14:00:12.8339966,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 14:00:12.83	3 "
	13477,13477,2025-07-29 13:57:34.6838910,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6464,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{\""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
00E 07 00 40.E7.04 00	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 13:57:34.68	
	13475,13475,2025-07-29 13:43:14.5806127,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,1008,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text""
	:""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name":""
	SubjectDomainName"",""#text":""NT AUTHORITY""},{""@Name"",""SubjectLogonId"",""#text"";"
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}



	13469,13469,2025-07-29 13:30:46.7628012,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8848, DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SebackupPrivilege, SekestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	Columnary and Dair illand Consider Consider Localization are noted Dair illand II a sould 10/257 Folio C/Ulland I/M/Doubton
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name"":""SubjectUserName"",""#text":""SYSTEM""),(""@Name":""
	SubjectDomainName", ""#text":"NT AUTHORITY""}, {""@Name":"SubjectLogonId"", ""#text"":"
	0x3E7"', (""@Name"": "PrivilegeList"', ""#text": "SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}}}}
025-07-29 13:30:46.762	·
	13467,13467,2025-07-29 13:12:43.9686243,4672,LoaAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
05 05 05 15 15 15	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]]}}
025-07-29 13:12:43.968	•
	13465,13465,2025-07-29 13:05:04.6639945,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,5136,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 40 05 04 000	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 13:05:04.663	•
	13463,13463,2025-07-29 12:42:45.0756568,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6416,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security, evtx, Audit success, 0,"{""EventData"": (""Data"": [(""@ Name"": """UspictUserSid"", ""#text"": "
	"S-1-5-18""),(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"", ""#text"": ""NT AUTHORITY""), {""@ Name": ""SubjectLogonId"", ""#text"": ""
	0x3E7""},(""@Name"",""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 12:42:45.075	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
12.42.43.0/5	
	13461,13461,2025-07-29 12:42:44.9163925,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6416,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx, Audit success,0," (""EventData"": (""Data"": [(""@Name"": ""SubjectUserSid"", ""#text"": """: """ [""@Name"": """ [""@Name": ""#text"": """ [""@Name": ""#text"": """ [""@Name": ""#text"": """ [""@Name": ""#text": """ [""@Name": """ [""@Name": ""#text": """ [""@Name": """ [""@Name": """ ["" [""@Name": """ [""@Name": """ [""@Name": """ [""@Name": """ ["" [""@Name": """ [""@Name": """ [""@Name": """ [""@Name": """ ["" ["" [""]@Name": """ ["" ["" [""]@Name": """ [""]@Name": """ ["" [""]@Name": """ [""]@Name": """]
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	Ox3E7""],{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-29 12:42:44.916	1
	42450 42450 2005 07 20 4240.57 0070540 4070 Levalueur Micros of Mi
	13459,13459,2025-07-29 12:40:57.9970548,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,7464,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"Privilege List:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	Security.evix,Audit success,u, { "EventData" :{ "Data" :[{"@Name" : "SubjectUserSid", "#text" : " "S-1-5-18""},[""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],[""@Name"":""
	SubjectDomainName", ""#text":"NT AUTHORITY""},{""@Name":"SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}



ime	_raw
	13457,13457,2025-07-29 12:05:32.7726764,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QNSS,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],[""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
5-07-29 12:05:32.7	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}} 72 "
	13455,13455,2025-07-29 12:05:32.5370448,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 12:05:32.5	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
:J-U1-Z8 1Z:U5:3Z.5	
	13453,13453,2025-07-29 12:05:29.4452067,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,2288,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList: SAAssign Primary Tylog Privilege ST-SP Privilege SeSasy in the Privilege ST-St-St-Ownership Privilege St-St-Ownership Privilege St-Ownership Privilege S
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx, Audit success, 1008, "{""EventData"":{{""@Name"":""SubjectUserSid"", ""#text""
	:""S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 12:05:29.4	45 "
	13451,13451,2025-07-29 11:42:28.4935898,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#ext"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*
25-07-29 11:42:28.4	
	13449,13449,2025-07-29 11:42:28.1947396,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QNSS,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""},[""@Name"".""PrivilegeList"",""#text"".""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
5-07-29 11:42:28.1	
	13447,13447,2025-07-29 11:12:29.8711250,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3672, DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", JegonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":((""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugBrivilege**]}}



ime	_raw
	13445,13445,2025-07-29 10:57:20.3322422,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3328, DESKTOP-5A3QN5S,159,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),[""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 10:57:20.332	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
20-07-25 10.07.20.002	10 LIG 10 LIG 20 C C C C C C C C C C C C C C C C C C
	13443,13443,2025-07-29 10:57:09.7282238,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3328, DESKTOP-5A3QN5S,158,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	, ,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,,
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelateIntegateSessionUserImpersonatePrivilege, Logo, Gody, SelmpersonatePrivilege, SeDelateSessionUserImpersonatePrivilege, Logo, Gody, SelmpersonatePrivilege, SeDelateSessionUserImpersonatePrivilege, Logo, Gody, SelmpersonatePrivilege, SeDelateSessionUserImpersonatePrivilege, SeDelateSessionUserI
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name":""
	SubjectDomainName"" ""#text"::"NT AUTHORITY"" "@Name":""SubjectLogonid"", ""#text"::""
	0x3E7"",[""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
25-07-29 10:57:09.728	#
	13433,13433,2025-07-29 10:56:56.0595586,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3328,
	DESKTOP-5A3QN5S,158Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\\M\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 10:56:56.059	
	13417,13417,2025-07-29 10:44:08.4791714,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8824,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
OF 07 00 40-44-00 470	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}}
25-07-29 10:44:08.479	
	13415,13415,2025-07-29 10:42:24.3797779,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8824,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "\$-1-5-18""\/""@Name"":""Upject UserName"":""#text"":""SYSTEM""\/""@Name"":""
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name":""SubjectLogonId"",""#text"":""
	Ox3E7""},{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	OXACT IN SWanie - Prinsigetais , max - Sensaigh initiary locality to the Commission of the Commission
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"; }}}
25-07-29 10:42:24.379	" " " " " " " " " " " " " " " " " " "
	13413,13413,2025-07-29 10:42:24.1301855,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8824,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx.Audit success.0.(""EventData":(""Data"::[("@Name:":"SubjectUserSid":",";;;; #text*":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""



time	_raw
	13411,13411,2025-07-29 10:12:48.2445485,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#ext"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#ext"":""
	0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDeougrifvilege SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege" SeXuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege" SeXuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege SeXuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege SeXuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege SeXuditPrivilege, SeXuditPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege SeXuditPrivilege, SeXuditPrivileg
025-07-29 10:12:48.24	
020 07 20 70.72.70.27	
	13409,13409,2025-07-29 09:42:50.4769045,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6116,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, Logold: 0x3E7,,False,C:Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""],{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 09:42:50.476	
	13407,13407,2025-07-29 09:42:38.9878859,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6116,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 00 40 00 00	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}}
025-07-29 09:42:38.987	
	13405,13405,2025-07-29 09:42:38.7865296,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6116,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]}}
025-07-29 09:42:38.786	
020 07 20 00.42.00.700	
	13403,13403,2025-07-29 09:30:40.1491359,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,158,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTctPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""),(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege!"\}}
025-07-29 09:30:40.149	
	13284,13284,2025-07-29 09:29:06.5239991,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name":""
	SubjectDomainName",""#text":""NT AUTHORITY""),{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7*"],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



me	_raw
	13282,13282,2025-07-29 09:29:04.9322130,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 09:29:04.93	2 "
	13280,13280,2025-07-29 09:27:52.6605744,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,5140,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]}}
25-07-29 09:27:52.66	0 "
	12365 12365 2025 07 20 00:27:45 7996044 4573 LogAlyana Microsoft Windows Consults Auditing Consults 700 0700
	13265,13265,2025-07-29 09:27:45.7886041,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8728,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx.Audit success,0,";(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{\""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege
25-07-29 09:27:45.78	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
25-07-29 09:27:45.78	0
	13263,13263,2025-07-29 09:27:44.7655391,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8728,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
25-07-29 09:27:44.76	5 "
	43364 43364 3035 07 30 00:33:43 4454475 4673 LegAlveyre Microsoft Windows Society Auditing Society 736 4649
	13261,13261,2025-07-29 09:22:13.1151475,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4648, DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	Sebackuperivilege, Serestoreprivilege, Sebebugprivilege, SeAuditPrivilege, SeSystemenvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":" "\$ 1.5.18""\ (""@Name"":""\$ ubject learName"" ""#text"":""\$ Y\$TEM""\ (""@Name"":""
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":"" SubjectDomainName"",""#text"::""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":""
	SubjectDomainVarine , #lext : N1 AOTHORTTY);{ @Name : SubjectDogniid , #lext : 0x3E7"];{""@Name"":""PrivilegeList"",""#lext"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebuqPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeDebugP
5-07-29 09:22:13.11	
.0-01-23 03.22.13.11	
	13259,13259,2025-07-29 09:22:12.9475315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,4648,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	CoPoolum Privillago, CoPootora Privillago, CoPoblum Privillago, CoA del Privillago, CoCootora Francisco de Privillago
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,*{""EventData"":(""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,*{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},[""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],[""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""],[""@Name"":""SubjectLogonId"",""#text"":""



time	_raw
	13257,13257,2025-07-29 09:16:19.1977315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""@Name"":(""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
025-07-29 09:16:19.197	, seAuditrivillege, seSystemEnvironimentrivillege, seimpersonaterrivillege, seDelegateSessionOserimpersonaterrivillege }}}}
020 07 20 00.10.10.10.	10055 10055 005 07 00 00 1000 1000 1000
	13255,13255,2025-07-29 09:13:22.0610633,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", Logondi: 0x3E7,,False,C:\Users\UMNDektop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"),{""@Name":""SubjectUserName": ""#tex*1:""SYSTEM""},{""@Name"":""
	SubjectDomainName", ""#text"": ""NT AUTHORITY""},{""@Name": "SubjectLogonId"", ""#text"": ""
	0x3E7"",[""@Name":""PrivilegeList", ""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
025-07-29 09:13:22.061	
	13253,13253,2025-07-29 09:07:08.6985275,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x35F,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 09:07:08.698	
	13250,13250,2025-07-29 08:05:56.1159351,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8340,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 00:05:50 115	, seAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
025-07-29 08:05:56.115	
	13248,13248,2025-07-29 08:04:55.7091214,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,6960,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""Septional success,0,"(""EventData"":(""@Name"":""Septional success,0,"(""EventData"":(""@Name"":""Septional success,0,"(""EventData"":""Septional success,0,"(""EventData"":""Septional success,0,"(""EventData"":""Septional success,0,"(""EventData"":""":""Septional success,0,"(""EventData"":""":""":""":""":""":""":""":""":""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"",""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}}
025-07-29 08:04:55.709	, Johann Ittioge, Jeogstein Livitorin Ittioge, Jennyersonater Itviege, Jedesgate Jessen it Jensen in Jensen at Filvinge
0. 20 00.04.00.700	4224C 4224C 2005 07 20 00:04:02 7004704 4070 Levalueur Micros - 4: Windows - 4: Win
	13246,13246,2025-07-29 08:04:22.7864784,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,5432,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":"SubjectUserName"",""#text"::"SYSTEM""),{""@Name"::""
	SubjectDomainName"" ""#text"" ""NT ALITHORITY"" { ""@Name" ""SubjectLogopId" ""#text"" ""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"'PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege.
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



_time	_raw
	13244,13244,2025-07-29 07:50:22.0581205,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,2868,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7"],{""@Name"".""PrivilegeList"",""#text"".""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 07:50:22.05	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
020 07 20 07 100.22.000	
	13242,13242,2025-07-29 07:49:36.9649253,4672_LogAlways,Microsoft-Windows-Security-Auditing,Security,736,1620,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,False,C:\Users\UMDesktop\
	Security.evtx, Audit success, 0, "{""EventData"": [""Data"": [""@Name"": "SubjectUserSid"", ""#text"": "
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"::""SubjectLogonId"",""#text"":""
	0x3E7"",("@Name"::"PrivilegeList",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 07:49:36.96	
	13240,13240,2025-07-29 07:48:38.3536756,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,1620,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssianPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"", ""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":"
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":"'SubjectLogonId"",""#text"":""
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
2025-07-29 07:48:38.35	1 -
	13238,13238,2025-07-29 07:43:08.3976047,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,156,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 07:43:08.39	, »
	13206,13206,2025-07-29 07:42:17.7935968,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8532,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{\""Data"":{\""@Name"":\""SubjectUserSid"",""#text"":\"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},{\"@Name"":"\SubjectLogonId\"",\"#text\":\"
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege
00E 07 00 07:40:47 70:	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 07:42:17.79	
	13204,13204,2025-07-29 07:42:15.2927751,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,8532,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":["""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{\"@Name"":"\SubjectLogonId\"",\"#text\"":\"
	0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}



ime	_raw
	13202,13202,2025-07-29 07:42:11.9400747,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),[""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
25-07-29 07:42:11.	340
	13199,13199,2025-07-29 07:31:53.1899999,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 07:31:53.	189
	13107 13107 2025.07-20 07-31/41 7371024 4672 Londburgs Microsoft Windows Society Audition Society 725 5052
	13197,13197,2025-07-29 07:31:41.7371924,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,5952, DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*(LogonId: 0x3E7,,False,C:USers\VM\Desktop\
	Security.evtx.Audit success.0.1(""EventData":1(""Data":1(""@ Name"::""SubjectUserSid": ""#text"::"
	"S-1-5-18"},("@Name":"SubjectUserName": ""#SYTEM"),("@Name": ""
	SubjectDomainName", ""#text": ""NT AUTHORITY""}, (*"@Name": "SubjectLogonId"", ""#text"": ""
	Ox3E7*"\{""@\Name":"PrivilegeList"; "#text"::""SAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecutifyPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeRestorePrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege" []])
25-07-29 07:31:41.	
20 01 20 01.01.41.	
	13195,13195,2025-07-29 07:31:31.2709309,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 07:31:31.	270 "
	13193,13193,2025-07-29 07:31:29.1701863,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-SA3QNSS,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0, "(""EventData"": (""Data") [""@Name": "SubjectUserSid" "#text": "
	"S-1-5-18"},("@Name": "SubjectUserName": ""Hext": "SYSTEM"),("@Name": ""
	SubjectDomainName",""#text":""NT AUTHORITY"];\"@Name":""SubjectLogonid",""#text":""
	0x3E7*"], [*"@Name*": "PrivilegeList", ""#text*": "SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
25-07-29 07:31:29.	
	13191,13191,2025-07-29 07:26:40.7817511,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3592,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":"
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}}



_time	_raw
2025-07-29 07:24:21.070	13189,13189,2025-07-29 07:24:21.0704213,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820, DESKTOP-5A3QN5S,155,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBeckupPrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0,"(""EventData"":(""@Name":""SubjectUserSidi"",""#text"":" "S-1-5-18""},\""@Name":""SubjectUserName",""#text":""SySTEM"},\\"@Name":""SubjectLogonId",""#text":"" SubjectDomainName",""#text"::"NT AUTHORITY"'),\\\"@Name":"SubjectLogonId",""#text"::"" 0x3E7""},\\\\"@Name"::"PrivilegeList"",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
.025-07-29 07.24.21.070	13169,13169,2025-07-29 07:22:35.2026899,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""QName":""SubjectUserSid"",""#text"":" "\$-1-5-18""),{""@Name":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name":"""SubjectUserName"",""#text"":""SUbjectDomainName",""#text":""NT AUTHORITY"),{""@Name":""SubjectLogonId",,"#text"":"" 0x3E7""),{""@Name":""PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTebPrivilege, SeSecutityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBeackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege"]]]}
025-07-29 07:22:35.202	
2025-07-29 07:22:14.222	13165,13165,2025-07-29 07:22:14.2228258,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,155,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,False,C:Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name":""SubjectUserName"";""#text"":""Sv-1-5-18""],{""@Name"":""SubjectUserName"";""#text"":""SubjectDomainName",""#text*":""NT AUTHORITY""},(""@Name":""SubjectLogonId"",""#text*":""0x3E7""),(""@Name":""PrivilegeList"",""#text*":""SeAssignPrimaryTokenPrivilege, SeTorPrivilege, SeBebugPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege", SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege""}}}}
025-07-29 07:22:08.140	13159,13159,2025-07-29 07:22:08.1408633,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,3540, DESKTOP-5A3QN5S,155,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,"Privilege,Ist: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeSestorePrivilege, SeSestorePrivilege, SeImpersonatePrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x199241,,,,,False,C:Ubsers/VM\Desktop\Security.evtx,Audit success,0."(""EventData"":{"Data"":{"QName":""SubjectUserSid", "#text*":""S-1-5-21-3151804214-3226339955-2188200191-1001""),{""QName":""SubjectUserName"","#text*":""VM""},{""QName":""SubjectUserName"",""#text*":""VM""},{""QName":""SubjectUserName":"SubjectLogonId", "#text*":""VM""},{""QName":""SubjectLogonId", "#text*":""SubjectLogonId", "#text*":""SubjectLogonId", "#text*":""SeSecurityPrivilege, SeSestorePrivilege, SeDebugPrivilege, SeSestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege*
025-07-29 07:21:42.582	13154,13154,2025-07-29 07:21:42.5827153,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776, DESKTOP-5A3QN5S,155,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"":""SubjectUserSidi"",""#text"":"" "S-1-5-18"},{""@Name":""SubjectUserName",""#text":""SYSTEM"},{""@Name":""SubjectLogonId",""#text":"" SubjectDomainName",""#text"::"NT AUTHORITY""),{""@Name"::"SubjectLogonId",""#text"::"" 0x3E7""},{""@Name"::"PrivilegeList"",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege seSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege seAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege"]]}}
2025-07-29 07:20:43.411	13149,13149,2025-07-29 07:20:43.4110661,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820, DESKTOP-5A3QN5S,155,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeDebugPrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"":""SubjectUserSid"","#text*":""S*1-5-18""},{""@Name"*:"SubjectUserSid"","#text*":""SubjectUserSid"","#text*":""SubjectDomainName"","#text*":""SubjectDomainName"","#text*":""SubjectDomainName"","#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege"]]]}



time	_raw
	13079,13079,2025-07-29 07:19:51.2263209,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"".""SubjectUserName"",""#text"".""SYSTEM""),(""@Name"".""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"";}}}
025-07-29 07:19:51.22	
	13076,13076,2025-07-29 07:19:51.1996480,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QNSS,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),[""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}
025-07-29 07:19:51.19	9 "
	13070,13070,2025-07-29 07:19:46.1618410,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},[""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 07:19:46.16	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
023-07-23 07.13.40.10	
	13068,13068,2025-07-29 07:19:46.0639354,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY"",\{""@Name":""SubjectLogonId"",""#text":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
025-07-29 07:19:46.06	
	13066,13066,2025-07-29 07:19:46.0206891,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,153,.Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"],{""@Name":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName","#text":""NT AUTHORITY"",{;""@Name":"SubjectLogonId"",""#text"":""
	0x3E7***],{***@Name**:**PrivilegeList***,***#text***:***SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
025-07-29 07:19:46.02	0 "
	13063,13063,2025-07-29 07:19:45.0300440,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text'":"SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	one in the state of the state o
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
	13061,13061,2025-07-29 07:19:44.8344855,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""@name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 07:19:44.8	334
	13059,13059,2025-07-29 07:19:43.5053694,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"[""EventData"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"":"SubjectUserName"":"#text":""SYSTEM""),{""@Name"":""
	SubjectDomainName", "#text":""NT AUTHORITY""), ("" @ Name"": ""SubjectLogonId"", ""#text"":""
	0x3E7"),{""@Name":-"PrivilegeList": ""#text":""SeAssignPrimaryTokenPrivilege, SeTcDPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeSeturityPrivilege, SeStatesperioremental Setup
OF 07 00 07:40:40	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}}}
25-07-29 07:19:43.	טע
	13057,13057,2025-07-29 07:19:43.0225458,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName","#text":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"","#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#ext"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeSeturityPrivilege, SeStatesperioremental Setup
025-07-29 07:19:43.0	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
725-01-25 01.15.45.	7.2
	13055,13055,2025-07-29 07:19:42.7345012,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,False, C:\Users\VM\Desktop\ Sourish cuts /\user\undersonatePrivilege\undersonate\undersonatePrivilege\undersona
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""
	"S-1-5-18""},(""@Name"":"SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	ONDET IN STREET INVINGELIST, FREAT SEASSIFF INITIATY OF THE PROPERTY OF THE SEASON OF
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege="""" 3eSuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""" 3eSeCuditPrivilege, SeDelegateSessionUserImpersonatePrivilege=""" 3eSeCuditPrivilege 3eSeCuditPriv
25-07-29 07:19:42.7	
	13053,13053,2025-07-29 07:19:42.7043619,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E5,,,,,,False,C:\Users\VM\
	Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#
	text"":""S-1-5-19""},{""@Name"":""SubjectUserName"",""#text"":""LOCAL SERVICE""),{""@
	Name"":""SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""# text"":""0x3E5""],{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
25-07-29 07:19:42.7	
	13051,13051,2025-07-29 07:19:42.6836491,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xDC44,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit
	success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1
	""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName""
25-07-20 07-40-42	,""#text"".""Window Manager""},{""@Name"".""SubjectLogonId"",""#text"":""0xDC44!""},{""@
25-07-29 07:19:42.6	Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}}}}"
	13050,13050,2025-07-29 07:19:42.6836474,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,776,
	DESKTOP-5A3QN5S,153,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xDB6E,,,,,,False,C:\Users\VM\
	Desktop\Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#
	text"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"
	":""SubjectDomainName"",""#text"":""Window Manager""},(""@Name"":""SubjectLogonId"",""#text""
	:""0xDB6E""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege,
	SelmpersonatePrivilege"" }}"



_time	_raw
025-07-29 07:19:42.676	13046,13046,2025-07-29 07:19:42.6763522,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18"",{""@Name"":""SubjectUserName"","#text*":""SYSTEM*"),{""@Name"*:""SUbjectUserName","#text*":""SYSTEM*"),{""@Name*":""SUBJectDomainName*","#text*":"" 0x3E7"",{""@Name*":""PrivilegeList*",""#text**:""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege*")]}}
025-07-29 07.19.42.676	
2025-07-29 07:19:41.928	13044,13045-07-29 07:19:41.9289059,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITYNETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",Logonide 0.x3E4,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData"::{""Data"::{\"@Name"::"SubjectUserSid"",""# text*"::""S-1-5-20\"],{\"@Name"::"SubjectUserName"","#text*":"NETWORK SERVICE*"],{\"@Name"::"SubjectUserName","#text*":"NT AUTHORITY*"],{\"@Name"::"SubjectLogonid\","\# text*":\"0.x3E4\"],{\"@Name"::"PrivilegeList*",\"#text*":\"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege*
	13042,13042,2025-07-29 07:19:41.6165146,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,820,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18""),(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""SubjectUserName"",""#text"":""SubjectDomainName",""#text"":""SubjectDomainName",""#text"":""SubjectLogonId",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege""]]]}
2025-07-29 07:19:41.616	#
2025-07-29 07:19:12.325	13013,13013,2025-07-29 07:19:12.3253346,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeSimpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData"":\""Data"":\""OName"":\""SubjectUserSid"""#text"\":\""S\S-1-5-18"\),\""@Name"\":\""SubjectUserSid"""#text\":\""S\SYSTEM\"\""@Name\"\"\"" S-1-5-18"\),\""@Name\"\"\""#text\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
	13011,13011,2025-07-29 07:19:12.1504165,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""@Name"":"SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":"SubjectUserName"",""#text"":"SYSTEM""),(""@Name"":"SubjectUserSid"","#text"":" SubjectDomainName":,"#text":""NT AUTHORITY""),(""@Name":""SubjectLogonId","#text"::" 0x3E7""),{""@Name"":""PrivilegeList"",""#text"::"SeAssignPrimaryTokenPrivilege, SeTctDerivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege""}}}
2025-07-29 07:19:12.150	
	13006,13006,2025-07-29 07:19:06.9870614,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248, DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0.x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"("EventData"",""Data":[{"@Name"::"SubjectIoserSid"","#text":"" "S-1-5-18"",{""@Name"::"SubjectUserName"",""#text":""SYSTEM"],{""@Name"":""SubjectLogonId"",""#text":"" SubjectDomainName",""#text":""NT AUTHORITY"",{""@Name"::"SubjectLogonId"",""#text":"" 0.x3E7""},{""@Name"::"PrivilegeList"","#text"::"SAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, "}}}



time	_raw
	13004,13004,2025-07-29 07:19:06.9094877,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY"],{""@Name"":"SubjectLogonId"",""#text"":"
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
025-07-29 07:19:06.909	, SeAuditrivilege, SeSystemenvironmentrivilege, Sempersonaterivilege, SeDelegateSessionOsemipersonaterivilege }}}
020-01-25 01.15.00.505	
	13002,13002,2025-07-29 07:19:06.9046213,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name":""SubjectUserName"",""#text"::""SYSTEM""],{""@Name":""
	SubjectDomainName", ""#text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"", ""#text"":""
	Ox3E7""},(""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"; }}}
025-07-29 07:19:06.904	
	2000 42000 2005 07 00 0740 06 0400506 4670 Local National Williams Williams County Available County 700 46 10
	12999,12999,2025-07-29 07:19:06.0460506,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""),{""@Name":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7"",[""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}}}}
025-07-29 07:19:06.046	
	12997,12997,2025-07-29 07:19:05.5526837,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248,
	DESKTOP-5A3QN5S,153,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[(""@Name":""SubjectUserSid"",""#text"":"
	"S-1-5-18"};{"'@Name"":"'SubjectUserName"",""#text"":"'SYSTEM"");{""@Name"":""
	SubjectDomainName"","#text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 07:19:05.552	
	1117 1117 2025 07 20 07:44:47 0250559 4672 LogAlyaye Microsoft Windows Courity Auditing Courity 742 920
	1117,1117,2025-07-29 07:14:47.9269558,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebuqPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18"),{"'@Name":"SubjectUserName",""#text":""SYSTEM""},{"'@Name":""
	SubjectDomainName"","#lext"::"NT AUTHORITY"},(""@Name":,""SubjectLogonid",""#text"";""
	0x3E7""},{""@Name":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]}}
025-07-29 07:14:47.926	
	1115,1115,2025-07-29 07:14:47.7005570,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name":""
	SubjectDomainName"",""#text"";""NT AUTHORITY""},{""@Name"";""SubjectLogonId"",""#text"";""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"::"PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



_time	_raw
2025-07-29 07:14:47.653	1113,1113,2025-07-29 07:14:47.6536026,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITYLOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,1"("EventData":":(""@Name":":"SubjectUserSid"",""# text*":""S-1-5-19\"],{\""@Name":":"SubjectUserName","#text*":""LOCAL SERVICE"],{\""@\""@Name":""SubjectDomainName","#text*":"NT AUTHORITY"},{\""@Name":"SubjectLogonId","\"# text*":""0x3E5\"],{\""@Name":":"PrivilegeList*",\"#text*":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",]}}
2025-07-29 07:14:47.651	1111,1111,2025-07-29 07:14:47.6511067,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,824, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeNetsorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebugPrivilege, SeMactivilege, SeSystemEnvironmentPrivilege, SecImpersonatePrivilege, SeDebugPrivilege, SeSemenvironmentPrivilege, SeImpersonatePrivilege, SeSemenvironmentPrivilege, SeMactivilege, SeMactivilege, SeMactivilege, SeMactivilege, SeMactivilege, SeTcbPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*
	1109,1109,2025-07-29 07:14:47.4383603,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,756,
2025-07-29 07:14:47.438	DESKTOP-5A3QN5S,12,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xC128,,,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"\""EventData"*:\"Data"*:\"\@\Name"*:\"SubjectUserSid"\"#\ext**:\"S-1-5-90-0-1 "\"\(\text{\text}\)\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29 07:14:47.438	1108,1108,2025-07-29 07:14:47.4383589,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,756, DESKTOP-5A3QN5S,12,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege,",LogonId: 0xC0FF,,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"("EventData":(""Data"::[{""@Name"::"SubjectUsersid"",""# text*":""Su-1-5-90-0-1*"],(""@Name":""SubjectUserName"",""#text*":""DWM-1*"],(""@Name":""SubjectUserName"",""#text*":""SubjectUserName"",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""SubjectLogonId**,""#text*":""#text*":""SubjectLogonId**,""#text*":""#text*":""SubjectLogonId**,""#text*":""#text*":""SubjectLogonId**,""#text*":""#text*":""SubjectLogonId**,"#text*":""#text*":""SubjectLogonId**,"#text*":""#text*":""SubjectLogonId**,"#text*":""#text*":""#text*":""SubjectLogonId**,"#text*":""#t
2025-07-29 07:14:47.229	1104,1104,2025-07-29 07:14:47.2295673,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,824, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData":",(""@Name":""SubjectUserSid"",""# text":""S-1-5-20""),{\""@Name":"\""S-1-5-20""},\{\""@Name":\""S-1-5-20""\""@Name":\""S-1-5-20""\""@Name":\""S-1-5-20""\""@Name":\""S-1-5-20"\""\"@Name":\""S-1-5-20"\""\""\""\""\""\""\""
	1098,1098,2025-07-29 07:14:47.0728279,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,768, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"("EventData":",(""@Name":.""SubjectUserSid"",""#text"":" "S-1-5-18""),(""@Name":.""SubjectUserName"",""#text"":""SYSTEM""),(""@Name":."" "SubjectDomainName",""#text"":""NT AUTHORITY""),(""@Name":.""SubjectLogonId"","#text":"" 0x3E7"",\(""@Name":.""PrivilegeList"",""#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeloadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}
2025-07-29 07:14:47.072	п
	2093,2093,2095-07-29 07:12:09.5719088,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,4848, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY'SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"" "S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""SubjectLogonId"","#text":"" SubjectDomainName"","#text"":""NT AUTHORITY""),{""@Name"::"SubjectLogonId"","#text":"" 0x3E7""},{""@Name"::""PrivilegeList",","#text"::""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}



time	_raw
	1073,1073,2025-07-29 07:11:38.7700602,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],[""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}}
25-07-29 07:11:38.77	
	1071,1071,2025-07-29 07:10:51.2009458,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,804,
	DESKTOP-5A3QNSS.12Administrative logon,NT AUTHORITYSYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},[""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-20 07-40-54 02	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 07:10:51.20	
	2091,2091,2025-07-29 07:10:04.4776450,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,6196,
	DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx.Audit success.0,"(""EventData":(""@Name":""SubjectUserSid": "#text":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@ Name":""SubjectLogonId"", ""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
)25-07-29 07:10:04.47	7
	1059,1059,2025-07-29 07:10:00.5919274,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,804,
	DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	. SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"";}}}
25-07-29 07:10:00.59	
	1057,1057,2025-07-29 07:09:49.6044915,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,732,
	DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"",""PrivilegeList",""#text"",""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 07:09:49.60	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
	1055,1055,2025-07-29 07:09:44.2580642,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,732,
	DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackunPrivilege, SeRestorePrivilege, SeDebunPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""}.{""@Name"":""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),[""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""],[""@Name"":"SubjectLogonId"",""#text"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""



time	_raw
	1053,1053,2025-07-29 07:09:42.0160989,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,732, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugateSessionUserImpersonatePrivilege""}]}}
25-07-29 07:09:42.016	1043,1043,2025-07-29 07:09:40.1102492,4672,LogAlways.Microsoft-Windows-Security-Auditing,Security,696,792,
	DESKTOP-5A3QN5S,11,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege,
	SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x2AD60,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{\""Data"":{\""@Name"":\""SubjectUserSid\"",\"#text\"":\"S-1-5-21-
	3151804214-3226339955-2188200191-1001""},{""@Name"":""SubjectUserName"",""#text"":""VM""},{"" @Name"":""SubjectDomainName"",""#text"":"DESKTOP-5A3QN5S""),{""@Name"":""SubjectLogonId"", ""#text"":""0x2AD60""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege,
25-07-29 07:09:40.110	#text : 0X2AD00);{
	1034,1034,2025-07-29 07:09:39.2330888,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#tex*t"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":" SubjectDomainName",""#text"":"NT AUTHORITY""),{""@Name"::"SubjectLogonld",""#text":""
	0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
25-07-29 07:09:39.233	
	1032,1032,2025-07-29 07:09:39.1818070,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"),{""@Name":,""#text":,"""""""""""""""""""""""""""""""""""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-29 07:09:39.181	
	1030,1030,2025-07-29 07:09:38.7633276,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	Subject:Domainisame ", #text :: NT AUTHORITY);{
25-07-29 07:09:38.763	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
	1026,1026,2025-07-29 07:09:37.5098331,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,792, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeNestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeNestorePrivilege, SeNe
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugateSessionUserImpersonatePrivilege""}]}}



_time	_raw
	1024,1024,2025-07-29 07:09:37.4080284,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,792,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege***}
025-07-29 07:09:37.408	
020 07 20 07 100.07 110	
	1022,1022,2025-07-29 07:09:37.3884794,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, Logonid: 0x3E7,,False,C:UsersIVM/Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},[""@Name":."'SubjectUserName"","#text"::""SYSTEM""),[""@Name":."
	SubjectDomainName", "#text": "NT AUTHORITY" }, (""@ Name": ""SubjectLogonId", ""#text"': ""
	0x3E7""},(""@Name":""PrivilegeList"",""#text'":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 07:09:37.388	"
	1019,1019,2025-07-29 07:09:36.8085457,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege="*]]}}
025-07-29 07:09:36.80	
	1017,1017,2025-07-29 07:09:36.8078522,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[(""Data"":[(""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY"],{""@Name"";""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 07:09:36.807	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
023-01-23 01.03.30.80	
	1015,1015,2025-07-29 07:09:35.6476438,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTctPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeSecurityPrivilege, SeUnderprivilege, SetakeOwnershipPrivilege, SetakeOwnershipPri
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "\$.4.5.48""](""@Name":""SubjectUserSid"",""#text"":"" "\$.4.5.48""](""@Name":""SubjectUserSid"",""#text"":""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, "I]]}
025-07-29 07:09:35.64	
	1013,1013,2025-07-29 07:09:35.4388606,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,792,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18"],{"@Name":"SubjectUserName"",""#text"":"SYSTEM""],{""@Name":""
	SubjectDomainName", "#text": "NT AUTHORITY" }, (""@ Name": ""SubjectLogonId", ""#text"': ""
	0x3E7""},(""@Name":"'PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
2025-07-29 07:09:35.403	1011,1011,2025-07-29 07:09:35.4034503,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,792, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITYLOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E5,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""# text*":""S-1-5-19*"),(""@Name*":"SubjectUserName*","#text*":""LOCAL SERVICE*"),{""@Name*":""SubjectDogonId*",""# text*":""LOCAL SERVICE*"),{""@Name*":""SubjectLogonId*",""# text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege*",}]])
025-07-29 07:09:35.401	1009,1009,2025-07-29 07:09:35.4014722,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-5A3QNSS,11,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SePastorePrivilege, SeDebugPrivilege, SeAuditFrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":\""Data":\"("@Name":\""SubjectUserSid"\"\"#text":\""S-1-5-18\"),\("\"@Name\"\"\""SubjectUserName\"\"\""SubjectUserName\"\"\""SubjectUserName\"\"\""SubjectUserName\"\"\"\""SubjectUserName\"\"\"\""SubjectUserName\"\"\"\""SubjectUserName\"\"\"\""\""\""\"\"\"\"\"\"\"\"\"\"\"\
	1007,1007,2025-07-29 07:09:35.1658714,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744,
	DESKTOP-5A3QN5S,11,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xBBCA,,,,False,C:\Users\VM\Desktop\Security.evtx, Audit success,0,"(""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90- 0-1""),{""@Name"":"SubjectUserName"","#text"":""DWM-1""},{""@Name"":"" SubjectDomainName"","#text"":""Window Manager"],{""@Name":""SubjectLogonId"","#text"":""
2025-07-29 07:09:35.165	0xBBCA""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege"")]}} "
2025-07-29 07:09:35.165	1006,1006,2025-07-29 07:09:35.1658701,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-5A3QN5S,11,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0xBB88,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":""5-1-5-90-0-1""},(""@Name":""SubjectUserName"",""#text"":""DWM-1""},(""@Name" Name" ":""SubjectDomainName",""#text":""Window Manager!"},(""@Name":""SubjectLogonId",""#text"":""0xBB88""),(""@Name":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]]}
2025-07-29 07:09:34.847	1002,1002,2025-07-29 07:09:34.8470687,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,792, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY/NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"{""EventData"":(""Data"":(""@Name"":""SubjectUserSidi"",""# text"":""S-1-5-20""),(""@Name"":""SubjectUserName",""#text"":"NETWORK SERVICE""),{""@Name"":""SubjectLogonId"",""# text"":""NT AUTHORITY"],{""@Name"":"SubjectLogonId"",""# text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeAuditPrivilege, SeImpersonatePrivilege"",]}])"
	996,996,2025-07-29 07:09:34.6600748,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,732,DESKTOP -5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBescurity.evtx,Audit sexcess,0.,"(""EventData":(""@Name":""SubjectUserSid",""#text":""S-1-5-18""), ""@Name":""SubjectUserName"",""#text":""S'bijectDomainName","" #text"":"NT AUTHORITY"),(""@Name":"SubjectLogonld",""#text":""0x3E7"),("@Name": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeAuditPrivilege, SeAuditPrivilege,
2025-07-29 07:09:34.660	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}"
	2089,2089,2025-07-29 06:57:01.5521678,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QNSS,27,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SVSTEM""},{""@Name"":""SubjectLogonld"",""#text"":"" SubjectDomainName"",""#text"":""SubjectLogonld"",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTebPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebuaPrivilege



time	_raw
	971,971,2025-07-29 06:50:24.7815694,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonia: 0x3E7,,False,C:Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"".""NT AUTHORITY""},{""@Name"".""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""]]}}
25-07-29 06:50:24.78	1 "
	969,969,2025-07-29 06:49:55.9576113,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"],(""@Name":""SubjectUserName",""#text":""SYSTEM""),(""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	SesecurityPrivilege, Se l'akeOwnersnipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeBackupPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-29 06:49:55.95	
25-01-29 00.49.00.90	
	967,967,2025-07-29 06:49:47.8171513,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"::""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY"",{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7"),{"@Name":"PrivilegeList", "#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 06:49:47.81	
	065-065-2025-07-20-08-40-22-0224402-4672-LogAlwaye Microsoft Windows Socurity Auditing Socurity 699-2549
	965,965,2025-07-29 06:49:22.9324403,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548, DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 06:49:22.93	2 "
	963,963,2025-07-29 06:48:52.9966238,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548,
	DESKTOP-5A3QN5S,11,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7***],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 06:48:52.99	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
20-01-23 00.40.02.98	
	961,961,2025-07-29 06:48:52.6974618,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,3548,
	DESKTOP-5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"LogonId: 0x3E7,,,,,,,Falst, 2 C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},(""@Name"".""SubjectUserName"",""#text"".""SYSTEM""),(""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text"":"" 0x2F7"") (""@Name":""Privilegel ict" ""#text"":""SchestenBriman/TekenBrivilege SoTehBrivilege
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}



_time	_raw
2025-07-29 06:48:49.440	959,959,2025-07-29 06:48:49.4409716,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege',Logonld: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name":""SVSTEM""},{""@Name":""SubjectDomainName"","" #text"":""NT AUTHORITY"],{""@Name":""SubjectLogonld"",""#text":""0x3E7""),{""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}"
2025-07-29 06:48:49.237	957,957,2025-07-29 06:48:49.2379973,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege*, Logonld: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""@Name"":\""SVSTEM\""\""@Name\"":\""SV)sipctDomainName\"",\"" \""@Name\"":\""SV\STEM\""\""@Name\"":\""Sv)sipctUbomainName\"",\"" \""#text\"":\""NT AUTHORITY\"\""@Name\"":\"SubjectLogonld\"\""\"#text\"\"\"\\""\\""\\""\\""\\""\\""\\""\\""
2025-07-29 06:48:30.278	2087,2087,2025-07-29 06:48:30.2789381,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,9020, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBentylege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0,"\"EventData"":\""Data":\"\""\"@Name":\""SubjectIosrSid"\""#text":\""\""S-1-5-18\"\"\""@Name\"\":\""SubjectUserName\"\""#text\"\":\""Sv5TEM\"\\""@Name\"\:\""SubjectLogonId\"\""#text\"\":\""SubjectDomainName\"\""#text\"\":\""NT AUTHORITY\"\"\"@Name\"\:\""SubjectLogonId\"\"\"#text\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29 06:43:24.060	955,955,2025-07-29 06:43:24.0604906,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0.'\"EventData\":\"\"Data\":\"\"@\Amme\":\"SubjectUserSid\",\"#ext\":\"S-1-5-18\"\"\"\"Aumines\":\"SubjectUserName\",\"#ext\":\"SYSTEM\"\"@\Amme\":\"\"SubjectUbomainName\",\"#ext\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-29 06:40:45.375	953,953,2025-07-29 06:40:45.3757639,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,800,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."\""EventData"":\""Data"":\""@Name"":\""SubjectUserSi\d"\","#text*":\""S-1-5-18"\", \"\""@Name\"":\""SubjectUserName\",\""#text*":\""SYSTEM\""),\"\"@Name\":\"\""\SubjectDomainName\"\"\" #text*\":\"\NT AUTHORITY\"\\"\"@Name\":\"SubjectLogonld\",\"#text*\"\"\"\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29 06:39:10 367	941,941,2025-07-29 06:39:10.3677520,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."(""EventData"":{""Data"":{""QName"":""SubjectUserSid",""#text*":""SubjectUserSid",""#text*":""SubjectUserName"",""#text*":""SubjectUserSid",""#text*":""SubjectUserName"",""#text*":""Name":"""Name":"""Name":"""Name":"""Name":"""Name":"""Name":"""Name":"""Name":"""Name":"""""""""""""""""""""""""""""""""""



_time	_raw
2025-07-29 06:38:59.218	939,939,2025-07-29 06:38:59.2181783,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QNSS,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege',LogonId: 0x3E7,,False,C:UsersIVMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""QName"":""SUbjectUserName"",""#text"":""SYSTEM"},(""QName":""SubjectDomainName"","" #text"":""NAUTHORITY"),{""QName":"SubjectLogonId"","#text":""0x3E7""],{""QName"": """PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}]])"
025-07-29 06:38:53.582	937,937,2025-07-29 06:38:53.5824251,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,Logonld: 0x3E7,,False,C:Users\WMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""StyDijectUserName"",""#text"":""SYSTEM""},{""@Name*":""SubjectDomainName*","" #text"":""NAUTHORITY"),{""@Name*":"SubjectLogonld"","#text":""0x3E7""},{""@Name*": ""PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*]]]}"
025-07-29 06:38:48.834	933,933,2025-07-29 06:38:48.8347267,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QNSS,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid",""#text"::""S-1-5-18""), {""@Name":""SubjectUserName"",""#text":"""SF-1-5-18"", {""@Name":""NT AUTHORITY""},(""@Name":""SubjectLogonId",""#text":""0x3E7""],{""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}]]])"
025-07-29 06:38:46.193	923,923,2025-07-29 06:38:46.1938224,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),, "PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x2F930,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0.*[""EventData"":{""Data"":{"Data":{"Data"":{"Data":{"Dat
025-07-29 06:38:44.758	916,916,2025-07-29 06:38:44.7582859,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\UserS\WI\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name":""SubjectUserSid"","#text"":""S-1-5-18""}, {""@Name"":"SubjectUserName",""#text":""SYSTEM""),{""@Name":""SubjectDomainName"","" #text":""NT AUTHORITY"*],{""@Name":""SubjectLogonId",""#text":""0x3E7"*],{""@Name":" ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege")]}}
	912,912,2025-07-29 06:38:44.5157100,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QNSS,10,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(""@Name":.""SubjectUserSid",,"#text":""S-1-5-18""), {""@Name":"SubjectUserName","#text":""SYSTEM"),(""@Name":.""SubjectDomainName","" #text":""NT AUTHORITY""),(""@Name":""SubjectLogonId", ""#text":""0x3E7""),{""@Name":"" ""PrivilegeList","#text":""S4SAssignPrimaryTokenPrivilege, SeTotPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeNauditPrivilege, SeDeblegateSessionUserImpersonatePrivilege")}}}"



_time	_raw
025-07-29 06:38:44.446	910,910,2025-07-29 06:38:44.4461176,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, ,SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, ,SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonIdc: 0x3E7,,,False,C:Users\WMDesktop\Security.evtx,Audit success,0,"(""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"","" #text":""NT AUTHORITY\""},{""@Name":""SubjectLogonId\"",\"#text\":\""\0x3E7\"},\{\""@Name\"": ""PrivilegeList\",\""#text\":\""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\"]])"
2025-07-29 06:38:42.599	908,908,2025-07-29 06:38:42.5994878,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData":",""Data":"{""@Name":""SubjectUserSid"","#text"":"5-1-5-18""}, {""@Name":"SubjectUserName"","#text"":""SYSTEM""},{"@Name":"SubjectDomainName"","" #text"":"NT AUTHORITY""},{""@Name":"SubjectLogonId",""#text"":""0x3E7""},{""@Name":" ""PrivilegeList","#text":":"SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege*; }}}
2025-07-29 06:38:40.479	905,905,2025-07-29 06:38:40.4794414,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"::"SubjectUserName"","#text":""SidestUserSid",""#text":"""S-1-5-18""), *#text":""NT AUTHORITY"",(""QName"::"SubjectLogonId",""#text":""0x3E7""}, *#text":""NT AUTHORITY"",(""QName":"SubjectLogonId",""#text":""\30x3E7""}, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]])"
2025-07-29 06:38:40.440	903,903,2025-07-29 06:38:40.4407558,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData":(""@Name":""SubjectUserSid":,"#text"":"5-1-5-18""}, {""@Name":""SubjectUserName","#text"":"SYSTEM""},{"@Name":""SubjectDomainName"","" #text"":"NT AUTHORITY""},{""@Name":"SubjectLogonId","#text"":""0x3E7""},{""@Name": ""PrivilegeList","#text":""SeAssignPrimaryTokenPrivilege, SeTobrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege"]]}}
	901,901,2025-07-29 06:38:39.4192725,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,'{""EventData"":(""Data"":(""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"::""SubjectUserName","#text":""SYSTEM"),{""@Name"::""0x3E7""},\""@Name"":""" *#text"":""NT AUTHORITY"),{""@Name"::""SubjectLogonId",""#text":""\38-28SecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]])}"
2025-07-29 06:38:39.223	899,899,2025-07-29 06:38:39.2231691,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""Data":(""@Name":""SubjectUserSid":,"#textt"::"S-1-5-18""), "("@Name":"SubjectUserName"","#text"::"SYSTEM"*),"("@Name"::"SubjectDomainName"","" #textt"::"NT AUTHORITY"*),"("@Name"::"SubjectLogonId"*,"#textt"::"0x3E7"*),"("@Name": ""PrivilegeList","#text"::"SeAssignPrimaryTokenPrivilege, SeTestPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege")]])"
2025-07-29 06:38:39 166	897,897,2025-07-29 06:38:39.1661993,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QNSS,10,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege*,LogonId: 0x3E5,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""SubjectUserSid"",\""# text*":\""S-1-5-19"\"\"@Name\":\""SubjectUserName\",\"\"#text\":\"\LOCAL SERVICE\"\"\@Name\":\"SubjectUserSid\"\"\"# Name\":\"SubjectDomainName\",\"\#text\":\"\NT AUTHORITY\"\"\@Name\":\"\SubjectUserSid\"\"\# text\"\"\"0x3E5\"\(\mathreal\),\"\"\@Name\"\\"\"\"#text\"\\"\"\"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SelmpersonatePrivilege\"\}\)\"



_time	_raw
025-07-29 06:38:39.157	895,895,2025-07-29 06:38:39.1576147,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege , SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege , SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"::{""Data"::{""@Name"::"SubjectUserSid",""#text*":""S-1-5-18"}, {""@Name"::"SubjectUserName",""#text*":""SYSTEM""),{""@Name"::"SubjectDomainName"","" #text*":""NT AUTHORITY"*],{""@Name"::"SubjectLogonId","#text*":""0x3E7"*],{""@Name": ""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}]})"
025-07-29 06:38:38.903	893,893,2025-07-29 06:38:38.9030801,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QN5S,10,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xBE4C,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."(""EventData:":("Data:":"("@Name"::"SubjectUserSid:",""#text*"::"S-1-5-90-0-1 ""),\"@Name":"SubjectUserName"",""#text*"::"Whindow Manager"),\"@Name":"SubjectDomainName"" "#text*":"Window Manager"),\"@Name":"SubjectLogonId*",\"#text*":""0xBE4C"],\"@ Name":"PrivilegeList:",\"#text*":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege")}});"
2025-07-29 06:38:38.903	892,892,2025-07-29 06:38:38.9030785,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,796,DESKTOP -5A3QN5S,10,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xBE1D,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"{""EventData":{{""QName"":""SubjectUserSid"",""# text"":""S-1-5-90-0-1""},{""@Name"":""SubjectIserName"","##ext"":"Dwhame",""#text"":"SubjectIserName"",""#text"":"SubjectIserName",""#text"":"SubjectIserName",""#text"":"SubjectIserName",""#text"":"SubjectIserName","#text":"SubjectIserName","#text":"":"SubjectIserName","#text":"":"SubjectIserName","#text":"":"SubjectIserName","#text":"":"SubjectIserName","#text":"":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text":":"SubjectIserName","#text
2025-07-29 06:38:38.620	888,888,2025-07-29 06:38:38.6206751,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,804,DESKTOP -5A3QN5S,10,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData":",(""@Name":""SubjectUserSid"",""# text"":""S-1-5-20""},{\""@Name"":""SubjectUserName"",""#text"":"NETWORK SERVICE""},{\""@Name"":"SubjectUserName",""#text"":"NETWORK SERVICE"],{\""@Name"":"SubjectUserName",""#text"":"S-1-5-20"",\""@Name":"SubjectUserName",""#text":"S-1-5-20"",\""@Name":"SubjectUserName",""#text":"S-1-5-20"",\""@Name":"SubjectUserName",""#text":"S-1-5-20"",\""@Name":"SubjectUserName",""#text":"S-1-5-20"",\""@Name":"SubjectUserName",""#text":""S-1-5-20"",\""@Name":"SubjectUserName",""#text":""S-1-5-20"",\""@Name":"SubjectUserName",""#text":""S-1-5-20"",\""@Name":"SubjectUserName",\""#text":""S-1-5-20"",\""#text":"S-1-5-20"",\""#text":"SubjectUserName",\""#text":"S-1-5-20"",\""#text":"SubjectUserName",\""#text":\""S-1-5-20"",\""#text":\""S-1-5-20"",\""#text":\""S-1-5-20"",\""#text":\""SubjectUserName",\""#text":\""S-1-5-20"",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""SubjectUserName",\""#text":\""#text":\""SubjectUserName",\""#text":\""#text":\""#text":\""SubjectUserName",\"#text":\""#text
025-07-29 06:38:38.350	882,882,2025-07-29 06:38:38.3509202,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,740,DESKTOP -5A3QN5S,9,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName":""SubjectUserSid","#text*":""S-1-5-18""}, {""@Name"":"SubjectUserName"",""#text*":""SYSTEM""),{""@Name":"SubjectDomainName"","" #text*":""NT AUTHORITY"*],{""@Name":"SubjectLogonId","#text*":""0x3E7"*],{""@Name"": ""PrivilegeList","#text*":""SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege";"]}}"
025-07-29 06:34:36.148	857,857,2025-07-29 06:34:36.1482998,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeSetivetprivilege, SeDebugPrivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeDebugPrivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSetivetprivilege, SeSesystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSesystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeSestivetprivilege, SeSestivetprivilege, SeSestivetprivilege, SeSestivetprivilege, SeDebugPrivilege, SeSestivetprivilege, SeDebugPrivilege, SeSesystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege*
2025-07-29 06:34:26.176	855,855,2025-07-29 06:34:26.1764125,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,740,DESKTOP -5A3QN5S,9,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,FaIse,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""QName":""SubjectUserSid",""#text*":""S-1-5-18""}, {""@Name":""SubjectUserName",""#text*":""SYSTEM"),{""@Name":"SubjectDomainName"","" #text*":""NT AUTHORITY"),{""@Name":"SubjectLogonId","#text*":""0x3E7"],{""@Name": ""PrivilegeList","#text*":""SeAssignPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege"}}}]"



_time	_raw
2025-07-29 06:33:36.046	851,851,2025-07-29 06:33:36.0464396,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,740,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text*":""SYSTEM*"},{""@Name"":""SubjectDomainName","" #text*":""NT AUTHORITY*"},{""@Name*":""SubjectLogonId",""#text*":""0x3E7*"},{""@Name*": ""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]}}}"
2025-07-29 06:32:31.145	849,849,2025-07-29 06:32:31.1456116,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,9,Administrative logon,NT AUTHORITY'SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTackeOwnershipPrivilege, SeDadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"",""#text"":""SYSTEM""},{""@Name"":"""SYSTEM""},{""@Name"":""""SYSTEM""},{""@Name"":"""SYSTEM""},{""@Name"":""SYSTEM""},{""@Name":""SYSTEM""},{""@Name":""SYSTEM"},{""
2025-07-29 06:31:38.231	847,847,2025-07-29 06:31:38.2314817,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAsuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:Users\WhDesktop\Security.evtx,Audit success,0."(""EventData":":(""@Name"::""SubjectUserSid",."#text":""S-1-5-18"), (""@Name":""SubjectUserSid",""#text":""S-1-5-18"), (""@Name":""SubjectUserSid",""#text":""SYSTEM"), (""@Name":""SubjectDomainName"",""#text":""NT AUTHORITY"), (""@Name":""SubjectLogonId", ""#text":""0x3E7""), (""@Name":"""""); (""@Name":""""); (""@Name":""SubjectLogonId", ""#text":""0x5E7""), (""@Name":""SeAssignPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]})"
2025-07-29 06:31:12.223	845,845,2025-07-29 06:31:12.2235334,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN55,9,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":"SubjectUserSid"","#text":""S-1-5-18""), {""@Name":"SubjectUserName"","#text":""SYSTEM""},{""@Name":"SubjectDomainName"","" #text"":""NT AUTHORITY""},{""@Name":"SubjectLogonId"",""#text":""0x3E7""},{\""@Name": ""PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}}}"
2025-07-29 06:30:04.246	822,822,2025-07-29 06:30:04.2469168,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,9,Administrative logon,NT AUTHORITY'SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTackoPrivilege, SeDescurityPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"",""#text"":""S*1** #text":""NA AUTHORITY** #text":""NA HOTHORITY** #text":""SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRationDervilege, SeDelegateSessionUserImpersonatePrivilege""]}})"
2025-07-29 06:29:54.198	814,814,2025-07-29 06:29:54.1987614,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\WhDesktop\Security.evtx,Audit success,0."(""EventData":"(""Data":"(""@Name":""SubjectUserSid",,""#text":""S-1-5-18""), {""@Name":""SubjectUserName"",""#text":""SYSTEM""),(""@Name":"SubjectDomainName"","" #text":""NT AUTHORITY""),{""@Name":""SubjectLogonId",""#text":""0x3E7""),{""@Name": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDelegateSessionUserImpersonatePrivilege")}})"



_time	_raw
2025-07-29 06:29:54.02	812,812,2025-07-29 06:29:54.0245441,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeCourityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,"False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":"SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserSid"",""#text"":""S'AID-5-18""}, {""@Name"":""SubjectUserSid"",""#text":""SubjectDomainName",""#text":""SubjectUserSid",""#text":""SubjectDomainName","" #text"":""NT AUTHORITY""),(""@Name":""SubjectLogonId","#text":""0x3E7"),(""@Name":"""Shatsid Privilege, SeTostPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeAuditPrivilege, SeSeSeurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSeSeurityPrivilege,
2025-07-29 06:29:49.49	810,810,2025-07-29 06:29:49.4972095,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeEackupPrivilege, SeBackupPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Otaa"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text":""SYSTEM""},{""@Name"":""SubjectDomainName"","" #text"":""N AUTHORITY"",{""@Name"":""SubjectLogonId"","#text":""0x3E7""},{""@Name"": ""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSestorePrivilege, SeDebugPrivilege"]]}}
2025-07-29 06:29:45.96	808,808,2025-07-29 06:29:45.9610416,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,9,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSestorePrivilege, SeInpersonatePrivilege, SeInpersonatePrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,,Palse,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\mathred{"}}"@Name":""SubjectUserSid",""#text":""S-1-5-18"", {\mathred{"}}"@Name":""SubjectUserName",""#text":""SYSTEM""),{\mathred{"}}"@Name":""SubjectDomainName",""#text":""SHEXTEM:"",\mathred{"}"@Name":""SubjectDomainName",""#text":""SHEXTEM:"",\mathred{"}"@Name":""SubjectDomainName",""#text":""SHEXTEM:"",\mathred{"}",""#text":""SASSignPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSeystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}}}"
2025-07-29 06:29:44.29	799,799,2025-07-29 06:29:44.2988890,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,DESKTOP-5A3QN5S\VM (\$-1-5-21-3151804214-3226339955-2188200191-1001),," PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3045B,,,,,False,C:\Users\VM\Desktop\Security,evtx,Audit success,0."(""EventData\"":\""Data\"":\""Data\"":\"\""\Bata\"":\""\""\Bata\"":\""\""\""\"\""\""\"\""\"\""\"\""\
2025-07-29 06:29:38.75	788,788,2025-07-29 06:29:38.7576430,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False,C:Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":"S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"",""#text"":""S":"S":"S":"S":"S":"S":"S":"S":"S"
2025-07-29 06:29:38.74	786,786,2025-07-29 06:29:38.7454567,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,8.,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAsuitPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, Logonld: 0x3E7,,,,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0.*(""EventData"*:(\""@Name":\""SubjectUserSid",\""#text":\""S-1-5-18\"",\""@Name":\""SubjectUserSid",\""#text":\""S-1-5-18\"",\""@Name\":\""SubjectUserSide\",\""#text\":\""SVSTEM\"'),\""@Name\":\"SubjectDomainName\"\"\"#text\"\"\""\""\"@Name\":\""SubjectLogonld\"\""#text\"\"\\""\"@Name\"\\"\"\""\"\"@Name\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\



_time	_raw
025-07-29 06:29:36.710	782,782,2025-07-29 06:29:36.7109983,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugprivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\UMDesktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":"SubjectUserSid"",""#text":""S-1-5-18""), {""@Name":""SubjectUserName"",""#text":""SYSTEM""},{""@Name":""SubjectDomainName"","" #text":""NT AUTHORITY"},{\""@Name":"SubjectLogonId",""#text":""0x3E7"*],{\""@Name": ""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugateSessionUserImpersonatePrivilege"]]})"
025-07-29 06:29:36.695	780,780,2025-07-29 06:29:36.6950210,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTotPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege",Logonld: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), ""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonld"",""#text"":""0x3E7""),{""@Name"": ""PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTotPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege"; })"
025-07-29 06:29:36.193	777,777,2025-07-29 06:29:36.1938915,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP 75A3QN5S,8,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""], {""@Name"":"SubjectUserName"",""#text"":""SYSTEM"},{""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY"],{\""@Name"":""SubjectLogonId"",""#text"":""0x3E7""],{\""@Name"": ""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}])"
2025-07-29 06:29:36.092	775,775,2025-07-29 06:29:36.0922643,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAudritPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"","#text"":"5-1-5-18""), {""@Name":""SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY""},{""@Name":""SubjectLogonld"",""#text"":""0x3E7""},{""@Name"": ""PrivilegeList","#text":""SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugSerimpersonatePrivilege"]}})"
025-07-29 06:29:35.344	773,773,2025-07-29 06:29:35.3446355,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QNSS,8,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAudritPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VMDbektop\Security.evtx,Audit success,0,"(""EventData":(""Data":(""@Name":""SubjectUserSid":,"#text"::"S-1-5-18""), ""@Name":""SubjectUserName"","#text"::"SYSTEM"),(""@Name"::"SubjectDomainName"","" #text"::""NT AUTHORITY\"),(""@Name"::"SubjectLogonld":,"#text"::"0x3E7"),(""@Name": ""PrivilegeList",""#text"::"SeAssignPrimaryTokenPrivilege, SeTextPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege")]})"
2025-07-29 06:29:35.174	771,771,2025-07-29 06:29:35.1744974,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,1(""EventData":(""@Name":""SubjectUserSid","#text"::"S-1-5-18"), {""@Name":""SubjectUserName"",""#text"::"SYSTEM""},{""@Name"::"SubjectDomainName"","" #text"::""NT AUTHORITY""},{""@Name":"SubjectLogonld":,"#text"::"0x3E7";},{"@Name": ""PrivilegeList",""#text"::"SeAssignPrimaryTokenPrivilege, SeTestPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege";]}),"
	769,769,2025-07-29 06:29:35.1370519,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QNSS,8,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E5,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text*":""S-1-5-19""},(""@Name"",""\$ubjectUserName"",""#text*":""LOCAL SERVICE""},{""@Name":""SubjectUomainName"",""#text*":"NT AUTHORITY*"},(""@Name":""SubjectLogonId"",""# text*":""0x3E5"*],(""@Name"":""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege";}})



_time	_taw
2025-07-29 06:29:35.129	767,767,2025-07-29 06:29:35.1299782,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,792,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, Logonld: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"::""StyDijectUserName",""#text*":""SYSTEM""},{""@Name*":""SubjectDomainName*","" #text*":""NT AUTHORITY*"},{""@Name*":"SubjectLogonld",""#text*":"0x3E7*"},{""@Name*": ""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}}}"
025-07-29 06:29:35.008	765,765,2025-07-29 06:29:35.0086513,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xC1EE,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#Evert":""SubjectDomainName"",\""@Name"":""SubjectUserName"",""#Evert":""SubjectDomainName"",\""#Exert":""Vindow Manager"\""@Name"":""SubjectLogonId",\""#text"":""\(""@\DWAME"":""\)\""@Name"":""\(""\)\""@\DWAME":""\)\""\(""\)\""\(""\)\""\)\""\(""\)\""\(""\)\""\\""\
025-07-29 06:29:35.008	764,764,2025-07-29 06:29:35.0086501,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0xC1AC,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,""EventData":(""Data":(""@Name":""SubjectUserSid"",""# text*":""S-1-5-90-0-1"",(""@Name":""SubjectUserName"","*#text*":""DWM-1""),(""@Name" ":""SubjectDomainName","*#text*":""Window Manager"),{""@Name":""SubjectLogonId"","*#text*" :""0xC1AC"",(""@Name":""PrivilegeList*",""#text*":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege"")]}})"
2025-07-29 06:29:34.796	760,760,2025-07-29 06:29:34.7964686,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP -5A3QN5S,8,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData":(;""@Name"::"SubjectUserSid"","## text*":""S-1-5-20""),{""@Name"::""SubjectUserName"","##text*":""NETWORK SERVICE"],{""@Name":""GubjectLogonId","## text*":""SubjectDomainName",""#text*":""NT AUTHORITY"],{""@Name":""SubjectLogonId","## text*":""SubjectLogonId*","## text*":""## text*":""",## text*":""## text*":"""## text*":""## text*":""## text*":""## text*":""## text*":""## text*":""## te
025-07-29 06:29:34.543	754,754,2025-07-29 06:29:34.5430523,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,8,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeRestorePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY""},\""@Name"":""SubjectLogonId",""#text":""0x3E7""},\""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTebrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}]}"
1005 07 20 05 40 22 05G	2085,2085,2025-07-29 05:48:32.0537257,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,7756, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName"":""SubjectUserSid"",""#text"":""S\S+15-18"",{""@Name"":""SubjectUserSid"",""#text"":""S\SubjectDomainName"",""#text"":""S\SYSTEM"",{\""@Name":""SubjectLogonId"",""#text":"""0x3E7""],{\""@Name":""PrivilegeList",""#text":""S\SASsignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}
2025-07-29 05:48:32.053	2083,2083,2025-07-29 05:14:58.6078860,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,6068, DESKTOP-5A3QN5S,27,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"";(""Datat");(""@Name":""SubjectUserSid"","#text"":" "S-1-5-18"");(""@Name":""SySTEM""),(""@Name":""SySTEM"");(""@Name":""SySTEM"");(""@Name":""SySTEM"");(""@Name":""SySTEM*");(""@Name":"");("@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");(""@Name":"");("@Name":");(""@Name":");("@Name":");(""@Name":");(""@Name":");("@Name":");(""@Name":");("");("@Name":");(""@Name":");(""@Name":");(""@Name":");(""@Name":");(""@Name":");("");("@Name":");("");("@Name":");("");("@Name":");("@Name":");("");("@Name":");("");("@Name":");("");("@Name":");("");("@Name":");("");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":");(");("@Name":"



_time	_raw
	2068,2068,2025-07-29 04:59:26.7367145,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,9164, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege',LogonId: 0x3E7,,False,C:Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"","#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":"" "S-1-5-18""],(""@Name"":""NauTHORITY"),(""@Name"":""SubjectUserName"",""#text":"" SubjectDomainName",""#text":""NauTHORITY"),(""@Name":""SubjectLOgenId",""#text":"" 0x3E7""],(""@Name":""PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege "SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege")]}}
025-07-29 04:59:26.7	
025-07-29 04:55:02.5	298,298,2025-07-29 04:55:02.5445950,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,3,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY"",{""@Name":""SubjectLogonId"","#text":""0x3E7""),{""@Name":""SubjectDomainName"","" #rvivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}]}"
	296,296,2025-07-29 04:55:02.3061776,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP
2025-07-29 04:55:02.3	-5A3QN5S,3,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAscignPrivilege, SeSpetingPrivilege, SeDebugPrivilege, SeSpetingPrivilege, SeSpetingPrivi
025-07-29 04:55:01.3	291,291,2025-07-29 04:55:01.3247127,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,3,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\Wh\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text":""SYSTEM"},{""@Name":""SubjectDomainName"","" #text"":""NT AUTHORITY"",{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"": ""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]}}"
025-07-29 04:55:00.8	285,285,2025-07-29 04:55:00.8294743,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,3,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"::"SubjectUserName"",""#text":""SyTEM"),(""@Name"::"SubjectDomainName"","" #text"":""NT AUTHORITY""),(""@Name"::""SubjectLogonId"",""#text"":""0x3E7""),(""@Name":: ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBelogateSessionUserImpersonatePrivilege""]]]}"
2025-07-29 04-55-00 4	213,213,2025-07-29 04:55:00.4612439,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""QName"":\""SubjectUserSid"\",\""#text"":\""S-1-5-18\" \"\"@Name\":\""SubjectUserName\",\"\"#text\"\":\""SYSTEM\"\(\frac{1}{2}\),\"\"@Name\":\""\SubjectDomainName\"\\"\"\"#text\"\"\"\"\"\"AuTHORITY\\\\\\\\\"\"\"\"&Name\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\



_time	_raw
2025-07-29 04:55:00.029	211,211,2025-07-29 04:55:00.0290933,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":"\""Data":"\""oame":""SubjectUserSid"",""#text"":"S-1-5-18""), \""@Name":"SubjectUserName":""SubjectUserSid",""#text":""S1-5-18""), \""@Name":""SubjectUserName":""SubjectUserName":""SubjectDomainName"",""#text":""NT AUTHORITY""},\""@Name":""SubjectLogonId"",""#text":""0x3E7""},\""@Name":"""#text":""BeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"""]})"
2025-07-29 04:55:00.002	209,209,2025-07-29 04:55:00.0002898,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,2,,Administrative logon,DESKTOP-5A3QN5S\defaultuser0 (S-1-5-21-3151804214-3226339955-2188200191-1000),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x148CD,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":\"Data":\"@Name":\""SubjectUserSid",\"#text\":\"S-1-5-21-3151804214-3226339955-2188200191-1000\"\],\"@Name\":\"SubjectUserName\"\"#text\":\""SubjectUserName\"\"#text\"\":\""SubjectUserName\"\"#text\"\":\""SubjectUserName\"\"#text\"\":\""SubjectUserName\"\"#text\"\"\"\""SubjectUserName\"\"#text\"\"\"\"\"SubjectUserName\"\"\"\"#text\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-29 04:54:57.013	188,188,2025-07-29 04:54:57.0130042,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDebugPrivilege, SeSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"(""EventData":\"[""Data"":\"[""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""),\""@Name":\"""#text"":""SubjectUserName"",\""#text":\""SUbjectUserName"\",\""#text":\""SubjectUserName"\",\""#text":\""SubjectUserName"\",\""#text":\""SubjectUserName"\",\""#text":\""SubjectUserName\",\""#text":\""SubjectUserName\",\""#text":\""SubjectUserName\",\""#text":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\"\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\""#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\""SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"SubjectUserName\",\"\"#text\":\"\"SubjectUserName\",\"\"#text\":\"\"SubjectUserName\",\"\"#text\":\"\"SubjectUserName\",\"\"#text\":\"\"\"SubjectUserName\",\"\"#text\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-29 04:54:52.354	186,186,2025-07-29 04:54:52.3547172,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,'{\"EventData"":\"Data"":\"\@Name"\":\"SubjectUserSid"",\"# text\":\"S-1-5-19\"\\"\@Name\":\"\USeT\SERVICE\"\\\"\@Name\":\"\USeT\SERVICE\"\\\\"\\\"\\\"\\\\"\\\\"\\\\\\\\\\\
2025-07-29 04:54:52.209	184,184,2025-07-29 04:54:52.2097798,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":\"\"\"\substata\"\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29 04-54-54 002	182,182,2025-07-29 04:54:51.9920452,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xBDDF,,,,,False,C:\Users\VM\Desktop\Security.evtx, Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text*":""S-1-5-90- 0-1""},{{""@Name"":""SubjectUserName"",""#text*":""DWM-1""},{{""@Name"":""SubjectLogonId"",""#text*":"" SubjectDomainName"",""#text*":""Window Manager*"},{{""@Name"":"SubjectLogonId"",""#text*":"" 0xBDDF*"),{{""@Name"":""PrivilegeList*"",""#text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}}}}
2025-07-29 04:54:51.992	181,181,2025-07-29 04:54:51.9920424,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0xBDCD.,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,'{""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""# text"":""S-1-5-90-0-1""},(""@Name"":""SubjectUserName"",""#text"":""DWM-1""},(""@Name" ":""SubjectDomainName"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege")}}}"



_time	_raw
025-07-29 04:54:51.528	177,177,2025-07-29 04:54:51.5284125,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,2,,Administrative logon,NT AUTHORITY\NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege*, LogonId: 0x3E4,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\"@Name"":""SubjectUserSid"",\""#text*":""SubjectUserSid"",\""#text*":""SubjectUserSid"",\""#text*":""NETWORK SERVICE""},{\"@Name"":""SubjectDomainName"",\""#text*":""NT AUTHORITY""},{\"@Name"":"SubjectLogonId"",\"#text*":""SubjectLogonId"",\"#text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege*
025-07-29 04:54:51.216	171,171,2025-07-29 04:54:51.2168137,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,736,DESKTOP -5A3QN5S,2.,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text"":""SYSTEM"},{""@Name"":""SubjectDomainName"","" #text"":""N AUTHORITY"],{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""],{""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcDPrivilege, SeEcurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]})"
025-07-29 04:54:14.102	150,150,2025-07-29 04:54:14.1026895,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,440,WIN-NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:Users\VM\Desktop\ Security,evtx,Audit success,0,"("EventData":":""Data":":[""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18"",{""@Name":""SubjectUserName"",""#text"":""SYSTEM"],{""@Name"":"" SubjectDomainName"",""#text":""NT AUTHORITY"",}{""@Name":""SubjectLogonId"",""#text":"" 0x3E7"],{""@Name":"PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
2025-07-29 04:54:11.268	148,148,2025-07-29 04:54:11.2687659,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0,"(""EventData"":[""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18"",{""@Name"::"SubjectUserName",""#text":""SYSTEM"),{""@Name"":"" SubjectDomainName"",""#text":""NT AUTHORITY"",{""@Name"::"SubjectLogonId"",""#text"":"" 0x3E7"",{""@Name"::"PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
2025 07 20 04-54-40 560	146,146,2025-07-29 04:54:10.5602005,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NoIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData":(""Data":(""Oame"::""subjectUserSid"",""#text"":" "S-1-5-18"",(""@Name":""SubjectUserName",""#text"":""SVSTEM"),(""@Name"::"" SubjectDomainName",""#text":"NT AUTHORITY"),(""@Name":"SubjectLogonId","#text":"" 0x3E7""),(""@Name":""PrivilegeList"",""#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebuge**]}}}
2025-07-29 04:54:10.560 2025-07-29 04:54:10.076	144,144,2025-07-29 04:54:10.0764677,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),(""@Name"",""SubjectUserName"",""#text"":""SySTEM"),(""@Name"":"" SubjectDomainName"",""#text":""NT AUTHORITY""),(""@Name":""SubjectLogonId"",""#text"":"" 0x3E7""),(""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege"]}}}



time	_raw
	142,142,2025-07-29 04:54:09.4279984,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"","#text":":"SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"'PrivilegeList"",""#text"":"'SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 04:54:09	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
	140,140,2025-07-29 04:54:08.9667855,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,1,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],(""@Name"": ""PrivilegeList"",""#text"": ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
:5-07-29 04:54:08	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
	138,138,2025-07-29 04:54:08.5603119,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,1,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":(""Datata"":(""@Name"":""SubjectUserSid""."#text":"."#text":"."
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"'PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
25-07-29 04:54:08	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
23-07-29 04.34.00	136,136,2025-07-29 04:54:07.6043751,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"", ""#text"":"
	"S-1-5-18""},{"'@Name"":"'SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"'PrivilegeList"",""#text"":"'SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]]}
25-07-29 04:54:07	604 " 134,134,2025-07-29 04:54:07.1266541,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0."(""EventData"::[(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"::""SubjectUserName"",""#text"":""SYSTEM""),{""@Name":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 04:54:07	
	132,132,2025-07-29 04:54:06.7218292,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7*"),(*"@Name*".*"PrivilegeList*",""#text*":""SAAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege



ime	_raw
	130,130,2025-07-29 04:54:06.3855087,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,,,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY""],{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-29 04:54:06.3	
	128,128,2025-07-29 04:54:06.0849341,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{\""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":"SubjectLogonId"",""#text"":"
	0x3E7""},(""@Name"":"PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
5-07-20 04-E4-00 0	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
25-07-29 04:54:06.0	
	126,126,2025-07-29 04:54:05.5042494,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text":""IT AUTHORITY""},(""@Name"",""SubjectLogonId"",""#text"",""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 04:54:05.5	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
20 07 20 0 110 110010	
	124,124,2025-07-29 04:54:04.2517870,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	NOIRNITIGIFG,1,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0," (""EventData"": (""Data"": [{""@Name"": ""SubjectUserSid"", ""#text"": ""
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY""],{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7""], [""@Name": "PrivilegeList", "#text": "SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}
25-07-29 04:54:04.2	
	121,121,2025-07-29 04:53:53.7973497,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":(""Data"":({""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
5-07-29 04:53:53.7	77
	119,119,2025-07-29 04:53:52.2870930,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	So Società Privilogo So Tako Ouropphia Privilogo Sol cod Priving Privilogo So Books a Privilogo Books a Priv
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
	114,114,2025-07-29 04:52:27.3436424,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege".LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#ext"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege ""}}}}
25-07-29 04:52:27.3	
	111,111,2025-07-29 04:52:12.2088576,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-
	NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":"
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
005 07 00 04 50 45	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
)25-07-29 04:52:12.2	U8 "
	109,109,2025-07-29 04:52:10.3562509,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""N AUTHORITY"",(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 04:52:10.3	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-25 04.52.10.0	
	107,107,2025-07-29 04:52:08.9795905,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,736,WIN-
	NOIRN/179IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeCondation and Season and
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0," {""EventData"": {""Data"": [{""@Name"": ""SubjectUserSid"", ""#text"": ""."
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text":""NT AUTHORITY""],(""@Name":""SubjectLogonId"",""#text"":""
	0x3E7"),("'@Name":"PrivilegeList", "#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeRestorePrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege.""}}}
025-07-29 04:52:08.9	
	104,104,2025-07-29 04:52:08.0268001,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security evtx, Audit success, 0, "{""EventData"": (""Data"": (""@Name"": ""SubjectUserSid"", ""#text"": "
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"".""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text*":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text*":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 04:52:08.0	26 "
	102,102,2025-07-29 04:52:07.9440968,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-
	NOIRN1T9IF6,1,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],(""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}



me	_raw
	99,99,2025-07-29 04:52:06.8629610,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSesionUserImpersonatePrivilege*, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,*(""EventData":(""Data"::{\"@Name"::\"\substitute{"}\substitut
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"" SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
25-07-29 04:52:06.862	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]} "
	95,95,2025-07-29 04:52:05.9070491,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN1T9IF6,1,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,*(*"EventData":(*"Data"::{\"@Name"::"SubjectUsers\","#text"::" Security.evtx,Audit success,0,*(*"EventData":(*"Data"::{\"@Name"::"SubjectUsers\","#text"::"#text"::" Security.evtx,Audit success,0,*(*"EventData":(*"Data"::{\"@Name"::"SubjectUsers\","#text"::"#text:::"#text:::"#text:::"#text:::"#text:::"#text:::"#text::::"#text::::"#text::::"#text::::"#text::::"#text::::"#text::::"#text:::::#text::::#text:::::#text::::::::#text::::::::::
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"" SubjectDomainName",""#text"":""NTAUTHORITY",{""@Name":""SubjectLogonId","#text"":"" 0x3E7""},{"@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 04:52:05.907	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]} "
	93,93,2025-07-29 04:52:05.6651534,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-N0IRN1T9IF6,0,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,*{""EventData":{""Data":{""@Name"::""SubjectUsers\dim",""#text"":"
	"S-1-5-18""},(""@Name"":""SubjectUserName"", ""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName", "#text"":"NAUTHORITY",(""@Name":""SubjectLogonId"", "#text"":"" 0x3E7""},{""@Name":""PrivilegeList"", ""#text":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-29 04:52:05.665	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
	91,91,2025-07-29 04:52:05.5165202,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-NOIRN1T9IF6,0,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""@Name"":"SubjectUserSid"","#text"":"
25-07-29 04:52:05.516	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"" SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name":"PrivilegeList",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
20 07 20 0 110210010 10	63,63,2025-07-29 04:51:55.3680628,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN1T9IF6,0,,Administrative logon,NT AUTHORITY/LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,,False,C:\Users\VM\
	Desktop/Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text"":""S-1-5-19""},{""@Name"":""SubjectUserName"",""#text"":""LOCAL SERVICE""},{""@ Name"":""SubjectDomainName"",""#text"":"NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""# text"":""0x3E5""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
25-07-29 04:51:55.368	, SelmpersonatePrivilege"")]])" 61,61,2025-07-29 04:51:55.1168919,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN179IF6,0,.Administrative logon,Window ManagenDWM-1 (S-1-5-90-0-1),"PrivilegeList:
	NUIRN119IFb,(),,,dministrative logon,window managenDWM-1 (S-1-5-90-0-1),, PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0x12BE7,,,,,False,C:\UserSid",""#text*":"S-1-5-90- 0-1""),{""@Name"":"SubjectUserName"",""#text*":""DWM-1""),{""@Name"*:""S-1-5-90- 0-1""),{""@Name"*:"SubjectUserName",""#text*":""DWM-1""),{""@Name*":"SubjectLogonId*",""#text*":""SubjectLogonId*",""#text*":"" SubjectDomainName*",""#text*":""Window Manager*"),{""@Name*":""SubjectLogonId*",""#text*":"" 0x12BE7""),{""@Name*":"PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege*")}}}
25-07-29 04:51:55.116	60,60,2025-07-29 04:51:55.1168901,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-
	NOIRN1T9IF6,0,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x12BD5,,,,,False,C:\Users\VM\ Desktop\Security,evtx,Audit success,0,"(""EventData"":[""Data"":[[""@Name"":""SubjectUserSidi",""# text"":""S-1-5-90-0-1""],(""@Name"":""SubjectUserName",""#text":""DWM-1""),(""@Name" ":""SubjectDomainName",""#text":""Window Manager"),(""@Name":""SubjectUserQonId"",""#text""
25-07-29 04:51:55.116	:"0x12BD5""},(""@Name"::""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege";}}}



time	_raw
	56,56,2025-07-29 04:51:54.9417969,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,756,WIN-NOIRN1T9IF6,0,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""@Name"":"SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text":""SYSTEM""),{""@Name"":""SubjectUserName",""#text":"" SubjectDomainName",""#text":""NT AUTHORITY"*,(""@Name"":""SubjectLogonId","#text":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege""]}}}
025-07-29 04:51:54.941	•
025-07-29 04:51:54.016	54,54,2025-07-29 04:51:54.0167640,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,800,WIN-N0IRN1T9IF6,0,,Administrative logon,NT AUTHORITY/NETWORK SERVICE (S-1-5-20),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x3E4,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""# text*"":""SubjectIomainName"","**Text*":""NETWORK SERVICE*"),{""@Name*":""SubjectLogonId*",""# text*"":""SubjectDomainName*","#text*":""NT AUTHORITY*"),{""@Name*":""SubjectLogonId*",""# text*"":""0x3E4*"),{""@Name*":""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege*"]]])"
	48,48,2025-07-29 04:51:53.6036654,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,736,WIN-
))))25, 07, 20, 04:54:52:500	NoIRN1T9IF6,0,,Administrative logon,NT AUTHORITY\SYSTEM (\$-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSestaepPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeSestorePrivilege, SeDebugPrivilege, SeAudltPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeBestorePrivilege, SeDebugPrivilege, SeAudltPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""@Name"":"SubjectUserSid"",""#text"":" "S-1-5-18""),{""@Name"":""SubjectUserName"",""#text":""SYSTEM"),{""@Name"":""" "SubjectDomainName"","#text":""NAUTHORITY""),{""@Name":""SubjectLogonId"","#text":"" 0x3E7""),{""@Name":""PrivilegeList","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege"")]}}
025-07-29 04:51:53.603	0000 0000 0005 07 00 04 40 04 000000 4070 Landburg Minary (UMF along Openity Audition Openity 740 000
2025-07-29 04:48:21.008	2066,2025-07-29 04:48:21.0088680,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QNSS,27,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeSexemershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,*[""EventData"::[""@Name"::"SubjectUserSid"",""#text"::" "S-1-5-18"",\[""@Name"::"SubjectUserName"",""#text*"::"SYSTEM*"),\[""@Name*":""SubjectUserName*",""#text*"::" SubjectDomainName*","#text*"::"NAT AUTHORITY**],\[""@Name*":"SubjectLogonId*","#text*"::" 0x3E7*"],\[""@Name*":"PrivilegeList*",""#text*":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]]}}
	2064,2064,2025-07-29 04:14:41.1659761,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5160, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBescurityPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,1"("EventData":1"\"@Name":"SubjectUserSid","#text":""\"%Name":""\"#text":""\"@Name":""\"#text":"\"%YSTEM"\),{\"@Name":\""
2005 07 00 04 44 44 405	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
2025-07-29 04:14:41.165	" 2062,2062,2025-07-29 03:59:21.6265711,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QN5S,27,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":{""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectLogonId"","#text"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"","#text"":"" 0x3E7""},{""@Name":""PrivilegeList"",""#text"":""SAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}}}



_time	_raw
2025-07-29 03:48:38.620	2060,2060,2025-07-29 03:48:38.6202751,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,8652, DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeSystemEnvironmentPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeSeSecurityPrivilege, SeSeCountivePrivilege, SeSe
2025-07-29 03:48:05.028	12994,12994,2025-07-29 03:48:05.0283375,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,1248, DESKTOP-5A3QN5S,152,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""SubjectUserSid"",\""#text"":\" "S-1-5-18"\""@Name":\""SubjectUserName"\"\"#text"\":\""SYSTEM"\""@Name\":\"" SubjectDomainName\",\""#text\"\":\""NT AUTHORITY\"\""@Name\":\"SubjectLogonId\",\"\"#text\"\":\" 0x3E7\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-29 03:48:04.599	12992,12992,2025-07-29 03:48:04.5990904,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,772, DESKTOP-5A3QN5S,152,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\"Data"":\""@Name"":\"SubjectUserSid",\"\"#ext\"":\"S-1-5-18\"),\"\"@Name\":\"SubjectUserSid\",\"\"#ext\"":\"S-1-5-18\"),\"\"@Name\":\"\"SubjectUserName\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-29 03:44:33.026	6403,6403,2025-07-29 03:44:33.0262426,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,808, DESKTOP-5A3QN5S,76,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebupPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18"},{"@Name":""SubjectUserName"",""#text":""SYSTEM"},{""@Name":"" SubjectDomainName"",""#text":""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text"":"" 0x3E7"*],{""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebupPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}}
2025-07-29 03:44:32.839	6401,6401,2025-07-29 03:44:32.8390527,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760, DESKTOP-5A3QN5S,76,,Administrative logon,NT AUTHORITY\LOCAL SERVICE (S-1-5-19),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E5,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,1(""EventData":(,""@Name"::(""@Name"::""SubjectUserSid"",""# text"::""S-1-5-19"",1(""@Name"::""LOCAL SERVICE"],1(""@Name":""N# \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
2025-07-29 03:44:32.816	6399,6399,2025-07-29 03:44:32.8160390,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760, DESKTOP-5A3QN5S,76,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xD26F,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":(""@Name"::"SubjectUserSid":,"#text"::"S-1-5-90-0-1 ""},\{""@Name"::"SubjectUserName"","#text"::"DWM-1"),\{""@Name"::"SubjectDomainName"" ,""#text"":"Window Manager"',\{""@Name"::"SubjectLogonId",""#text"::"0xD26F""},\{""@Name"::"PrivilegeList"",""#text"::"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}
2025-07-29 03-44-32 846-	6398,6398,2025-07-29 03:44:32.8160364,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760, DESKTOP-5A3QN5S,76,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0xD259,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""# text":""S-1-5-90-0-1""},{""@Name":""SubjectUserName"",""#text":""DWM-1""},{""@Name" ":""SubjectDomainName",""#text":""Window Manager""},{""@Name":""SubjectLogonId"",""#text"" ":""0xD259""},{""@Name":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}}})"



_time	_raw
	6394,6394,2025-07-29 03:44:32.5280043,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,808,
	DESKTOP-5A3QN5S,76,,Administrative logon,NT AUTHORITY/NETWORK SERVICE (S-1-5-20),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege",LogonId: 0x3E4,,,,,,False,C:\Users\VM\
	Desktop\Security.evtx,Audit success,0,"{""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#
	text"":""S-1-5-20""},{""@Name"":""SubjectUserName"",""#text"":""NETWORK SERVICE""),{""@
	Name"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#
	text"":""0x3E4""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege
025-07-29 03:44:32.528	, SeImpersonatePrivilege""]]}}"
	6392,6392,2025-07-29 03:44:32.3100958,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,812,
	DESKTOP-5A3QN5S,76,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAudilPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
025-07-29 03:44:32.310	•
	2058,2058,2025-07-29 03:14:21.1949958,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2084,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{[""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 03:14:21.194	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
025-07-29 03.14.21.194	
	2056,2056,2025-07-29 02:48:00.6743536,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name"":"SubjectUserName"","#text*":"SYSTEM""),(""@Name"":"
	SubjectDomainName", ""#ext": "NT AUTHORITY"),{"" @ Name": ""SubjectLogonId", "#ext": "
	0x3E7""},{""@Name"":""PrivilegeList"",""#ext"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 02:48:00.674	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
023-07-29 02.40.00.074	
	2054,2054,2025-07-29 01:59:23.3476122,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,372,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"".""SubjectUserName"",""#text"".""SYSTEM""},{""@Name"".""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":"" 0x3F7"") (""@Name":""Privilegel ict" ""#text"":""SaAssignPrivilegel SaTchPrivilegel SaTchPrivilegel
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebuggateSessionUserImpersonatePrivilege [1] }
025-07-29 01:59:23.347	Services Services
0. 20 01.00.20.047	
	2052,2052,2025-07-29 01-48-30.5835509,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2352,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}



time	_raw
	2044,2044,2025-07-29 01:16:02.4523867,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,7668,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*
25-07-29 01:16:02.4	
	2040,2040,2025-07-29 01:16:02.3143825,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,7668,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
OF 07 00 04:10 00 5	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 01:16:02.3	14 "
	2038,2038,2025-07-29 01:15:27.4495189,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 01:15:27.4	
	2036,2036,2025-07-29 01:09:52.4921393,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,8072,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
025-07-29 01:09:52.4	32 "
	2034,2034,2025-07-29 01:06:23.4240190,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2032,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#ext"":""SYSTEM""},{""@Name"":"" SubjectDomainName"" ""#text"":""NT_ALITHORITY"") (""@Name":""System ("" ""#text"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebuqPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}
25-07-29 01:06:23.4	
	2018,2018,2025-07-29 00:53:43.8817009,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,6172,
	2018;2018;2025-07-29 00:53:43.8817009;4672;LogAlways;Microsoft-Windows-Security-Auditing,Security,712;6172, DESKTOP-5A3QN5S;26,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege", LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx.Audit success,0."(""EventData":(""Data":(;1"@Name"::"SeptimizetUserSid":,"#textt":"
	"S-1-5-18""},{*"@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{*"@Name"":""
	SubjectLogonid", "#text": "NT AUTHORITY", ("@Name": "SubjectLogonid", "#text": "
	- Cabject Communitation , more than the more of the manner of the community of the communit
	0x3E7""},(""@Name"":""PrivilegeList"",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,



time	_raw
	2003,2003,2025-07-29 00:53:28.9815315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2132, DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"", ""#text": ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBeskupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"}}}}
25-07-29 00:53:28.981	
	1999,1999,2025-07-29 00:51:59.7154467,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2132,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, 'PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"";""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-29 00:51:59.715	
20 07 20 00.01.00.710	
	1991,1991,2025-07-29 00:51:55.3015363,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	Selmpersonate/Privilege, SeDelegateSessionUser/Impersonate/Privilege, SevysitemEntrivilege, SetSelmpersonate/Privilege, SetSetSelmpersonate/Privilege, SetSetSetSetSetSetSetSetSetSetSetSetSetS
	Security.evtx,Audit success,0."(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"" "##text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]]}
025-07-29 00:51:55.301	
	1987,1987,2025-07-29 00:51:55.0444351,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,3680,
	DESKTOP-5A3QN5S,26,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege***}]}} *
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052,
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
)25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052,
25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege ""}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
)25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QNSS,14,,Administrative logon,NT AUTHORITYSYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTebPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":(""@Name"":"SubjectUserSid"","#text"":"
)25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\ Security,evtx,Audit success,0."(""EventData":(""@Name":""SubjectUserSid"", ""#text"":" "S-1-5-18"},(""@Name":"SubjectUserName", ""#text":""SYSTEM""),{""@Name":""
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SePostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeDeb
25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."{""EventData":"{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""},{""@Name":""SySTEM""SySTEM""},{""@Name":""SySTEM""SySTEM"*SySTEM************************************
25-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"","#text*":" "S-1-5-18"},{""@Name"":""SubjectUserName"",""#text*":""SYSTEM""},{""@Name"":"" SubjectDomainName"",""#text*":""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text*":"" 0x3E7""),{""@Name":""PrivilegeList*","#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege,",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY"),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":"PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}}
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege,",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY"),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":"PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}}
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."\(""EventData"":\(""Data"":\(""@Name"":\""SubjectUserSid"",\""#text"":\"" "S-1-5-18""\(""@Name"":\""SubjectUserName"\(",\""#text"":\""SYSTEM\("")\(""@Name"\(",\""#text\("":\"")\) SubjectDomainName\(",\""#text\("\":\""\)"NT AUTHORITY\("\",\""@Name\("\",\""\)"\) SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege\("")\) 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052,
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},[""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName",""#text":""NT AUTHORITY"),{""@Name"":""SubjectLogonId",""#text":"" 0x3E7""),[""@Name"":""PrivilegeList","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAsditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData":"(""@Name":""SySTEM""),{""@Name":""" "S-1-5-18""},{""@Name":""SubjectUserName",""#text*":""SySTEM*"},{""@Name":"" SubjectDomainName",""#text*":""SubjectUserName",""#text*":"" SubjectDomainName",""#text*":""SubjectUserName",""SubjectLogonId","#text*":"" SubjectDomainName",""#text*":""SubjectUserName":"SubjectLogonId","#text*":"" 0x3E7""},{""@Name":""FivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
025-07-29 00:51:55.044	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}} "1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."{""EventData"":{""Data"":{""QName"":""SySTEM""},{""@Name"":""SubjectUserSid"","#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"","#text"":"SYSTEM""},{""@Name"":""SubjectLogonId"","#text":"" SubjectDomainName"","#text"":"NT AUTHORITY""),{""@Name":""SubjectLogonId"","#text":"" 0x3E7""},{""@Name":""PrivilegeList","#text*":""SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} " 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebegateSessionUserImpersonatePrivilege, LogonId: 0.43E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"","#text"":" "S-1-5-18""),{""@Name"":""SubjectUserName"":""SubjectUserSid"","#text"":" SubjectDomainName"","#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"","#text":"" SubjectDomainName"","#rivilegeList","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeRestorePrivilege"]}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTcbPrivilege, SeDebugPrivilege, SeSexotemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSecurityPrivilege, SeSuddItPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData"":[""Data"":[""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY"),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),{""@Name"":""PrivilegeList",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeBecutyPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeTakeOwnershipPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeCoudDriverPrivilege, SelmpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData":"(""Data":"(""Data":"SubjectUserSid"","#etxt":"
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeAstorePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAstorePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAsionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."(""EventData":"(""Datat":"(""@Name":""SySTEM""),{""@Name":"""""""""""""""""""""""""""""""""""
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")}}} "1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-SA3QNSS,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0."(""EventData":"(""Data":"(""@Name":""SySTEM""),{""@Name":""" "S-1-5-18""},{""@Name":""SubjectUserName",""#text*":""SYSTEM*"),{""@Name":""" SubjectDomainName":""#text*":""SubjectUserName","#text*":""SubjectLogonld*","#text*":"" 0x3E7"*),{""@Name":""PrivilegeList*","#text*":""SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeDebugPrivilege ,SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege ,SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege "}}} 1215,1215,2025-07-29 00:48:05.7632315,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052,DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList:SeAssignPrimaryTokenPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, Selngary, """ """" """" """" """ """ """ """ """
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} 1217,1217,2025-07-29 00:48:06.9096569,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeAstorePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAstorePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAsionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."(""EventData":"(""Datat":"(""@Name":""SySTEM""),{""@Name":"""""""""""""""""""""""""""""""""""



_time	_raw
	1213,1213,2025-07-29 00:48:05.6966395,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,5052,
	DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName", ""#text"": "NT AUTHORITY"), (""@Name": "SubjectLogonId", ""#text": ""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeInpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege
025-07-29 00:48:05.696	, Sendulir ivilege, Sesystemenvillement ivilege, Sempersonater ivilege, Sebelegalesessionosemipersonater ivilege ///////////////////////////////////
	2044 4044 2005 07 00 00 45 05 0504005 4070 Lord Nursin Missearch Windows Country Available Country 740 4550
	1211,1211,2025-07-29 00:45:05.0581805,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,4552, DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogorIc 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":(\"@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectIDomainName", ""#text"::"NT AUTHORITY""}, (""@Name":, "SubjectLogonid", ""#text""; ""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
025-07-29 00:45:05.058	T .
	1209,1209,2025-07-29 00:29:30.5866601,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,3104,
	DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
100E 07 00 00:00:00 E00	, seAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]} """
025-07-29 00:29:30.586	
	1207,1207,2025-07-29 00:15:47.9879294,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,2852,
	DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	Selmpersonate Privilege, SeDelegate SessionUser Impersonate Privilege", LogonId: 0x3E7,,False, C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":""
	Ox3E7""},{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege
025-07-29 00:15:47.987	, 55. 65. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1. 1.
	400F 400F 000F 07 00 00 45 47 000 10 40 4070 Landburg Alburg Albu
	1205,1205,2025-07-29 00:15:47,9094949,4672,L0gAlways,Microsoft-Windows-Security-Auditing,Security,712,2852,
	DESKTOP-5A3QN5S,14,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SebackupPrivilege, SekestorePrivilege, SebebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),(""@Name":"SubjectUserName"",""#text"":"SYSTEM""),(""@Name":""
	SubjectDomainName", ""#text"::""NT AUTHORITY""},{""@Name":""SubjectLogonId"", ""#text"":""
	0x3E7""],{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeRestorePrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}
025-07-29 00:15:47.909	
	1203,1203,2025-07-29 00:15:05.1325168,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,6468,
	DESKTOP-5A3QNS,13,,Administrative logon,NT AUTHORITY/STEM (6-1-5-18), "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"},{""@Name"::"SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	ONDET J, WHATHE . I THINGSELIST , MEXT . CEASSIGHT HITIERY FORCETT HITIERS, SETEDITIVINESSE,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege



time	_raw
	1201,1201,2025-07-28 23:59:14.2609321,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,3120, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":[(""@Name":,""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""),(""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}}}}
25-07-28 23:59:14.26	
	1199,1199,2025-07-28 23:48:09.2849303,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,3996,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"","#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":"NT AUTHORITY""},(""@Name"':"SubjectLogonId"",""#text"":""
	0x3E7***],{"**@Name***:""PrivilegeList***,"**#text***:"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege ("]}}}
25-07-28 23:48:09.28	
	1197,1197,2025-07-28 23:14:50.1212429,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,8100, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
NOE NO 20 22:14:EN 11	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
025-07-28 23:14:50.12	
	1195,1195,2025-07-28 22:57:23.1628702,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,7796,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0," (""EventData"": (""Data"": [{""@Name"": ""SubjectUserSid"", ""#text"": "
	"S-1-5-18"],{"@Name":""SubjectUserName": ""#text":""SYSTEM""],{"@Name": ""
	SubjectDomainName", ""#text": ""NT AUTHORITY"], (""@Name": "SubjectLogonId", ""#text": ""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-28 22:57:23.16	52 "
	1193,1193,2025-07-28 22:45:11.5584550,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{\""@Name"":""SubjectUserSid"",""#text"":" "\$.1.5.19""\
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
25-07-28 22:45:11.5	
	1190,1190,2025-07-28 22:34:57.6816868,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":"
	SubjectDomainName"",""#text":""IT AUTHORITY""},{""@Name"",""SubjectLogonId"",""#text"",""
	0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}



time	_raw
	1188,1188,2025-07-28 22:31:42.7525153,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,984, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{(""Data"":{[""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName", ""#text": ""NT AUTHORITY""}, ("" @ Name": ""SubjectLogonId"", "#text": ""
	0x3E7***],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}
25-07-28 22:31:42.75	
	1186,1186,2025-07-28 22:29:53.7643796,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":{(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""),{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{ ""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},[""@Name"":"PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-28 22:29:53.76	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}
LU-U1-20 ZZ.ZY.33./t	
	1179,1179,2025-07-28 22:16:54.5391646,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,824,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData":(""Olata":(""@Name"::"SubjectUserSid": "#text"::"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]]}
25-07-28 22:16:54.53	99
	1173,1173,2025-07-28 22:15:15.0879346,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,832,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""],(""@Name"":""
	SubjectDomainName",""#text":""NT AUTHORITY"",{""@Name":""SubjectLogonId"",""#text"":""
	0x3E7";\"@\name":"PrivilegeList":""#ext":"SeAssignPrimaryTokenPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]]}}
25-07-28 22:15:15.08	
	1171,1171,2025-07-28 22:15:04.5358829,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,824,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),, "PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"","#text"":""SYSTEM""),{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7***],{""@Name"":""PrivilegeList"",""#text*"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege ""}}}
25-07-28 22:15:04.53	
	1169,1169,2025-07-28 22:14:58.6392308,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,832, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:USers\VM\Desktop\
	Security.evtx,Audit success,0,"("EventData"":(""Data"":[(""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},;""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""),{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""]}}}



time	_raw
	1163,1163,2025-07-28 22:14:56.2579735,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,832, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
07.00.00.44.50.05	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, seAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege=""}]]}
5-07-28 22:14:56.25	1144,1144,2025-07-28 22:14:53.6235015,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712.828,
	DESKTOP-5A3QN5S,13,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-
	1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege,
	SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x282DF,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit
	success,0,"(""EventData"":(""Data"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-1001""},(""@Name"":""SubjectUserName"",""#text"":""VM""),(""
	@Name"":""SubjectDomainName"",""#text"":""DESKTOP-5A3QN5S""},{""@Name"":""SubjectLogonId"",
	""#text"":""0x282DF""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege,
5-07-28 22:14:53.62	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}"
	1135,1135,2025-07-28 22:14:52.6368425,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[(""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-28 22:14:52.63	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}}
25-07-26 22.14.52.05	1133,1133,2025-07-28 22:14:52.6086645,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7"],(""@Name"":""PrivilegeList"",""#text"".""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"">}}}
25-07-28 22:14:52.60	8 "
	1129,1129,2025-07-28 22:14:51.4042283,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBestorePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeBestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeSystemEnvironme
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":"
	"S-1-5-18"},{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""],(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-28 22:14:51.40	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}} 4 "
	1127,1127,2025-07-28 22:14:51.3637503,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828,
	DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRostorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"(""EventData"":(""Data"":[(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"",""#text"":""SYSTEM""),(""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""],{""@Name"":""SubjectLogonId"",""#text"":""
	0x3E7"],{""@Name"":""PrivilegeList"",""#text"".""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
	Separation in the second secon



time	_raw
	1125,1125,2025-07-28 22:14:51.3380480,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,828, DESKTOP-5A3QN5S,13,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTcbPrivilege, S
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":""SYSTEM""},{"@Name"":"" SubjectDomainName"",""#text"":""NT AUTHORITY""),{"@Name"":""SubjectLogonId"",""#text"":""
	0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
025-07-28 22:14:51.338	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}} "
	1122,1122,2025-07-28 22:14:50.6120438,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,756, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""),(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},(""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
025-07-28 22:14:50.612	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*")]]}
720 07 20 22.14.00.012	1120,1120,2025-07-28 22:14:50.5870444,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,756, DESKTOP-5A3QN5S,12,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList:
	SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege,
	SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""],{""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":"" SubjectDomainName",""#text"":"NT AUTHORITY""],{""@Name"::""SubjectLogonId"",""#text"":""
	0x3E7""},{""@Name"":""PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]]}
)25-07-28 22:14:50.587	"716,716,2025-07-28 21:07:32.3341552,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864,
	DESKTOP-5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":"SubjectUserSid"",""#text"":"
	"S-1-5-18""},{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""},{""@Name"":" SubjectDomainName"",""#text"":"NT AUTHORITY""},{""@Name"":"SubjectLogonId"",""#text"":""
	0x3E7**},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege
25-07-28 21:07:32.334	, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
	714,714,2025-07-28 20:56:31.8114260,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864, DESKTOP-5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege,
	SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\
	Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""],{""@Name"":"SubjectUserName"",""#text"":"SYSTEM""],{""@Name"":""
	SubjectDomainName"",""#text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":"PrivilegeList"",""#text"":"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege,
25-07-28 20:56:31.811	SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"}]]}
23-07-20 20:30:31:011	699,699,2025-07-28 20:54:12.4738734,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege,
	SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege,
	SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:Users\VMDesktop\Security.evtx,Audit success,0,"("EventData":{\"Data":{\"Balance":"\subjectUserSid",\"#text":\"S-1-5-18\"}, \"\"\"\"S\\Data":\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
	{""@Name"":""SubjectUserName"",""#text"":"SYSTEM""),{""@Name"::""SubjectDomainName"","" #text":""NT AUTHORITY"),{""@Name":"SubjectLogonld"",""#text":""0x3E7""),{""@Name": ""Driviteral ist" ""#text":""SubscingPrimanyTokenPrivilene SeTchePrivilene Setup
	""PrivilegeList"", ""#text"", ""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege,



_time	_raw
2025-07-28 20:45:13.382	669,669,2025-07-28 20:45:13.3826076,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864, DESKTOP-5A3QN5S,T,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":"SubjectUserSid"",""#text"":" "S-1-5-18""},{""@Name"":""SubjectUserName"","#textt":""SYSTEM"*],{""@Name":"" SubjectDomainName"","#text":""NAT AUTHORITY**],{""@Name":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*"]]}}
025-07-28 20:41:31.990	667,667,2025-07-28 20:41:31.9904166,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":[""Data"":[(""@Name"":""SubjectUsersid"",""#text"":""S-1-5-18""), ""@Name":""SubjectUsername"",""#text"":""SYSTEM"),("@Name":"""SubjectDomainAmer","" #text":""NT AUTHORITY"),(""@Name":""SubjectLogonId",""#text":""0x3E7""),""@Name":" ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]})"
025-07-28 20:37:36.728	684,684,2025-07-28 20:37:36.7282377,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7.,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonIdd: 0x3E7,,False,C:Users\WMDesktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text*":""S-1-5-18""), {""@Name":.""SUbjectUserName"",""#text*"::""SYSTEM"},{""@Name*":""SubjectDomainName*","" #text*":""NT AUTHORITY"],{""@Name*":""SubjectLogonId",""#text*":""0x3E7*"],{""@Name*": ""PrivilegeList*",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*]]})"
2025-07-28 20:27:42.808	651,651,2025-07-28 20:27:42.8086130,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1996, DESKTOP-5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"\"EventData":(\""\@Name":\"\"\"\subjectUserSid"\"\"\#text\"\"\"\" "S-1-5-18\"\"\@Name\"\"\"\"\"\subjectUserName\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
025-07-28 20:25:36.991	646,646,2025-07-28 20:25:36.9918107,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,7904, DESKTOP-5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData"":[""@Name":""SubjectUserSid"",""#text"":" "S-1-5-18"",{""@Name":""SubjectUserName",""#text"":""SYSTEM"!},{""@Name":"" SubjectDomainName"",""#text":""NT AUTHORITY"",{""@Name"::"SubjectLogonId"",""#text":"" 0x3E7"",{\"@Name"::"PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege "SeMuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]]}
	644,644,2025-07-28 20:25:36.9191743,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,7904, DESKTOP-5A3QN5S,7,,Administrative logon,NT AUTHORITY/SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0.x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"(""EventData":(""@Data":(""@Name":""SubjectUserSid",""#text"": "S-1-5-18"),(""@Name":""SubjectUserSid",""#text":"" SubjectDomainName",""#text":""NT AUTHORITY"),(""@Name":""SubjectLogonId"",""#text":"" 0x3E7"),(""@Name":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege")]}}



time	_raw
	632,632,2025-07-28 20:22:15.6857765,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSentenPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeSesionUserImpersonatePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeTales-C:Users\WMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"":""SubjectUserSid"",""#text":""S-1-5-18"", {""@Name":""SubjectUserName",""#text":""SYSTEM""},{""@Name":""SubjectDomainName"",""#text":""NAUTHORITY"),{""@Name":""SubjectLogonld"","#text":""0x3E7"*],{""@Name": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege,
25-07-28 20:22:15.685	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"")]]}"
25-07-28 20:22:15.561	630,630,2025-07-28 20:22:15.5619255,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDebugPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeBackupPrivilege, SeDebugPrivilege, SeSustemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeDebugPrivilege, SeImpersonatePrivilege, SeImpersonatePrivilege, SeImpersonatePrivilege, SeImpersonatePrivilege, SeImpersonatePrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeJimpersonatePrivilege, SeJimpersonatePriv
025-07-28 20:17:18.537	628,628,2025-07-28 20:17:18.5374116,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,7,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,,False,C:\Users\VM\Desk\to\Security.evtx,Audit success,0,"{""EventData"":{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserSid"",""#text"":""SubjectDomainName"",""#text"":""#text"":""NT AUTHORITY"),{""QName"":""SubjectLogonId"",""#text"":""0x3E7""},{""QName":"""SubjectLogonId"",""#text"":""0x3E7""},{""QName":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeImpersonatePrivilege, SeImpersonatePri
025-07-28 20:16:48.428	626,626,2025-07-28 20:16:48.4288075,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,6.,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeSecurityPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"",""Data"":{(!""@Name"":""SubjectUserSid"",""#text":"""SubjectUserSid"",""#text":"""SubjectUserSid",""#text":""SubjectUserSid",""#text":"""SubjectUserSid",""#text":"""NT AUTHORITY""},{""@Name":""SubjectLogonId"",""#text":""\"""\"""\"""\"""\"""\"""\"""\"""\""
	597,597,2025-07-28 20:12:25.9354384,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864, DESKTOP-5A3QN5S,6,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18), "PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonIdc 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text*":""S-1-5-18""},{""@Name"":""SubjectUserName",""#text*":""SYSTEM!"",{""@Name":""SySTEM!"",{""@Name":""SySTEM!"",*"@Name":""SySTEM!"",*"@Name":""" SubjectDomainName",""#text*":""NAT AUTHORITY"",{""@Name":""SubjectLogonId",""#text*":"" 0x3E7""],{""@Name":""PrivilegeList",""#text*":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDebegetSessionUserImpersonatePrivilege"]]}}
2025-07-28 20:12:25.935	589,589,2025-07-28 20:11:14.4163581,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,6,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,False,C:\UserS\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"";""0xta":"["@Name":""SubjectUserSid"","#text"":"5-1-5-18""}, {""@Name":""SubjectUserName",""#text":""SYSTEM""},{""@Name":""SubjectDomainName"",""#text"":""StyStem","#text"":""StyStem","#text"":""0x3E7""},{""@Name":"""""""""""""""""""""""""""""""""""



_time	_raw
	538,538,2025-07-28 20:10:35.8489800,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864, DESKTOP-5A3QN5S,6,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege,"LogonId: 0x3E7,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":" "S-1-5-18""},(""@Name"":""SubjectUserName"","#text"":""SYSTEM""),(""@Name":"" SubjectDomainName","#text":""NT AUTHORITY""),(""@Name":""SubjectLogonId","#text":"" 0x3E7""),{""@Name"":""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"}]])}
025-07-28 20:10:35.848	
2025-07-28 20:10:35.140	535,535,2025-07-28 20:10:35.1401584,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,796,DESKTOP -5A3QN5S,6,,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),," PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SelmpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*,LogonId: 0x2671DB,,,,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"(""EventData":(""Data"::{"""Data"::{"""""""""""""""""""""""""""""""""
	531,531,2025-07-28 20:10:34.3296301,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,5,,Administrative logon,Window Manager\DWM-2 (S-1-5-90-0-2),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",Logonld: 0x26549A,,,,,,False,C:\Users\VM\Desktop\Security.evtx, Audit success,0,""EventData":(""Data":(!\"@Name":.\"SubjectUserSid\",\"\"&\":\"S-1-5-90- 0-2\"\"\"\@Name\":\"\"\subjectUserName\",\"\"\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-28 20:10:34.329	
2025-07-28 20:10:34.329	530,530,2025-07-28 20:10:34.3296286,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,5,,Administrative logon,Window Manager\DWM-2 (S-1-5-90-0-2),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SelmpersonatePrivilege",LogonId: 0x26547D,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name":""SubjectUserSid"",""# text"":""S-1-5-90-0-2"],{""@Name":""SubjectUserName"",""#ext"":"DWM-2""},{""@Name" ":""SubjectDomainName",""#ext":""Window Manager"],{""@Name":""SubjectLogonId"",""#text"" :""0x26547D""),{""@Name":""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""]}})
20025.07.28 20:06:07 687	489,489,2025-07-28 20:06:07.6875768,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,5,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SySTEM""},{""@Name"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text"":""SYSTEM"",{""@Name"":""SubjectDomainName","" #text"":""NT AUTHORITY"",{""@Name"":""SubjectLogonld"",""#text"":""0x3E7""},{""@Name"": ""PrivilegeList"",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeMentoreprivilege, SeDebugPrivilege, SeAuditPrivilege,
2025-07-28 20:03:24.473	SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")}}}" 486,486,2025-07-28 20:03:24.4736084,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,4868, DESKTOP-5A3QN5S,5,Administrative logon,DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191- 1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege',LogonId: 0x23057D,,,,,,,False,C:UsersIVM/Desktop\Security.evtx,Audit success,0,"(""EventData":";(""@Name"::"SubjectUserSid"",""#text":""S-1-5-21- 3151804214-3226339955-2188200191-1001""),{""@Name"::"SubjectUserName",,""#text":""VM""},{"" @Name"::"SubjectDomainName",""#text"::"DESKTOP-5A3QN5S'"},{""@Name"::"SubjectLogonId"", ""#text":""0x23D57D"},{""@Name":"PrivilegeList",,""#text"::"SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]})}"
	457,457,2025-07-28 19:58:28.1295711,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,5,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,1{""EventData"";(""@Name":""SubjectUserSid"","#text"":"5-1-5-18""), {""@Name":""SubjectUserName",""#text"":""SYSTEM""},{"@Name":""SubjectDomainName""," #text"":""NT AUTHORITY""},{""@Name":""SubjectLogonld"",""#text"":""0x3E7""},{""@Name": ""PrivilegeList","#text":":"SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDeblegateSessionUserImpersonatePrivilege";}})"



_time	_raw
2025-07-28 19:57:58.6	447,447,2025-07-28 19:57:58.6337888,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,5,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False,C:UlsersIvMDesktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"::"SubjectUserName"", ""#text"::""SYSTEM""},{""@Name"::"SubjectDomainName"","" ##ext"":"NT AUTHORITY""},{""@Name"::"SubjectLogonId", "##ext":""0x3E7""},{""@Name":: ""PrivilegeList", "#text":""SeAssignPrimaryTokenPrivilege, SeTobrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]]]}"
2025-07-28 19:57:58.4	445,445,2025-07-28 19:57:58.4995838,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QNSS,5,.Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDelegateSessionUserImpersonatePrivilege, LogonId: 0x3E7,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":"SubjectUserName"", ""#text"":""SYSTEM""),(""@Name"":""SubjectDomainName"","" #text"":""NT AUTHORITY""},(""@Name"":""SubjectLogonId"",""#text"":""0x3E7""),(""@Name"": ""PrivilegeList"","#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}"
2025-07-28 19:57:54.0	443,443,2025-07-28 19:57:54.0717995,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,5,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:Ulsers\W\Desktop\Security.evtx,Audit success,0,"(""EventData":(""@Name"::"SubjectUserSid"",,"#text"::"S-1-5-18""), {""@Name"::"SubjectUserName",""#text"::"SYSTEM""},(""@Name"::"SubjectDomainName"","" #text"::"NT AUTHORITY"),(""@Name"::"SubjectLogonId"","#text"::"\0.3E7""),(""@Name"::""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeEcurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}
025-07-28 19:57:11.4	441,441,2025-07-28 19:57:11.4626590,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,796,DESKTOP -5A3QNSS,5,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,False,C:USers\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18"}, {""@Name"":""SubjectUserName"",""#text"":""SVEME"",{""@Name"":""SubjectDonainName"","" #text"":""NT AUTHORITY""},{""@Name":""SubjectLogonId",""#text"":""0x3E7""},{""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege")]}}"
2025-07-28 19:56:12.6	429,429,2025-07-28 19:56:12.6076704,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808,DESKTOP -5A3QN5S,4,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAscupPrivilege, SeSestorePrivilege, SeDebugPrivilege, SeSestorePrivilege, SeSebelgateSessionUserImpersonatePrivilege*, LogonId: 0x3E7,,False,C:UsersIVM/Desktop\Security.evtx,Audit success,0,"{""EventData"":(""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""), {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""},{""@Name"":""SubjectDomainName"","" ##ext"":""NT AUTHORITY""},{""@Name":""SubjectLogonId"","#text":""0x3E7""},{""@Name":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SePauditPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SePalegateSessionUserImpersonatePrivilege""]}}}"
2025-07-28 19:55:45.8	368,368,2025-07-28 19:55:45.8880090,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QNSS,4,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,,,FaIse,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData":(""@Name"::"SubjectUserSid"","#text"::"S-1-5-18""), {""@Name"::"SubjectUserName",""#text"::"SYSTEM""},(""@Name"::"SubjectDomainName"","" #text"::"NT AUTHORITY"),(""@Name"::"SubjectLogonId",""#text"::"0x3E7""),(""@Name":: ""PrivilegeList","#text"::"SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, "}}}}



_time	_raw
025-07-28 19:55:32.429	353,353,2025-07-28 19:55:32.4297790,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,4,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName"":""SUbjectUserSid"",""#ext"":""S-1-5-18""), {""@Name"":"SubjectUserName"",""#text"":""SYSTEM""),{""@Name"":""SubjectDomainName"","" #text":""NT AUTHORITY""),{""@Name":""SubjectLogonId"","#text":""0x3E7""},{""@Name"": ""PrivilegeList","#text":""SAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilede. SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilede""]}}"
2025-07-28 19:55:29.467	320,320,2025-07-28 19:55:29.4676870,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,3,,Administrative logon,DESKTOP-5A3QN5S\defaultuser0 (S-1-5-21-3151804214-3226339955-2188200191-1000),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3BDD5,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData"\":\"Obata"\":\"\"@Name"\":\"SubjectUserSid"\"\"#text"\":\"S-1-5-21-3151804214-3226339955-2188200191-1000\"\],\"\"@Name\":\"\"SubjectUserName\"\"\"\"#text\"\"\"\"\"defaultuser0\"\},\"\"@Name\"\"\"\"SubjectDomainName\"\"\"\"\"\"DESKTOP-5A3QNSS\"\),\"\"@Name\"\\"\"\"SubjectDomainName\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-28 19:55:13.538	312,312,2025-07-28 19:55:13.5388541,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,DESKTOP -5A3QN5S,3,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTobPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{"""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName"",""#text"":""SYSTEM""],{""@Name"":""SubjectDomainName"","" #text":""NT AUTHORITY""},{""@Name":""SubjectLogonld"","#text*":""0x3E7""},(""@Name"": ""PrivilegeList",""#text":""SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege"]}]}"
2025-07-28 19:55:10.840	304,304,2025-07-28 19:55:10.8409549,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,3,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",Logonld: 0x3E7,,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""}, {""@Name"":""SubjectUserName",""#text"":""SYSTEM""},{""@Name":""SubjectDomainName"",""#text"","""SubjectUserName": """""""""""""""""""""""""""""""""""
2025-07-28 19:55:10.665	302,302,2025-07-28 19:55:10.6657081,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,748,DESKTOP -5A3QN5S,3,,Administrative logon,NT AUTHORITY\SYSTEM (S-1-5-18),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeTokPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeBackupPrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3E7,,FaIse,C:\UserSid","#ext*":"S-1-5-18""), {""@Name":""SubjectUserSid",""#ext*":"S-1-5-18""), {""@Name":""SubjectUserSid","#ext*":""S-1-5-18""), {""@Name":""SubjectUserName","#text*":""SYSTEM"], {""@Name":""SubjectDomainName","#text*":""NT AUTHORITY""), {""@Name":""SubjectLogonId","#text*":""0x3E7""], {""@Name":"""""""""""""""""""""""""""""""""""



New User Creation and Group Addition

New User Creation and Group Addition

Time	Event
2025-07-29T04:54:59+0000	190,190,2025-07-29 04:54:59.6669038,4720,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,808, DESKTOP-5A3QN5S,2,,A new account was created,WORKGROUP\WIN-NOIRN1T9IF6\$ (S.1-5-18),,Target: DESKTOP-5A3QN5S\defaultuser0 (S-1-5-21-3151804214-3226339955-2188200191-1000),,,,,,False,C:\Users\ VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(""@Name":""TargetUserName"" ,""#text"":""Gefaultuser0"),{\""@Name":""TargetDomainName"",""#text":""DESKTOP-5A3QN5S\"" }\;\""@Name":""SubjectUserSid"",""#text"":"S-1-5-21-3151804214-3226339955-2188200191-1000"),{\""}@Name":""SubjectUserSid"","#text":"S-1-5-21-3151804214-3226339955-2188200191-1000"),{\""}@Name":"SubjectUserSid"","#text":"S-1-5-21-3151804214-3226339955-2188200191-1000"),{\""}@Name":""WIN-NOIRN1T9IF6\$\""},{\""@Name":""SubjectUserName"","#text":""WORKGROUP"\"},{\""@Name":""SubjectUserName"","#text":""\"""\"""\"""\"""\"""\"""\""\""\""\""
2025-07-29T04:51:53+0000	43,43,2025-07-29 04:51:53.4850959,4720,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,688,WIN-NOIRN179IF6,0,,A new account was created,MINWINPC\$ (S-1-5-18),,Target: MINWINPCWDAGUtilityAccount (S-1-5-21-3151804214-3226339955-2188200191-504),,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":{""Data"":{""@Name"":"TargetUserName",""#ext*":""MINWINPC""},{;"@Name"":""TargetIDomainName",""#ext*":""MINWINPC""},{;"@Name"":""TargetIOmainName",""#ext*":""MINWINPC"},{;"@Name":""SubjectUserSid",""#text*":""S-1-5-21-3151804214-3226339955-2188200191-504""},{;"@Name":""SubjectUserSid",""#text*":""MINWINPC\$""},{;"@Name":"SubjectUserName","*#text*":""MINWINPC\$""},{;"@Name":""SubjectUserName","*#text*":""MINWINPC\$""},{;"@Name":""SubjectUsomainName"",**#text*":""SuhjectLogonId","*#text*":"""MINWINPC\$""},{;"@Name":""DisplayName",""#text*":""%M1793""},{;"@Name":""SamAccountName"","#text*":""%M1793""},{;"@Name":""BaplayName","#text*":""%M1793""},{;"@Name":""SubjectUserPrincipalName","#text*":""%M1793""},{;"@Name":""SubjectUserPrincipalName","#text*":""%M1793""},{;"@Name":""ScriptPath","#text*":""%M1793""},{;"@Name":""ScriptPath",""#text*":""%M1793""},{;"@Name":""PrincipalName","#text*":""%M1793""},{;"@Name":""PasswordLastSett","#text*":""%M1793""},{;"@Name":""PrincipalName","#text*":""%M1793""},{;"@Name":""PasswordLastSett","#text*":""%M1793""},{;"@Name":""PrincipalName":""#text*":""%M1793""},{;"@Name":""PasswordLastSett","#text*":""%M1793""},{;"@Name":""PrincipalName":""#text*":""%M1793""},{;"@Name":""PasswordLastSett","#text*":"",**#t
2025-07-28T20:03:23+0000	



High-Risk Command Execution

High-Risk Command Execution

Time	Event
2025-07-30T02:40:16+0000	14238,14238,2025-07-30 02:40:16.7514757,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,168,,A new process has been created, \-\-, Parent process: C:\Windows\System32\wininit. exe,PID: 0x2D0,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, "C:\Windows\System32\lsass.exe "_False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"":{ ""@Name"::"SubjectUserSid"",""#text"":"S-1-5-18""},{""@Name"::"SubjectUserSid"",""#text"":"S-1-5-18""},{""@Name"::"SubjectUserName",""#text"":"",{""@Name"::"SubjectUserName",""#text"":"",{""@Name"::"NewProcessId"","#text"":"",{""@Name"::"NewProcessId"","#text"":"",{""@Name"::"TokenElevationType","#text":""."%\1980ang",""@Name":"ProcessId","#text "":"0x2DC"],{""@Name"::"CommandLine"],{""@Name"::"TargetUserSid"","#text "":"0x2CC"],{"@Name"::"TargetUserName","#text":":"","",""@Name"::"TargetDomainName "","#text":"","",("@Name":"TargetLogonId","#text":""0x0"),{""@Name"::"ProcessName":"ProcessName":"ProcessName":"ProcessName":"ProcessName":"" MandatoryLabel"","#text":"C:\\Windows\\System32\\wininit.exe"},{""@Name"::"" MandatoryLabel",""#text":""S-1-16-16384""]}})"
2025-07-30T02:40:16+0000	14237,14237,2025-07-30 02:40:16.6715761,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,168,,A new process has been created,-\-,,Parent process: C:\Windows\System32\winnit. exe,PID: 0x2B8,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C :\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"": \"Data"":\"SubjectServices.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"": \"Data"":\"SubjectUserSid"",""#text"":"S-1-5-18""\(\)\"@Name"":\""\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-30T02:40:16+0000	14236,14236,2025-07-30 02:40:16.5651152,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QNSS,168,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe ,PlD: 0x274,Parent PlD: 0x224,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#text":""-1-5-18"",{""@Name"":""SubjectUserSid"",""#text":""-""},{""@Name"":""SubjectUserName"","#text":""-""},{""@Name":""WeProcessId"",""#text":""-""},{""@Name":""NewProcessId"",""#text":""C:\Windows\System32\winlogon.exe"},{""@Name":""TokenElevationType"","#text":""6%\1966"",{""@Name":""ProcessId"",""#text":""S-1-0-0"},{""@Name":"TargetUserName",""#text":""-"",{""@Name":""TargetUserSid"",""#text":""S-1-0-0"},{""@Name":""TargetUserName",""#text":""-"",{""@Name":""TargetUserSid"",""#text":""S-1-0-0"",{""@Name":""TargetUserName",""#text":""-"",{""@Name":"""TargetUserName",""#text":""-"",{""@Name":"""TargetUserName",""#text":""-"",{""@Name":"""TargetUserName",""#text":""-"",{""@Name":"""","","",""@Name":"""","","","","","","","","",","","","
2025-07-30T02:40:16+0000	14235,14235,2025-07-30 02:40:16.4783622,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,168,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x234,Parent PID: 0x224,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"@Name"":""SubjectUserSid"",""#text"":""5-1-5-18"},{\"@Name":""SubjectUserSid"",""#ext"":""SubjectUserName"",""#text"":""-""},{\"@Name":""SubjectLogonId"","#text":""0x3E7""},{\"@Name":""NewProcessId"","#text":"""0x3E4""},{\"@Name":""TokenElevationType"",""#text":""6\%1936""},{\"@Name":""ProcessId"",""#text":""S-1-0-0"),{\"@Name":""TargetUserName",""#text":""S-1-0-0-"),{\"@Name":""TargetUserName",""#text":""S-1",{\"@Name":""TargetDomainName",""#text":""S-1",{\"@Name":""TargetDomainName",""#text":""Beatter:""
2025-07-30T02:40:16+0000	14234,14234,2025-07-30 02:40:16.4707701,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,168,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x22C,Parent PID: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\wininit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data*":{" "@Name"::""SubjectUserSid", "#text*":""S-1-5-18""},{""@Name"::""S\ SubjectUserName"", ""#text*":""-""},{""@Name":""SubjectUserName"", ""#text*":"""-""},{""@Name":""SubjectLogonld"", "#text*":""0x3E7""},{""@Name"":"NewProcessId"", ""#text*":"""","\"@Name":""TokenElevationType", ""#text*":""0x3E7"",\""@Name":""ProcessId"", ""#text*":""S-1-0-0"",\""@Name":""TargetUserName", "#text*":""S-1-18-16",\""@Name":""TargetDomainName ":""TargetDomainName ":""TargetLogonld", ""#text*":""S-1-16-16384"",\""#text*":""C:\\Windows\\System32\\smss.exe"},\""@Name":""TargetDomainName ":""TargetLogonld", ""#text*":""S-1-16-16384"",\""#text*":""C:\\Windows\\System32\\smss.exe"},\""@Name":""MandatoryLabel "",""#text*":""S-1-16-16384"",\""},\""@Name":""MandatoryLabel "",""#text*":""S-1-16-16384"",\")},\""#text



Time	Event
2025-07-30T02:40:16+0000	14233,14233,2025-07-30 02:40:16.4640074,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,168,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe PID: 0x224,Parent PID: 0x17C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\smss.exe ".False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{{"" QName"":"" SubjectUserSid"",""#text"":""S-1-5-18"",{"" @Name"":"" SubjectDomainName"","" #text"":"""},{"" @Name":"" SubjectDomainName"",""#text"":""",""},{"" @Name":""SubjectLogonId",""#text":""0x3E7"",{"" @Name":""NewProcessId"",""#text":"" "0x224"",{"" @Name":""NewProcessName"",""#text":""C:\\Windows\System32\\smss.exe"",{"" @Name:":"TochElevationType"",""#text":""%%1936"",{"" @Name":""TocessId"",""#text":""S-1 -0-0"),{"" @Name":""TargetUserName",""#text":""CommandLine"),{"" @Name":""TargetUserSid",""#text":""S-1 -0-0"),{"" @Name":""TargetUserName",""#text":""",{"" @Name":""TargetUserName",""#text":""" ParentProcessName",""#text":""C:\\Windows\\System32\\smss.exe""},{"" @Name":""TargetUserName",""#text":""S-1 -0-0-0",,{"" @Name":""TargetUserName",""#text":""",{"" @Name":""TargetUserName",""#text":""S-1 -0-0-0"),{"" @Name":""TargetUserName",""#text":""",{"" @Name":""TargetUserName",""#text":""Dx0"",{"" @Name":""TargetDomainName" ",""#text":""Dx0"",{"" @Name":""TargetDomainName" ",""#text":"" Ox30"",{"" @Name":""MandatoryLabel ",""#text":""C:\\Windows\\System32\\smss.exe""},{"" @Name":""MandatoryLabel ",""#text":""S-1-16-16384""]})}
2025-07-30T02:40:15+0000	14232,14232,2025-07-30 02:40:15.9544921,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,168,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PlD: 0x1E0,Parent PlD: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""" Data":\{\""@Name"\:""SubjectUser\Sid""\"#text\"\:""S-1-5-18\"\},\\"@Name\"\:"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-30T02:40:15+0000	14231,14231,2025-07-30 02:40:15.7572718,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,168,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1D4,Parent PID: 0x17C,\Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""" Data"":\"\""\""SubjectUserSid\"",\""#ext\"":\"">5-1-5-18\""\},\\""@\Name\"":\"""\""\""\""\""\""\""\""\""\""\""\"
2025-07-30T02:40:14+0000	14230,14230,2025-07-30 02:40:14.9807927,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,168,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x198,Parent PID: 0x17C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VM\Desktop\Security.evt,Audit success,0,"{""EventData"":{" "Data"::{" "@Name"::""SubjectUserSid"",""#text*":""S-1-5-18"},{""@Name"::""SubjectUserSid"",""#text*":""-""},{""@Name"::""SubjectDomainName",""#text*":"-""},{""@Name":""SubjectLogonId"","#text*":"""","@Name":""NewProcessId"",""#text*":"""",""@Name":""NewProcessId"",""#text*":"""",""@Name":""TokenElevationType"","#text*":""C:\\Windows\\System32\\autochk.exe*"},{""@Name":""TokenElevationType"","#text*":""@Name":""TargetUserSid"",""#text*":""",""@Name":""TargetUserSid"",""#text*":""","",""@Name":""TargetUserSid"",""#text*":""",",""@Name":""TargetUserName",""#text*":"",",",""@Name":""TargetUserName",""#text*":"",",",""@Name":""",",","@Name":""",",",","@Name":""",",",","@Name":"",",",",",",",",",",",",",",",",",",
2025-07-30T02:40:08+0000	14229,14229,2025-07-30 02:40:08.0790890,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,168,A new process has been created,-\-,-,"Parent process: ",PID: 0x17C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{\""Q Name"":"\""Q Name"":"\"""\"",\""Q Name":"\"""\"",\""\""\"",\""\""\""\""\""\"",\""\""



Time	Event
2025-07-30T02:40:08+0000	14226,14226,2025-07-30 02:40:08.0725003,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,168,,A new process has been created,-\-,,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,1{""EventData":(""Data":!{""@Name"::""SubjectUserSid"",""#text*":"""""""""""""""""""""""""""""""""""
2025-07-30T02:21:42+0000	14080,14080,2025-07-30 02:21:42.3473007,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,167,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2D4,Parent PID: 0x230,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C :\Windows\System32\\sass.exe",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"":{""@Name"":""SubjectUserSid!"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"":""SubjectUserName"":""SubjectDomainName"",""#text"":"",{""@Name"":""SubjectLogonId\",""#text"":""0x3E7""},{""@Name"":"NewProcessId\",""#text\"":""",{""@Name"":""NewProcessId\",""#text\"":""",{""@Name\":""TokenElevationType\",""#text\"":""0x320\",{""@Name\":""TokenElevationType\",""#text\"":""S-1-1-0-0\",{""@Name\":""TargetUserName\",""#text\":"\",""@Name\":""TargetUserSid\",""#text\":"\""S-1-0-0\",{\""@Name\":"TargetUserName\",""#text\":"\"\",{\"@Name\":"TargetDomainName\"\"""ParentProcessName\",""#text\":"\"\",\"@Name\":\""TargetDomainName\"\"""ParentProcessName\",""#text\":\"\"\"\"\"@Name\"\":\"""TargetDomainName\"\"\"""ParentProcessName\"\"\""#text\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-30T02:21:42+0000	14079,14079,2025-07-30 02:21:42.2312994,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,400, DESKTOP-5A3QN5S,167,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x28C,Parent PID: 0x230,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx_Auditi success,0,*(""EventData": \"""SubjectUsers\indexity:=vtx_Auditi success,0,*(""EventData": \"""SubjectUser\indexity:=vtx_Auditi success,0,*(""EventData": \"""SubjectUser\indexity:=vtx_Auditi success,0,*(""EventData": \"""SubjectUser\indexity:=vtx_Auditi success,0,*(""EventData": \"""SubjectUser\indexity:=""""""SubjectUser\indexity:=""""""""""""""""""""""""""""""""""""
2025-07-30T02:21:42+0000	14078,14078,2025-07-30 02:21:42.1181758,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,396, DESKTOP-5A3QN5S,167,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x290,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"":{ "@Name"::""SubjectUserSid",""#text*":""S-1-5-18*"},{"@Name"::""},{""@Name*":""SubjectUserSid","#text*":""S-1*5-18*"},{"@Name*":""*lext*":""-""},{""@Name*":""SubjectLogonId"","#text*":""0x3E7""},{""@Name*":"NewProcessId"","#text*":"""0x3e0""},{""@Name*":"NewProcessId"","#text*":"""0x290""},{""@Name*":"NewProcessId*","#text*":""0x290""},{""@Name*":"TokenElevationType*","#text*":""0x3e1*",""@Name*":""ProcessId*",""#text*":""S-1-0-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0-0"),{""@Name*":""TargetUserName*","#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0"),{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""",""",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserName*",""#text*":""S-1-0",{""@Name*":""TargetUserNa
2025-07-30T02:21:42+0000	14077,14077,2025-07-30 02:21:42.003100,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,400, DESKTOP-5A3QN5S,167,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x238,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\"\""SubjectUserSid"",""#text"":\""S-1-5-18""\},\\""@Name"\"\""SubjectUserName"\",\""#text"\"\"""\"\""\""\""\""\""\""\""\""\""\""



Time	Event
2025-07-30T02:21:41+0000	14076,14076,2025-07-30 02:21:41.9907030,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,396, DESKTOP-5A3QN5S,167,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x230,Parent PID: 0x1DC,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smin.exe ,False,C:\Users\VMDesktop\Security.evtx,Audit success,0,*{""EventData"":{" "Data"":{" "@Name":""SubjectUserSid"",""#text"":""S-1-5-18""},{" "@Name":""},{" "@Name":""SubjectUserSid",""#text"":""S-1-5-18"",*""WayrocessId",""#text"":"",*{" "@Name":""SubjectLogonId",""#text":""0x3E7"},{""@Name":""NewProcessId",""#text":""""",{" "@Name":""NewProcessName",""#text":""C:\\Windows\System32\\wininit.exe"*),{""@Name":""TokenElevationType"",""#text"":""C:\\Windows\System32\\wininit.exe"*],{""@Name":""TargetUserName":"""""""""""""""""""""""""""""""""""
2025-07-30T02:21:41+0000	14075,14075,2025-07-30 02:21:41.9881195,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,396, DESKTOP-5A3QN5S,167,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss,exe ,PID: 0x228,Parent PID: 0x174,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID, Target User: -\-,-,"C:\Windows\System32\smss,exe ,PID: 0x228,Parent PID: 0x174,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID, Target User: -\-,-,"C:\Windows\System32\smss,exe ,PID: 0x228,Parent PID: 0x174,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID, Target User: -\-,-,"C:\Windows\System32\smss,exe ,PID: 0x228,"-\-,""EventData"":{""} Data":\{"@\Ame":""SubjectUserSid", ""#text*":""S-1-5-18"\},\{""@\Ame":""Hext*":""-""},\{""@\Ame":""SubjectUserName"", ""#text*":""""",\{""@\Ame":""NewProcessId", ""#text*":""""\"""\"""\"""\"""\"""\"""\"""\"""\
2025-07-30T02:21:41+0000	14074,14074,2025-07-30 02:21:41.2616234,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,400, DESKTOP-5A3QN5S,167,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1E4,Parent PID: 0x1DC,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."{""EventData"":{""Data"":{\"@Name"":""SubjectUserSid"","#text"":"S-1-5-18""},{""@Name"":""SubjectUserSid"",""#text"":""SubjectUserSid"","#text"":""SubjectUserSid"","#text"":"""},{\"@Name"":""SubjectUserSid"","#text"":"""},{\"@Name"":""NewProcessId"","#text"":"""},{\"@Name"":""NewProcessId"",""#text"":""",{\"@Name"":""NewProcessId"",""#text"":""",{\"@Name":""TokenElevationType",""#text"":""0\%\1936"",{\"@Name":""ProcessId"",""#text":""S-1-0-0"),{\"@Name":"TargetUserName","#text":""-",{\"@Name":"TargetDomainName":""TargetDomainName":""TargetUserName","#text":"":""\",{\"@Name":""TargetDomainName":""ParentProcessName",""#text":""""TargetLogonId","#text":""0x0"",{\"@Name":""TargetDomainName":""ParentProcessName",""#text":""C\\Windows\System32\smss.exe"",{\"@Name":""MandatoryLabel",\""#text":""S-1-16-16384"\}};""C\\Windows\System32\smss.exe"",{\"@Name":""MandatoryLabel",\""#text":""S-1-16-16384"\}}}
2025-07-30T02:21:41+0000	14073,14073,2025-07-30 02:21:41.0844522,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,167, A new process has been created,-\-, Parent process: C:\Windows\System32\smss.exe ,PID: 0x1DC,Parent PID: 0x174,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, "C:\Windows\System32\smss.exe ",False,C:\Users\M\MDesktop\Security.evtx,Audit success,0."\""EventData"":\"" Data"":\\\""\""\""\""\""\""\""\""\""\""\""\"
2025-07-30T02:21:40+0000	14072,14072,2025-07-30 02:21:40.0873133,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,167,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe PID: 0x17A,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sutochk.exe ",False,C:\Users\Vm\Desktop\Security.evtx,Audit success,0,"(""EventData"":(" "Data"":([""@Name":""SubjectUserSid"",""#text":""5-1-5-18""),{(""@Name":"""""}""""""""""""""""""""""""""""""



Time	Event
2025-07-30T02:21:30+0000	14071,14071,2025-07-30 02:21:30.8601134,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,360, DESKTOP-5A3QN5S,167,,A new process has been created,-\-,-,"Parent process: ",PID: 0x174,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\Vm\Desktop\Security.evtx,Audit success,0,"(""EventData"":[""otala"::[{""oName"":""subjectUserSid"",""#ext"":""-""-""-""-""-""-""-""-""-""-""-""-"
2025-07-30T02:21:30+0000	14068,14068,2025-07-30 02:21:30.8539931,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,167,,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData":-{\"attains:"{\"attains:"SubjectUserSid"",""} #text":\"SubjectUserSid\",\"" @Name\":\""SubjectUserSid\",\"" @Name\":\""0x3E7\"{\"attains:"Attains:"\"attains:"\"attains:"\"attains:"\"attains:"\"attains:\"\"attains:\"\"attains:\"\"attains:\"\"attains:\"\"attains:\"\"attains:\"\"\"attains:\"\"attains:\"\"\"attains:\"\"\"attains:\"\"\"attains:\"\"\"attains:\"\"\"attains:\"\"\"attains:\"\"\"\"attains:\"\"\"\"attains:\"\"\"\"\"attains:\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-30T02:18:01+0000	13972,13972,2025-07-30 02:18:01.2431451,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,165,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2D8,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-30T02:18:01+0000	13971,13971,2025-07-30 02:18:01.1867265,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3CN5S,165,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2C4,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C :\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"": {""Data"":{""Cana"":{""Cana"":{""SubjectUserSid",""#text*":""S-1-5-16""},{""@Name"::""SubjectUserName";""#text*":""-""},{""@Name":""SubjectUserName";""#text*":""-""},{""@Name":""SubjectLogonId"","#text*":"""0x3E7""},{""@Name":""NewProcessId"","#text*":""""",""#text*":""""",""@Name":""TokenElevationType",""#text*":""0\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-30T02:18:01+0000	13970,13970,2025-07-30 02:18:01.1072172,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x27C,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sinlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"":{ ""@Name"::"SubjectUserSid",""#textt"::"S-1-5-18""},{""@Name"::""SubjectUserName";""#text":"-""},{"@Name"::"SubjectUserName";""#text":"-""},{"@Name"::"SubjectUserName";""Mext"::"-""},{"@Name"::"SubjectUserName";""Mext"::"-""},{"@Name"::""SubjectUserName";""Mext"::"-""},{"@Name"::""SubjectUserName";""#text"::""","@Name"::""TokenElevationType",""#text"::""C:\\Windows\System32\\windows\System32\\



Time	Event
2025-07-30T02:18:01+0000	13969,13969,2025-07-30 02:18:01.0345553,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x23C,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{{\textit{": "" SubjectUserSidi",""#text"":"" S-1-5-18""},{\textit{"" @ Name"":"" Statest ComainName"",""#text":"""},{\textit{"" @ Name"":"" SubjectUserName"",""#text":""",""},{\textit{"" @ Name"":"" NewProcessId",""#text"":"" 0x32C""},{\textit{"" @ Name":"" NewProcessId","#text":"" 0x32C""},{\textit{"" @ Name":"" TokenElevationType"",""#text"":""0x32C""},{\textit{"" @ Name":"" TargetUserName",""#text":"" S-1-0-0""},{\textit{"" @ Name":"" TargetUserName",""#text":"" S-1-10-0""},{"" @ Name":"" TargetUserName",""#text":"" TargetDomainName "",""#text":"" TargetDomainName "",""#text":"" TargetDomainName "",""#text":"" TargetDomainName "","#text":"" Rownended (",""#text":"" Rownended (",""#text":"" Rownended (",""#text":"" Rownended (",""" Rown
2025-07-30T02:18:01+0000	13968,13968,2025-07-30 02:18:01.0277352,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe ,PID: 0x234,Parent PID: 0x1D8,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\ Windows\System32\wininit.exe",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSidi"",""#text"":""S-1-5-18"),{""@Name"":""SubjectUser\Sidi",""#text"":""SubjectDomainName"",""#text":"""},{""@Name"":""SubjectDomainName"",""#text"":"""},{""@Name":""SubjectLogonIdi",""#text":""0x327""},{""@Name":""NewProcessId",""#text":""""""""""""""""""""""""""""""""""
2025-07-30T02:18:01+0000	13967,13967,2025-07-30 02:18:01.0207150,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x22C,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"" @Name"":""SubjectUserSid": ""#text":""S-1-5-18"\},{"" @Name":"" """ """ """ """ """ """ """ """ ""
2025-07-30T02:18:00+0000	13966,13966,2025-07-30 02:18:00.4255234,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1E8,Parent PID: 0x1D8,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."{""EventData"":{"" Data"":{\"" @Name"":""SubjectUserSid"",""#text"":""S-1-5-18"],{\"" @Name":""" #text"":""-""},{\"" @Name":""SubjectUserSid"",""#text":"""" """ """ """ """ """ """ """ """
2025-07-30T02:18:00+0000	13965,13965,2025-07-30 02:18:00.2330699,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe PID: 0x1D8,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False, C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":""Data"":{\""@Name":-""SubjectUserSid"",""#text":-"">-1-5-18""},{\""@Name":-""SubjectUserSid"",""#text":-"">-1-5-18""},{\""@Name":-""SubjectUserAme"","#text":-""},{\""@Name":-""SubjectDomainName","#text":-""},{\""@Name":-""\subjectDomainName","#text":-""},{\""@Name":-""\subjectDomainName","#text":-""},{\""@Name":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName","#text":-""\subjectDomainName",""#text":-""\subjectDomainName",""#text":-""\subjectDomainName","#text":-""\subjectDomainN



Time	Event
2025-07-30T02:17:59+0000	13964,13964,2025-07-30 02:17:59.5147051,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,165,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PlD: 0x1A0,Parent PlD: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"::""SubjectUserSid"",""#text*":""S-1-5-18""},{""@Name":"""SubjectUserName"",""#text*":"""""""""""""""""""""""""""""""""""
2025-07-30T02:17:51+0000	13963,13963,2025-07-30 02:17:51.2729757,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,165,,A new process has been created,-\-,,"Parent process: ",PID: 0x180,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData":\"\"ata":\"\"ata":\"\"ata":\"\"ata":\"\"subjectUserSid\"\","#text\":\"s-1-5-18\"\"\"\@\Name\":\"\"subjectUserName\"\",\"#text\":\"-\"\"\"\"ata\"\",\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-30T02:17:51+0000	13960,13960,2025-07-30 02:17:51.2656725,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,165,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""QName"":"SubjectUserSid"",""#text*":"""},{""@Name"":""SubjectUserSid"",""#text*":""""},{""@Name"":""SubjectDomainName",""#text*":""""},{""@Name"":""SubjectLogonId"",""#text*":"""",*******************************
2025-07-30T02:16:03+0000	13870,13870,2025-07-30 02:16:03.1353967,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2E0,Parent PID: 0x23C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C :\Windows\System32\sass.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\"EventData"":\""Data"":\""@\Name":\""SubjectUserSid"\"\"#ext\"\""5-1-5-18\"\\""@\Name"\"\"""\""\""\""\""\""\""\""\""\""\""\"
2025-07-30T02:16:03+0000	13869,13869,2025-07-30 02:16:03.0598552,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,164,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2C8,Parent PID: 0x23C,\Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C :\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"": {""Data*":{""Oxata*":{"Oxata*"



Time	Event
2025-07-30T02:16:02+0000	13868,13868,2025-07-30 02:16:02.9686023,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x284,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\windows\System32\windows\System32\smss.exe ,PID: 0x284,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\window
2025-07-30T02:16:02+0000	13867,13867,2025-07-30 02:16:02.8907865,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,A new process has been created, -\-, -, Parent process: C:\Windows\System32\smss.exe ,PID: 0x244,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, -, "C:\ Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0," {""EventData"": {"" Data"": {"" @ Name": "" SubjectUserSid"", ""#text": "" -1-5-18""}, {"" @ Name": "" SubjectUserName", ""#text": "" "" "" "" "" "" "" "" "" "" "" "" "
2025-07-30T02:16:02+0000	13866,13866,2025-07-30 02:16:02.8868168,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x23C,Parent PID: 0x1E0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\wininit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data"":{" "@Name"::""SubjectUserSid"",""#text"::""S-1-5-18"",{""@Name"::""SubjectUserSid"",""#text"::""S",{""@Name"::""SubjectUserSid"","#text"::""SubjectUserName"",""#text"::""SubjectLogonId"","#text"::""SubjectLogonId",""#text"::""SubjectLogonId","#text"::"SubjectLogonId","#text"::""SubjectLogonId","#text"::""SubjectLogonId","#text"::""SubjectLogonId","#text"::""SubjectLogonId","#tex
2025-07-30T02:16:02+0000	13865,13865,2025-07-30 02:16:02.8747252,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x234,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\"@Name"":""SubjectUserSid"","*#text"":""S-1-5-18""},{\"@Name"*:""},{\"@Name"*:""SubjectUserSid"","**text"":""SubjectUserName"","**text*":"""},{\"@Name":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""SubjectLogonId"","**text*":""ProcessId"","**text*":"""ProcessId"","**text*":"""ProcessId"","**text*":""ProcessId"","**text*":""ProcessId"","**text*":""SubjectLogonId"","**text*":""ProcessId"","**text*":""SubjectLogonId"","**text*":""ProcessId"","**text*":""SubjectLogonId"","**text*":""ProcessId"","**text*":""SubjectLogonId"","**text*":""Sub
2025-07-30T02:16:02+0000	13864,13864,2025-07-30 02:16:02.3594387,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,164,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1F0,Parent PID: 0x1E0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,C:\ Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\"" Data"":\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\



Time	Event
2025-07-30T02:16:02+0000	13863,13863,2025-07-30 02:16:02.1463160,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1E0,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ,PID: 0x1E0,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"*:{\mathbb{T}}}
2025-07-30T02:16:01+0000	13862,13862,2025-07-30 02:16:01.3369211,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,372, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1A8,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\sutochk.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"(""EventData"':(" "Data"':[(""@Name":-""SubjectUserSid"","#text"':""S-1-5-18"",(""@Name":-"" SubjectUserName"","#text"":""SubjectUserName"","#text":""SubjectUserName"","#text":""Ox3E7""),(""@Name":-""NewProcessId"","#text":"""SubjectUserName"","#text":""0x3E7""),(""@Name":-"NewProcessId"","#text":"""","",(""@Name":-""NewProcessId"","#text":""","",(""@Name":-""TokenElevationType"","#text":""%\1936""),(""@Name":-""ProcessId"","#text":""#text":""SubjectUserName":""TargetUserSid",""#text":""S-1-0-0"),(""@Name":-""TargetUserSid",""#text":""SubjectUserName":""TargetUserSid",""#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid",""#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""SubjectUserName":""TargetUserSid","#text":""Sub
2025-07-30T02:15:52+0000	13861,13861,2025-07-30 02:15:52.1170232,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,"Parent process: ",PID: 0x180,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\WMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""@Name"":"@Name"":""SubjectUserSid"",""#text"":""-\"},\"@Name":"SubjectUserName",""#text":""-\"},\"@Name":""SubjectDomainName",""#text":"-""-\",\"@Name":""SubjectDogonId",""#text "":""\"\"@Name":""Nx3E7""},\"@Name":""Nx3E7"",\\"@Name":""\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-30T02:15:52+0000	13858,13858,2025-07-30 02:15:52.1078815,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,164,,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData":",(""@Name":""SubjectUserSid"",""#text"":""-"},{\""@Name":""SubjectUserName",""#text"":"-""},{\""@Name":""" "0x3E7"",{\""@Name":""SubjectUserName",""#text":""-""},{\""@Name":""" "0x3E7""},{\""@Name":""" "1,""@Name":""" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,""@Name":"" "1,"" "1,""@Name":"" "1,"" "1,""@Name":"" "1,"" "1,""@Name":"" "1,
2025-07-30T02:07:45+0000	13557,13557,2025-07-30 02:07:45.4236785,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2D4,Parent PID: 0x230,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C \\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\



Time	Event
2025-07-30T02:07:45+0000	13556,13556,2025-07-30 02:07:45.3311898,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160, A new process has been created, \-, \-, Parent process: C:\Windows\System32\wininit. exe,PID: 0x230,Mandatory labe! SECURITY_MANDATORY_SYSTEM_RID,Target User: \-, \-, \-C:\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"": \"\-\Data":\!\(\text{"'eventData"}\): \"\=\text{"'eventData"}\":\"\=\text{"eventData"}\":\"\=\text{"eventData"}\":\"\="eventDat
2025-07-30T02:07:45+0000	13555,13555,2025-07-30 02:07:45.2374871,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x278,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18"},{""@Name"":""SubjectUserName"",""#text"":""SubjectUserName"",""#text":""SubjectUserName"",""#text":""SubjectUomainName",""#text":""\"@Name":""SubjectLogonId"",""#text":""\"%WProcessId"",""#text":""\"0x278"",{""@Name":""NewProcessId",""#text":""\"0x3E7""},{""@Name":""TokenElevationType",""#text":""\%1936""),{""@Name":""ProcessId"",""#text":"" 0x278""},{""@Name":""TokenElevationType",""#text":""\%1936""),{""@Name":""TargetUserSid"",""#text":"" 5-1-0-0"},{""@Name":""TargetUserName",""#text":""-"",{"@Name":""TargetUserSid",""#text":"" 1argetDomainName",""#text":""."",""@Name":""" 1argetDomainName",""#text":""."",""@Name":""" 1argetDomainName",""#text":""."",""@Name":""" 1argetDomainName",""#text":""."",\"@Name":""TargetLogonId",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid",""#text":""0x0"},{""@Name":""TargetUserSid
2025-07-30T02:07:45+0000	13554,13554,2025-07-30 02:07:45.1597569,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,-Parent process: C:\Windows\System32\smss.exe ,PID: 0x238,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\""@Name"":""SubjectUserSid"","#text":""SubjectDomainName",""#text*":"""},{\""@Name"":""SubjectUserName"",""#text*":""SubjectUserName",""#text*":"""""""""""""""""""""""""""""""""""
2025-07-30T02:07:45+0000	13553,13553,2025-07-30 02:07:45.1453404,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,-Parent process: C:\Windows\System32\smss.exe ,PID: 0x230,Parent PID: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\wininit.exe ",False,C:\Users\\\Windows\System32\sminit.exe ",False,C:\Users\\\\Windows\System32\sminit.exe ",False,C:\Users\\\\\Windows\System32\sminit.exe ",False,C:\Users\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-30T02:07:45+0000	13552,13552,2025-07-30 02:07:45.1384858,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A30N5S,160,,A new process has been created,-\-,-Parent process: C:\Windows\System32\smss.exe ,PID: 0x228,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\""@Name"":""SubjectUserSid"",""#text":""SubjectDomainName"",""#text":""""],{\""@Name"":""SubjectUserName"",""#text"":""SubjectUserName",""#text"":""""],{\""@Name"":""SubjectUserName",""#text"":""0x3E7""},{\""@Name"":"NewProcessId"",""#text"":"""""""""""""""""""""""""""""""""



Time	Event
2025-07-30T02:07:44+0000	13551,13551,2025-07-30 02:07:44.6867584,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1E4,Parent PID: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\scrss.exe ",False,C:\Users\M\NDesktop\Security.evtx,Audit success,0,"(""EventData"":["" Data"":[{""@Name":""S-1-5-18""},{""@Name":""S-1-5-18"",\""@Name":""S-1-5-18"",\""" ("" Windows\System32\scrss.exe "),{ """ ("" ("" Windows\System32\scrss.exe "),{ "" ("" ("" Wind
2025-07-30T02:07:44+0000	13550,13550,2025-07-30 02:07:44.4746240,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,204, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe ,PlD: 0x1D4,Parent PlD: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\smss.exe ,PlD: 0x1D4,Parent PlD: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":{"" Data"":{\}"@\Name":""SubjectUserSid",""#text*":"S-1-518"{\}"@\Name":"""\},{\}"@\Name":"""\},{\}"@\Name":"""\},{\}"@\Name":"""\},{\}"@\Name":"""\},{\}"@\Name":"""\},{\}"@\Name":""\},{\},{\}"@\Name":""\},{\},{\}"@\Name":""\},{\},{\}"@\Name":""\},{\},{\},@\Name":""\},{\},{\},@\Name":""\},{\},\},\},\}
2025-07-30T02:07:43+0000	13549,13549,2025-07-30 02:07:43.5571891,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,328, DESKTOP-5A3QN5S,160,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x19C,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data*":{""@Name"":"SubjectUserSid!",""#text*":""5-1-5-18*"],{""@Name*":""SubjectUserName*";""SubjectUserName*",""#text*":""SubjectUserName*",""#text*":""SubjectLogonld!",""#text*":""SubjectLogonld!",""#text*":""SubjectLogonld!",""#text*":""SubjectLogonld!",""#text*":""C\\Windows\System32\autochk.exe*"],{""@Name*":"NewProcessId*",""#text*":""C\\Windows\System32\autochk.exe*"],{""@Name*":"TokenElevationType*",""#text*":""C\\Windows\System32\autochk.exe*"],{""@Name*":""TargetUserName*",""#text*":""S-1-0-0"},{""@Name*":"TargetUserName*","#text*":""-""},{"@Name*":""TargetUserSid*","#text*":""S-1-0-0"},{""@Name*":""TargetUserName*","#text*":""-""},{"@Name*":""TargetUserSid*","#text*":""S-1-0-0"},{""@Name*":""TargetUserName*","#text*":""-""},{"@Name*":""TargetUserSid*","#text*":""Ox0*"},{""@Name*":""TargetUserName*","#text*":""-""},{"@Name*":""TargetUserSid*","#text*":""Ox0*"},{""@Name*":""TargetUserName*","#text*":""-"",{"@Name*":"""TargetUserSid*","#text*":""Ox0*"},{""@Name*":"""""""""""""""""""""""""""""""""""
2025-07-30T02:07:35+0000	13548,13548,2025-07-30 02:07:35.8171655,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A30N5S,160,,A new process has been created,-\-,-,"Parent process: ",PID: 0x180,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\WMDesktop\Security.evtx,Audit success,0,"(""EventData"":[""@Name"::""Data"":[""@Name":"""""""""""""""""""""""""""""""""""
2025-07-30T02:07:35+0000	13545,13545,2025-07-30 02:07:35.8127264,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,160,,A new process has been created,-\-, "Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, "Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0."(""EventData"*:(""Data"*:[""@Name"*:""SubjectUserSid"*",""



Time	Event
2025-07-29T07:19:41+0000	13033,13033,2025-07-29 07:19:41.0343798,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,208, DESKTOP-5A3QN5S,153,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2E0,Parent PID: 0x23C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-29T07:19:40+0000	13032,13032,2025-07-29 07:19:40.9440223,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit. exe,PID: 0x2C4,Parent PID: 0x23C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\services.exe ",False,C:\Users\VMDesktop\Security.evt.Audit success,0,"{""EventData"": {""Data"":{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text":""SubjectDomainName"",""#text":""","",{""@Name"":""SubjectDomainName"",""#text":"","",{""@Name"":""SubjectDomainName"",""#text":"","",{""@Name"":""SubjectDomainName"",""#text":"","","",{""@Name":""TokenElevationType",""#text":"","@Name":""ProcessId",""#text":"","","","","@Name":""TargetDomainName",""#text":"","","@Name":""TargetUserSid",""#text":"","","","","@Name":""TargetUserSid",""#text":"","","","","","","","","","","",","","
2025-07-29T07:19:40+0000	13031,13031,2025-07-29 07:19:40.8859850,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-Parent process: C:\Windows\System32\smss.exe ,PID: 0x2A0,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\swinlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"::{ ""Q Name"::"SubjectUserSid",""#text*":"S-1-5-18"},{""@ Name"::"SubjectUserName":""SubjectUserName":""SubjectUserName":""SubjectLogonId"","#text*":""0x3E7""},{""@ Name*":"NewProcessId*","#text*":""0x2A0""},{""@Name*":"NewProcessName*",""#text*":""0x2A0""},{""@Name*":"TokenElevationType*","#text*":""0x34""},{""@Name*":"ProcessId*","#text*":""S-1-0-0"},{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x34"",{""@Name*":"TargetUserName*","#text*":""0x0"",{""@Name*":""TargetUserName*","#text*":""0x34"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""TargetUserName*","#text*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":""0x00"",{""@Name*":"
2025-07-29T07:19:40+0000	13030,13030,2025-07-29 07:19:40.7557556,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-Parent process: C:\Windows\System32\text{kmss.exe}, PID: 0x244,Parent PID: 0x234,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\text{ksrs.exe}, "False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""SubjectUserSid"",""#text"":""S-1-5-18""},{\""@Name"":""SubjectUserName"",""#text"":""SubjectUserName"",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":""SubjectUserName",""#text":"""SubjectUserName",""#text":"""SubjectUserName",""#text":""""""""""""""""""""""""""""""""""
2025-07-29T07:19:40+0000	13029,13029,2025-07-29 07:19:40.7431627,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,153,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x23C,Parent PID: 0x1E0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smininit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(" "Datata"":(""@Name":""SubjectUserSid"",""#textt":""S-1-5-18""),(""@Name":""SubjectUserName"",""#textt":""-""),(""@Name"":""SubjectUserName"",""#textt":""-""),(""@Name"":""SubjectLOganinName",""#textt":""""),(""@Name"":""NewProcessId"",""#textt":""""),(""@Name"":""Cx\Windows\\System32\\wininit.exe""),(""@Name"":""Cx\Windows\\System32\\wininit.exe""),(""@Name"":""S-1-5-1-0-0""),(""@Name":""TargetUserSid"",""#textt":""S-1-0-0""),(""@Name":""TargetUserName"":""TargetUserSid"",""#textt":""TargetUserName":""TargetDomainName "",""#textt":""","",(""@Name":""TargetLogonId"",""#textt":"">"",("@Name":""TargetDomainName "",""#textt":""","",("@Name":""TargetLogonId"",""#textt":""Datatary \texture \



Time	Event
2025-07-29T07:19:40+0000	13028,13028,2025-07-29 07:19:40.7343099,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,336, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe PID: 0x234,Parent PID: 0x184,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{"@Name":-""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name":-""},{""SubjectUserName"",""#text":""SubjectDomainName":,""#text"::"""},{""@Name":""SubjectDomainName":,""#text"::""",",",""","","","","","","","","","
2025-07-29T07:19:40+0000	13027,13027,2025-07-29 07:19:40.2203621,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,208, DESKTOP-5A3QN5S,153,A new process has been created, - -, Parent process: C:\Windows\System32\sms.exe , PlD: 0x1F0,Parent PlD: 0x1E0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, "C:\Windows\System32\csrss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0."{""EventData"":{""Data"":{\""@Name":""SubjectUserSid"",""#text*":""S-1-5-18""},{\""@Name":"""},{\""@Name":"""},{\""@Name":"""},{\""@Name":"""},{\""@Name":"""},{\""@Name":"""},{\""@Name":"""},{\""@Name":""\"",""},{\""@Name":""\"",""},{\""@Name":""\"","",",\"@Name":""\"","",\"@Name":""\"",\"",\"@Name":""\"",\"",\"",\"",\"",\"",\"",\"",\"",
2025-07-29T07:19:39+0000	13026,13026,2025-07-29 07:19:39.9958118,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,208, DESKTOP-5A3QN5S,153,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1E0,Parent PID: 0x184,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"" @Name"":""SubjectUserSid"", ""#text"":"">-1-5-18"\;\"" @Name"":""*text":""-""},{\"" @Name":""SubjectUserSid"", ""#text":""">"" "" "" "" "" "" "" "" "" "" "" ""
2025-07-29T07:19:39+0000	13025,13025,2025-07-29 07:19:39.0957908,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,312, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe ,PID: 0x1A8,Parent PID: 0x184,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\autochk.exe ",False,C:\Users\\M\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data"":{" @Name"::"SubjectUserSid","#text"::"S-1-5-18"},{"@Name"::"}},\"@Name":"SubjectUserSid","#text":"SubjectDomainName":""SubjectLogonId"","#text":""""",\"@Name":""SubjectLogonId"","#text":"""\"\"@Name":""NewProcessId",""#text":"""\"\"\"@Name":""TokenElevationType","#text":""C:\\Windows\\System32\\autochk.exe"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"
2025-07-29T07:19:28+0000	13024,13024,2025-07-29 07:19:28.7048772,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-,"Parent process: ",PID: 0x184,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Q Name"":""SubjectUserSidi"","*#text*":""S-1-5-18"),{""@ Name":""SubjectUserName","*#text*":""-""},{""@ Name":""SubjectUserName","*#text*":""-""},{""@ Name":""SubjectUserName","*#text*":""Ox184""),{""@ Name":""SubjectLogonIdi","*#text "":""0x3E7""),{""@ Name":""NewProcessIdi","#text*":""0x184""),{""@ Name":"" NewProcessName",""#text*":""C:\\Windows\\System32\\smss.exe"},{\""@ Name":"" TokenElevationType"","#text*":""0x9",{\""@ Name":""ProcessIdi","#text*":""0x4"},{\""@ Name":""TargetUserName","#text*":""S-1-0-0"},{\""@ Name":""TargetUserName","#text*":""S-1-0-0"},{\""@ Name":""TargetUserName","#text*":""S-1-0-0"",{\""@ Name":""TargetUserName","#text*":""S-1-0-0"",{\""@ Name":""TargetUserName","#text*":""S-1-0-0"",{\""@ Name":""TargetUserName","#text*":""S-1-0-0"",{\""@ Name":""TargetUserName","#text*":""S-1-0-0"",{\""@ Name":""TargetUserName",""#text*":""S-1-0-0"",{\""@ Name":""TargetUserName",""#text*":""S-1-0-0"",{\""@ Name":""TargetUserName",""#text*":""S-1-0-0"",{\""@ Name":""TargetUserName","""TargetUserName",""TargetUserName",""TargetUserName",""TargetUserName",""



Time	Event
2025-07-29T07:19:28+0000	13021,13021,2025-07-29 07:19:28.6931714,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,153,,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,1(""EventData":(""Data":[(""@Name"::"SubjectUserSid"",""#text"":""""),""@Name":""SubjectUserSid"",""#text"":"""-"",1(""@Name":""SubjectUserSid"",""#text"":""",1,1(""@Name":"""),1,1(""@Name":"""),1,1(""@Name":"""),1,1(""@Name":"""),1,1(""@Name":""),1,1(""),1,1(""@Name":""),1,1(""@Name":""),1,1(""@Name":""),1,1(""@Name":""),1,1(""@Name":""),1,1(""@Name":""),1,1(""@Name":""),1,1("")
2025-07-29T07:14:46+0000	1093,1093,2025-07-29 07:14:46.7004555,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QNKS,12,,A new process has been created,--,Parent process: C:\Windows\System32\wininit.exe ,PID: 0x2C8,Parent PID: 0x2C2C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\lsass.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0."{""EventData"":{"" Data"":{\""@Name"::"SubjectUserSid"","#text"::"S-1-5-18""},{\""@Name"::""""""""""""""""""""""""""""""""""
2025-07-29T07:14:46+0000	1092,1092,2025-07-29 07:14:46.6545920,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe PID: 0x2BC,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\ Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"":""SubjectUserSid"",""#ext":""-""},{""@Name"::""SubjectUserSid"",""#ext":""-""},{""@Name":""SubjectLoganld"",""#text"":""0x3E7""},{""@Name":""BwProcessld"",""#text":"""0x3E7""},{""@Name":""NewProcessld"",""#text":"""0x3E7""},{""@Name":""NewProcessld"",""#text":"""0x3E0"",(""@Name":""TokenElevationType"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":""TargetUserSid"",""#text":""0x3E7"",{"@Name":"""TargetUserSid"",""#text":""0x3E7"",{"@Name":"""TargetUserSid"",""#text":""0x3E7"",{"@Name":"""TargetUserSid"",""#text":""0x3E7"",{"@Name":"""TargetUserSid"",""#text":""0x3E7"",{"@Name":""""","",{"@Name":""""TargetUserSid"",""#text":""0x3E7"",{"@Name":"""","",{"@Name":"""","",{"@Name":"""","",{"@Name":""","",{"@Name":""","",{"@Name":""","",{"@Name":""","",{"@Name":""","",{"@Name":""","",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":"",",{"@Name":",",{"@Name":",",{
2025-07-29T07:14:46+0000	1091,1091,2025-07-29 07:14:46.5597552,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x274,Parent PID: 0x224,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"*:{{ ""QaName"*:""SubjectUserSid"",""#ext*":"">-1*-5-18*"},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:""""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""},{\""@Name"*:"""}
2025-07-29T07:14:46+0000	1090,1090,2025-07-29 07:14:46.5063343,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x234,Parent PID: 0x224,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,*C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{"@Name"":""SubjectUserSid"",""#text"":"">-1-5-18""},{""@Name":""SubjectUserSid"",""#text"":"">-1-5-18""},{""@Name"":""SubjectUserMainName"",""#text":""-""},{""@Name"":""SubjectUserMainName",""#text":""-"">,{""@Name"":""SubjectUserMainName",""#text":""0x3E7""},{""@Name":""NewProcessId"",""#text":"""",""#text":"""",""#text":""","",{""@Name":""TokenElevationType"",""#text":""0x3E7",{""@Name":""TargetUserName",""#text":""",",{""@Name":""TargetUserName",""#text":""",",{""@Name":""TargetDomainName",""#text":""-"",{""@Name":""TargetUserName",""#text":""",",""@Name":""TargetDomainName",""#text":""TargetLogonId",""#text":""Ox0",,{""@Name":""TargetDomainName",""#text":""TargetOssName",""#text":""TargetOssName",""#text":""TargetOssName",""#text":""TargetOssName",""#text":""TargetOssName",""#text":""S,1-16-16384"]}}}" ParentProcessName",""#text":""C:\\Windows\\System32\\smss.exe"},{""@Name":""MandatoryLabel",""#text":""S-1-16-16384"]}}}"



Time	Event
2025-07-29T07:14:46+0000	1089,1089,2025-07-29 07:14:46.4958085,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,12,,A new process has been created,--,Parent process: C:\Windows\System32\smss.exe, PID: 0x2C,Parent PID: 0x1D0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\smsi.exe, PID: 0x2C,Parent PID: 0x1D0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\smsi.exe, PID: 0x2C,Parent PID: 0x1D0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\sinininit.exe":\""""""""""""""""""""""""""""""""""
2025-07-29T07:14:46+0000	1088,1088,2025-07-29 07:14:46.4948621,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x224,Parent PID: 0x17C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""SubjectUserSid"",""#text"":""S-1-5-18""},{\""@Name"":""SubjectUserName"",""#text"":""S"","""SubjectUserName"",""#text"":""SubjectUserName"",""#text"":""SubjectLogonid",""#text":"""SubjectLogonid",""#text":"""SubjectLogonid",""#text":""""""""""""""""""""""""""""""""""
2025-07-29T07:14:46+0000	1087,1087,2025-07-29 07:14:46.0805736,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1E0,Parent PID: 0x1D0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\"@Name"":""SubjectUserSid"","#text"":""S-1-5-18"},{\"@Name":""SubjectUserSid"","#text"":""SubjectUserName"",""#text"":""SubjectUserName",""#text"":""SubjectLogonId"","#text":""0x3E7""),{\"@Name":"NewProcessId"","#text":"""\"0x3E7""{\"@Name":""TokenElevationType",""#text":""0x3E7"{\"@Name":"TargetUserSid"","#text":""S-1-0-0"{\"@Name":"TargetUserName","#text":""S-1-10-0"{\"@Name":"TargetUserName","#text":""S-1-10-0"{\"@Name":"TargetUserName","#text":""S-1-10-0"{\"@Name":"TargetUserName","#text":""S-1-10-16:16384"\}\}" ParentProcessName",""#text":""C:\\Windows\System32\smss.exe"{\"@Name":"TargetUserName","#text":""S-1-16-16384"\}\}" ParentProcessName",""#text":"C:\\Windows\System32\smss.exe"{\"@Name":"TargetUserName":"TargetUserName":"TargetUserName":"TargetUserName":""TargetUserName":"TargetUserName":""Targ
2025-07-29T07:14:45+0000	1086,1086,2025-07-29 07:14:45.9706264,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1D0,Parent PID: 0x17C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\}""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserSid"",""#text"":""SubjectUserName"",""#text"":""SubjectUserName"",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text"":""SubjectLognid",""#text":""","""",""@Name":""TargetLognid",""#text":""",""",""@Name":""TargetLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid",""#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#text":""SubjectLognid","#tex
2025-07-29T07:14:45+0000	1085,1085,2025-07-29 07:14:45.3822063,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x198,Parent PID: 0x17C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0."{""EventData"":{" "Data"":{" @ Name"::"SubjectUserSid"",""#text"::"S-1-5-18""},{""@ Name"::""SUbjectUserName"",""#text"::"-""},{""@ Name"::"SubjectUserName"",""#text"::"0x3E7""},{""@ Name"::"NewProcessId"",""#text"::""0x3E7"",{""@ Name"::"NewProcessId"",""#text"::""0x3E7"",{""@ Name"::"ProcessId"",""#text"::""0x3E7"",{""@ Name"::"ProcessId"",""#text"::""0x3E7"",{""@ Name"::"ProcessId"",""#text"::""C:\Windows\System32\autochk.exe"",{""@ Name"::""TokenElevationType"",""#text"::"0x3E7",{""@ Name"::"ProcessId"",""#text"::""",{""@ Name"::""TargetUserSid"",""#text"::"",{""@ Name"::""TargetUserSid"",""#text"::"",{""@ Name"::""TargetUserSid"",""#text"::"",{""@ Name"::""TargetUserSid"",""#text"::"",{""@ Name"::""TargetUserSid"",""#text"::"",{""@ Name"::""",{""@ Name"::""",{""@ Name"::""",{""@ Name"::""",{""@ Name"::""",{""@ Name"::""",{""@ Name"::"",{""@ Name"::""",{""@ Name"::"",{""@ Name"::"",{"",{"@ Name"::"",{"",{"@ Name":



Time	Event
2025-07-29T07:14:38+0000	1084,1084,2025-07-29 07:14:38.7165067,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,372, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,-,"Parent process: ",PID: 0x17C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\DesktOp\Security.evt,Audit success,0,"(""EventData"::[""Data"::[""@Name"::""SubjectUserSid":,""#ext*":""-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-"-
2025-07-29T07:14:38+0000	1081,1081,2025-07-29 07:14:38.7098414,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,12,,A new process has been created,-\-,,"Parent process: ",PID: 0x6C,Parent PID: 0x4 ,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"::{""Data"::{""@Name":""SubjectUserSid"","" #text":""Su-1-5-18""},{""@Name":""SubjectUserName"","#text":""-"},{""@Name":""0x3E7""},{""@Name":""SubjectUserName"","#text":""0x3E7""},{""@Name":""NewProcessName"","#text":""-"",*"@Name":""NewProcessName"","#text":"""",*"@Name":""ParentProcessName",""#text":""",*"@Name":""TargetUserSid"","#text":""",*"@Name":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetLogonId"","#text":""0x0"",{""@Name":""TargetLogonId","#text":""0x0"",{""@Name":""TargetLogonId","#text":""0x0"",{""@Name":""TargetLogonId","#text":""S-1-16-16384""}]}}"
2025-07-29T07:09:34+0000	991,991,2025-07-29 07:09:34.1962642,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,300, DESKTOP-5A3QN5S,11,A new process has been created,-\-,-Parent process: C:\Windows\System32\wininit.exe ,PID: 0x2B8,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sass.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\""SubjectUserSid"","#text":\"""SubjectUserSid"","#text":\"""SubjectUserSid"",\""@Name":\""SubjectUserSid"",\""@Name":\""SubjectUserSid"",\""#text"\":\"""SubjectUserSid"\",\""@Name"\":\""SubjectUserSid\"",\""#text\"\":\"""SubjectUserSid\"",\""#text\"\"\""\""\""\""\""\""\""\""\""\"\"\"\
2025-07-29T07:09:34+0000	990,990,2025-07-29 07:09:34.1171443,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,300, DESKTOP-5A3QN5S,11,A new process has been created,-\-,-Parent process: C:\Windows\System32\wininit.exe ,PID: 0x2A4,Parent PID: 0x22C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data"":{ ""@Name"::"SubjectUserSid", ""#text"::"S-1-5-18""},{""@Name"::"},{""@Name"::"SubjectUserName":,"#text":"-""},{"@Name"::"SubjectUserName":,"#text":"-""},{"@Name"::"SubjectUserName":,"#text"::"0x3E7""},{"@Name"::"NewProcessId","#text"::""","#text"::""","@Name"::"TokenElevationType",""#text"::"0x3E7""},{""@Name"::"TargetUserSid",""#text"::""","#text"::""","#text"::""","#text"::"",""@Name"::"TargetUserSid",""#text"::""","#text"::""","#text"::""","#text"::"","
2025-07-29T07:09:33+0000	



Time	Event
2025-07-29T07:09:33+0000	988,988,2025-07-29 07:09:33.8593369,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,11,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x2C,Parent PID: 0x1C0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smsi.exe, PID: 0x2C,Parent PID: 0x1C0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sininit.exe ",False,C:\Users\WinDesktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\"""SubjectUserSid"",\"#text"":\""-\""\" @Name"\":\"""\""\""\""\""\""\""\""\""\""\""\"
2025-07-29T07:09:33+0000	987,987,2025-07-29 07:09:33.8387058,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,11,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x214,Parent PID: 0x20C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{""QName"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name":""SubjectUserName"",""#text"":""SubjectUserName"",""#text"":""SubjectUserName"",""#text"":""SubjectUserName",""#text":"""SubjectUserName",""#text":""SubjectUserName",""#text":"""SubjectUserName",""#text":"""SubjectUserName","#text":"""SubjectUserName","#text":"""SubjectUserName","#text":"""SubjectUserName","#text":""""""""""""""""""""""""""""""""""
2025-07-29T07:09:33+0000	986,986,2025-07-29 07:09:33.8252442,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,11,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x20C,Parent PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName":""SubjectUserSid"",""#text"::"S-1-5-18""},{""@Name":""""},{""@Name":""""},{""@Name":""SubjectUserName"","#text":""\c;\""\c;\""\c;\""\c;\""\c;\""\c;\""\c;\""\c;\""\c;\"\c;\"\c;\"\c;\"\c;\"\c;\"\c;\"\c;\\\c;\"\c;\\\\c;\\\\c;\\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\\c;\\\c;\\\\c;\\\c;\\\c;\\\c;\\\c;\\\\c;\\\c;\\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\\c;\\
2025-07-29T07:09:33+0000	985,985,2025-07-29 07:09:33.3497113,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,11,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1C8,Parent PID: 0x1C0,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""@Name"":""SubjectUserSid"","#text"":""S-1-5-18""},{\""@Name"":""SubjectUserName"",""#text"":""S"SubjectDomainName",""#text"":""{\""@Name":""SubjectLogonid"","#text"":""S"SubjectLogonid"","#text"":""{\""@Name":""SubjectLogonid"","#text"":""{\""@Name":""NewProcessId"","#text"":""{\""@Name":""TokenElevationType"",""#text"":""\""@Name":""ProcessId"",""#text "":""\0x1C8""},{\""@Name":""CommandLine"},{\""@Name":""TargetUserSid"","#text*":""S- 1-0-0""},{\""@Name":""TargetUserName",""#text*":""\;\""@Name":""TargetDomainName "","#text*":""-"},{\""@Name":""TargetLogonid"","#text*":""\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid"","#text*":""\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid"","#text*":""\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid"","#text*":""\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid"","#text*":""\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid"","#text*":"\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid","#text*":"\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid","#text*":"\""@Name":""TargetDomainName "","#text*":""\""@Name":""TargetLogonid","#text*":"\""\""@Name":""TargetDomainName "","#text*":""\""\""@Name":""\""\""\""\""\""\""\""
2025-07-29T07:09:33+0000	984,984,2025-07-29 07:09:33.2605578,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,11,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1C0,Parent PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\"@Name"":""SubjectUserSid"","#text"":""S-1-5-18"},{\"@Name"":""SubjectUserSid"","#text"":""SubjectDomainName",""#text":""""""""""""""""""""""""""""""""""



Time	Event
2025-07-29T07:09:32+0000	983,983,2025-07-29 07:09:32.5996680,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,11,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUser\Sid"","#text"":""S-1-5-18""},{""@Name"":""SubjectUser\Name"":""SubjectDomainName"",""#text"":""},{""@Name"":""SubjectDomainName"",""#text"":""0x3E7""},{""@Name":""NewProcessId"",""#text"":""0x3E7""},{""@Name":""NewProcessId"",""#text":"""","#text":"""","#text":"""","#text":""","#text":""","#text":""TocessId"",""#text":""TargetUserName",""#text":""TargetUserName",""#text":""SubjectDomainName",""#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName",""#text":""","","#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName",""#text":""","#text":""SubjectDomainName","#text":""","#text":""SubjectDomainName","#text":""Subjec
2025-07-29T07:09:26+0000	982,982,2025-07-29 07:09:26.6922264,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QN5S,11,,A new process has been created,-\-,-,"Parent process: ",PID: 0x164,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ", False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":\""Data"":\[""@Name"":\""SubjectUserSid"",\""#text"":\""-"-"-",\""@Name"":\""SubjectUserName"",\""#text"":\"-"-"-",\"",\""@Name"":\""SubjectUserName"\",\""#text"\":\"-"-"-\",\"",\""@Name\":\""SubjectUserName\",\"\"#text\":\"-\"-\",\""\",\""\"@Name\":\"\"-\"\",\"\""\",\""\",\""\",\"\",\"
2025-07-29T07:09:26+0000	979,979,2025-07-29 07:09:26.6823642,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QN5S,11,.A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\Desktop \ Security.evtx,Audit success,0."(""EventData"": ""Datat": """ [""@ Name":"""SubjectUserSid"", ""#text"" """
2025-07-29T06:38:36+0000	877,877,2025-07-29 06:38:36.9321557,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,9,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe, PID: 0x2B0,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\lsass.exe ",False,C:\Users\UMNDesktop\Security.evtx,Audit success,0,"(""EventData"":("" Data"":[{"" QName"":""SubjectUserSid"",""#text"":""S-1-5-18""},("" @Name"":""},{"" QName"":""},{"" QName"":""SubjectUserName"",""#text"":""-"},{"" QName"":""SubjectUserName"",""#text"":""-"},{"" QName":""SubjectUserName"",""#text"":""-"},{"" QName":""SubjectUserName"",""#text":""-"},{"" QName":""NewProcessId"",""#text"":""",""("QName":""NewProcessId"",""#text":""",""("QName":""NewProcessId"",""#text":""",""("QName":""NewProcessId"",""#text":""S-1-10-0"),("" QName":""TargetUserName",""#text":""S-1-10-0"),("" QName":""TargetUserName",""#text":""",""("QName":""TargetUserName",""#text":""",""("QName":""TargetUserName",""#text":""",""("QName":""TargetUserName",""#text":""",""("QName":""TargetUserName",""#text":""",""("QName":""TargetUserName",""#text":""",",""("QName":""TargetUserName",""#text":""",",""("QName":""TargetUserName",""#text":""",",""("QName":""TargetUserName",""#text":""",",""("QName":""TargetDomainName",""#text":""",",",""("QName":""TargetDomainName",""#text":""",",",""("QName":"""TargetDomainName",""#text":""",",",",",",",",",",",",",",",",","
2025-07-29T06:38:36+0000	· · · · · · · · · · · · · · · · · · ·



Time	Event
2025-07-29T06:38:35+0000	875,875,2025-07-29 06:38:35.9846305,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,9,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x258,Parent PID: 0x208,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"::{""Data"::{""@Name"::""SubjectUserSid"",""#text"::""SubjectUserName"::""SubjectUserName"::""SubjectUserName"::""SubjectUserName"::""SubjectUserName"::""SubjectLogonId"",""#text"::"0x3E7""},{""@Name"::"NewProcessId"",""#text"::""0x3E7""},{""@Name"::"NewProcessId"",""#text"::""0x258""},{""@Name"::"TokenElevationType:",""#text"::""0x3E7""},{""@Name"::"TargetUserName"::"TargetUserName"::"TargetUserSid",""#text"::""S-1-0-0"},{""@Name"::"TargetUserName":""TargetUserSid",""#text"::""S-1-0-0"},{""@Name"::"TargetUserName":""TargetUserSid",""#text"::""S-1-0-0"},{""@Name"::""TargetUserName":""TargetUserSid",""#text"::""S-1-0-0"},{""@Name"::""TargetUserName"::"TargetUserName"::""S-1-0-0"},{""@Name"::""TargetUserName"::""TargetUserName"::""S-1-0-0"},{""@Name"::""TargetUserName"::""S-1-0-0"},{""@Name"::""S-1-0-0"},{""@Name"::""S-1-0-0"},{""@Name"::""S-1-0-0"},{""@Name"::""S-1-0-0"},{""@Name"::""S-1-0-0"},{""@Name"::""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":"""S-1-0-0:00,1"":"""S-1-0-0:00,1"":""S-1-0-0:00,1"":"""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":"""S-1-0-0:00,1"":"""S-1-0-0:00,1"":""S-1-0-0:00,1"":"""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S-1-0-0:00,1"":""S
2025-07-29T06:38:35+0000	874,874,2025-07-29 06:38:35.8972455,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,9,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x228,Parent PID: 0x188,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\wininit.exe ",False,C:\Users\\Windows\System32\wininit.exe",""EventData"": "Data"":[""@Name"::"SubjectUserSid"","#text"":""S-1-5-18"],(""@Name":""SubjectUserName"","#text":""-"",{""@Name":""SubjectUserName"","#text"":""0x3E7""},{""@Name":""SubjectDomainName","#text":""-"",{""@Name":""SubjectLogonId",""#text":""0x3E7""},{""@Name":"NewProcessId"",""#text":"""",{""@Name":""TokenElevationType"",""#text":""0x3E7""},{""@Name":""TokenElevationType"",""#text":""0x3E7""},{""@Name":""TargetUserSid"",""#text":""S-1-0-0"",{""@Name":""TargetUserName",""#text":""S-1-0-0"",{""@Name":""TargetUserName",""#text":""S-1-0-0"",{""@Name":""TargetUserName",""#text":""S-1-1-16-16384"")}},""@Name":""TargetLogonId","#text":""\",{""@Name":""TargetDomainName":""ParentProcessName",""#text":""C:\\Windows\System32\\smss.exe"",{""@Name":""S-1-16-16384"")}})" ParentProcessName",""#text":""C:\\Windows\System32\\smss.exe""),{""@Name":""MandatoryLabel",""#text":""S-1-16-16384"")}})"
2025-07-29T06:38:35+0000	873,873,2025-07-29 06:38:35.8843618,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,9,,A new process has been created,-\-,Parent process: C:\Windows\System32\smss.exe, PID: 0x210,Parent PID: 0x208,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,1{""EventData"":{"" Data"":{"" QName":""SubjectUserSid"",""#text"":"S-1-5-18""},{"" QName"":""},{"" QName"":""},{"" QName"":""},{"" QName":"""},{"" QName":"""},{"" QName":""NewProcessId"",""#text":"","","","","","","","","","","","",""
2025-07-29T06:38:35+0000	872,872,2025-07-29 06:38:35.8713876,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,316, DESKTOP-5A3QN5S,9,A new process has been created,-\-,-,Parent process: C:Windows\System32\smss.exe, PID: 0x208,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\}""SubjectUserSid"",""#text"":""S-1-5-18""},{\}""@Name"":""SubjectUserSid",""#text"":""SubjectUserName"",""#text"":"""),{\}""@Name":""SubjectLogonid",""#text":"""\"""\"""\"""\"""\"""\"""\""\""\""\"
2025-07-29T06:38:35+0000	871,871,2025-07-29 06:38:35.2611127,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,336, DESKTOP-5A3QN5S,9,A new process has been created,--,Parent process: C:Windows\System32\smss.exe, PID: 0x1C4,Parent PID: 0x1B8,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"" @Name"":"" SubjectUserSid"","#text":""S-1-5-18"},{\"" @Name":"" "" "" "" "" "" "" "" "" "" "" "" ""



Time	Event
2025-07-29T06:38:35+0000	870,870,2025-07-29 06:38:35.1045841,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,9,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1B8,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID, Target User: -\-,-,"C:\Windows\System32\smss.exe
2025-07-29T06:38:34+0000	869,869,2025-07-29 06:38:34.4433715,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,228, DESKTOP-5A3QN5S,9,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x17C,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,*C:\Windows\System32\sutochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data"":{\"" @ Name":""SubjectUserSid"", ""#text":""S-1-5-18""},{\"" @ Name":"":""-""},{\"" @ Name":""" """ """,\"" @ Name":""" """ """ """ """ """ """ """ """ "
2025-07-29T06:38:29+0000	868,868,2025-07-29 06:38:29.0263182,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QNSS,9,A new process has been created,-\-,-,"Parent process: ",PID: 0x15C,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ", False,C:\Users\\WinDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Oata"":{""@Name"":""} SubjectUsers\indications**."">SubjectUsers\indications**.""**[""@Name"":""SubjectUser\indications**.""*,"#textt":""-"", {""@Name":""SubjectLogonId"","#textt"":""-", {""@Name":""SubjectLogonId"","#textt"":""-", {""@Name":""NewProcess\indications**.""*,""@Name":""*,""@Name":""* "\""@Name":""*,""*,""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""@Name":""*,""*,""@Name":""*,""*,""@Name":""*,""*,""@Name":""*,""*,""*,""*,""*,""*,""*,""\
2025-07-29T06:38:29+0000	865,865,2025-07-29 06:38:29.0229667,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QNSS,9,A new process has been created,-\-,-"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-"Registry ",False,C:\Users\VM\Desktop\Security. evtx,Audit success,0."(""EventData"":{""Data"":{""Qame":-"SubjectUserSid"",""#text"":""S-1 -5-18""),{""@Name":-""SubjectUserName", "#text":"-""},{"@Name":-""SubjectUserSid"",""#text"":"0x3E7""),{""@Name":-""SubjectDomainName", "#text":""-"",{"@Name":-""NewProcessName", "#text"":""\#ext":""\#ext":"\#e
2025-07-29T06:29:34+0000	



Time	Event
2025-07-29T06:29:34+0000	748,748,2025-07-29 06:29:34.1005808,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe, PID: 0x29C,Parent PID: 0x20C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evx,Audit success,0,"\""EventData"":\""Data"":\""@\Name":\""SubjectUser\Sid",\""#text"\:\""S-1-5-18"),\\""@\Name":\""SubjectUser\Name\"\"\""\""SubjectUser\Name\"\\"\""\""SubjectDomain\Name\"\\"\"#text\"\\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\
2025-07-29T06:29:34+0000	747,747,2025-07-29 06:29:34.0155738,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x270,Parent PID: 0x204,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\windows\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\System32\System32\\S
2025-07-29T06:29:33+0000	746,746,2025-07-29 06:29:33.9348466,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x218,Parent PID: 0x204,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":("" Data"":\""" \
2025-07-29T06:29:33+0000	745,745,2025-07-29 06:29:33.9144362,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,8,A new process has been created,-\-,,Parent process: C:Windows\System32\smss.exe, PID: 0x20C,Parent PID: 0x1B4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\wininit.exe ",False,C:Users\VMDesktop\Security,evtx,Audit success,0,"\""EventData"":\""Butar":\"\""\""\" \" \" \" \" \" \" \" \" \" \"
2025-07-29T06:29:33+0000	744,744,2025-07-29 06:29:33.9074920,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,8,A new process has been created,-\-,.Parent process: C:Windows\System32\smss.exe, PID: 0x204,Parent PID: 0x150,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"" @Name"":""SubjectUserSid"","#text":""S-1-5-18"},{\"" @Name":"""},{\"" @Name"":""},{\"" @Name"":""SubjectUserSid"",""#text":""-""},{\"" @Name":""SubjectUserName"",""#text":""-""},{\"" @Name":""SubjectLogonId"",""#text":""0x3E7""},{\"" @Name":"NewProcessId"",""#text":"""""","""",""",""",""",""",""","","",



Time	Event
2025-07-29T06:29:33+0000	743,743,2025-07-29 06:29:33.4793646,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1C0,Parent PID: 0x1B4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""@Name"":""SubjectUserSid"",""#text"":""5-1-5-18""{\""@Name"":""}""}" SubjectUserName"",""#text"":"-"",{\""@Name":""SubjectDomainName"",""#text"":""-""},{\""@Name":""Ox3E7""},{\""@Name":""NewProcessId",""#text":""",""\\""@Name":""\""\""\""\""\""\""\""\""\""\""\""\""
2025-07-29T06:29:33+0000	742,742,2025-07-29 06:29:33.3412413,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,356, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x184,Parent PID: 0x150,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\UMDesktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{{\textit{"}."".""}},{\textit{"}.""*subjectUser\Sid",""#text"":""S-1-5-18""},{\textit{"}."@Name"":"" SubjectUser\Name"":"" SubjectUser\Name"":""SubjectUser\Name"":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""SubjectUser\Name":""Subject\Opanin\Name":""#text":"""\{\textit{"}."""0x3E7""},{\textit{"}."@Name":""NewProcess\d",""#text":"""""\",{\textit{"}."""0x3E7""},{\textit{"}."@Name":""NewProcess\d",""#text":"""\",{\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}."""\textit{"}.""\texti
2025-07-29T06:29:32+0000	741,741,2025-07-29 06:29:32.6528407,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QNSS,8,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe,PlD: 0x178,Parent PlD: 0x150,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sutochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(""Data"":([""@Name"::"SubjectUserSid",""#text":""SubjectUserName"",""SubjectUserName"","""SubjectUserName",""#text":""""],(""@Name"::""SubjectUserName",""#text":""""],(""@Name"::""\text"::""\text":""\text"::""\text"::""\text"::""\text"::""\text"::""\text"::"\text:::"\text:
2025-07-29T06:29:29+0000	740,740,2025-07-29 06:29:29.4714724,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QNSS,8,A new process has been created,-\-,-,"Parent process: ",PID: 0x150,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ", False,C:\Users\\M\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""Qame"":""SubjectUsers\sid",""#text":""-"},
2025-07-29T06:29:29+0000	737,737,2025-07-29 06:29:29.4660248,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QN5S,8,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\Desktop\Security. evtx,Audit success,0."(""EventData"":([""@Name"":""SubjectUserSid"",""#text"":""S-1 -5-18""),(""@Name"::""SubjectUserName"","#text":"-""),(""@Name"":""SubjectUserSid"","#text":""0x3E7""),(""@Name"":""SubjectDomainName"","#text":"""),(""@Name"":""SubjectLogonId"",""#text"":""0x3E7""),(""@Name"":""SubjectDomainName"","#text":"""),(""@Name"":""SubjectLogonId"",""#text"":""0x3E7""),(""@Name"":""SubjectLogonId"",""#text"":""0x3E7""),(""@Name"":""SubjectLogonId"",""#text"":"0x3E7""),(""@Name"":""SubjectLogonId"",""#text"":"0x3E7""),(""@Name"":""SubjectLogonId"","#text":""0x3E7""),(""@Name"":""TargetUserSid"",""#text"":""SubjectLogonId"",""#text"":""TargetUserSid"",(""@Name"":"TargetUserSid"",(""@Name"":"TargetUserSid"",(""@Name":""TargetOomainName"","#text":""-"),(""@Name":""TargetUserName"","#text":""-"),(""@Name":""TargetUserName"","#text":""-""),(""@Name":""TargetUserName"","#text":""-""),(""@Name":"""SubjectUserName":"""","#text":""-""),(""@Name":""""),(""@Name":"""""),(""@Name":""""),(""@Name":""""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),(""@Name":""),("",("",""),(""@Name":""),("",("",""),("",",""),("",",","),("",",",",



Time	Event
2025-07-29T04:54:50+0000	166,166,2025-07-29 04:54:50.5332860,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\\wininit.exe, PID: 0x2AC,Parent PID: 0x21C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\\sass.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":[{""@Name":-""SubjectUserSidi",""#text"":""5-1-5-18""},{""@Name":-""},{""@Name":-""},{""@Name":-""SubjectDomainName"",""#text":-""},{""@Name":-""SubjectLogonId",""#text":-""},{""@Name":-""NewProcessId",""#text":-""},{""@Name":-""NewProcessId",""#text":-"",{""@Name":-""NewProcessId","#text":-"",{""@Name":-""TokenElevationType",""#text":-""%,{""@Name":-"TargetUserSid",""#text":-""S-1-0-0"],{""@Name":-""TargetUserName",""#text":-"",{""@Name":-""TargetDomainName":-""TargetDomainName":-""TargetDomainName":-""TargetDomainName":-""TargetDomainName":-""#text":-"",{""@Name":-""TargetLogonId",""#text":-""},{""@Name":-""TargetDomainName":-""Ta
2025-07-29T04:54:50+0000	165,165,2025-07-29 04:54:50.4525923,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\wininit.exe, PID: 0x2A4,Parent PID: 0x21C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,*C:\Windows\System32\services.exe",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,*[*"EventData"":{""Data"*:[{""@Name"*:""SubjectUserSid"","*#text*":""S-1-5-18"},{""@Name*":"""SubjectUserName"",""#text*":"""""""""""""""""""""""""""""""""""
2025-07-29T04:54:50+0000	164,164,2025-07-29 04:54:50.2524369,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x25C,Parent PID: 0x20C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\winlogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{ ""Data":!{""@Name"::""SubjectUserSid"",""#ext*":""S-1-5-18""},{""@Name"::""SubjectUserName"",""#text*":""-""},{""@Name":""NewProcessId"",""#text*":"""""""""""""""""""""""""""""""""""
2025-07-29T04:54:50+0000	163,163,2025-07-29 04:54:50.1473384,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,.A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x21C,Parent PID: 0x1B8,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\winnit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name"::""SubjectUserSid"",""#text"::""S-1-5-18"),{""@Name":""SubjectUserSid"",""#text"":""-""},{""@Name":""SubjectUserName"",""#text"":""-""},{""@Name":""SubjectLogonId"",""#text":""-""},"@Name":""NewProcessId",""#text"::""""","@Name":"""""""","""""",""""""""""""""""""""
2025-07-29T04:54:50+0000	162,162,2025-07-29 04:54:50.1471979,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x214,Parent PID: 0x20C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"@Name"":""SubjectUserSid"",""#text"":""5-1-5-18""},{\"@Name"":""SubjectUserName"",""#text"":""-""},{\"@Name":""SubjectLogonld"",""#text":""-""},{\"@Name":""NewProcessId"",""#text":""-"",{\"@Name":""TokenElevationType"",""#text":""0x3E7"",{\"@Name":""TokenElevationType"",""#text":""0\%196""),{\"@Name":""TargetUserName",""#text":""-17.\(\)("@Name":""TargetUserName",""#text":""-17.\(\)("@Name":""TargetDomainName",""#text":""-17



Time	Event
2025-07-29T04:54:50+0000	161,161,2025-07-29 04:54:50.1246233,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,,A new process has been created,-\-,-Parent process: C:\Windows\System32\smss.exe, PID: 0x20C,Parent PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-\"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0."\""EventData"":\""" Data"":\"""""""""""""""""""""""""""""""""
2025-07-29T04:54:49+0000	160,160,2025-07-29 04:54:49.6946800,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,216, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1C8,Parent PID: 0x1B8,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,*C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""QName":""SubjectUserSid"",""#text*":""5-1-5-18""},{""@Name"*:""} SubjectUserName"",""#text*":"-""},{""@Name":"SubjectDomainName"",""#text*":""-""},{""@Name":""Ox3E7""},{""@Name":"NewProcessId"","#text*":"""},{""@Name":""Toxing************************************
2025-07-29T04:54:49+0000	159,159,2025-07-29 04:54:49.5201004,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,240, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x188,Parent PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"" @Name"":""SubjectUserSid"",""#text"":"">-1-5-18""},{\"" @Name"":"" SubjectUserName"",""#text"":""-""},{\"" @Name"":""SubjectUserName"",""#text"":""-""},{\"" @Name"":""NewProcessId"",""#text"":"""",""#text"":""" 0x188""),{\"" @Name"":""C:\Windows\\System32\\smss.exe""},{\"" @Name":""TokenElevationType",""#text"":""0x164""},{\"" @Name"":"TargetUserSid"",""#text":""S-1-0-0""},\"" @Name"":"TargetUserName"",""#text":"""",""@Name":""TargetUserSid"",""#text":""S-1-10-10",\"" @Name"":""TargetUserName",""#text":"""",""@Name":""TargetUserName",""#text":""">-"",\"" @Name":""TargetUserName",""#text":""S-2-1-10-10",\"" @Name":""TargetUserName",""#text":""S-2-1-16-16384"",\""#text":""C:\\Windows\\System32\\smss.exe",\""@Name":""MandatoryLabel"",""#text":""S-1-16-16384"",\"""
2025-07-29T04:54:48+0000	158,158,2025-07-29 04:54:48.7751665,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,1,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x180,Parent PID: 0x164,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\autochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{" "Data":!{" @Name"::"SubjectUserSid"", "#text*":""S-1-5-18""}, ""@Name"::""S\ SubjectUserName"", ""#text*":""-""}, ""@Name*":""SubjectUserName"", ""#text*":""-""}, ""@Name*":""SubjectLogonId*", ""#text*":""0x3E7""}, ""@Name*":""NewProcessId*", ""#text*":"" 0x180""}, "@Name*":"NewProcessName*", ""#text*":""C:\\Windows\\System32\autochk.exe*"}, ""@Name*":""TokenElevationType*", ""#text*":""0x164""}, "@Name*":""ProcessId*", ""#text*":""S-1-0-0"), ""@Name*":"TargetUserName*", ""#text*":""", ""@Name*":""TargetUserName*", ""#text*":"", ""@Name*":""TargetUserName*", ""#text*":"", ""@Name*":"" 0x180"", "@Name*":"TargetUserName*", ""#text*":"", "", "@Name*":""TargetUserName*", ""#text*":"", "", "@Name*":"" 0x180"", ""@Name*":"TargetUserName*", ""#text*":"", "", ""@Name*":"" 0x180"", ""@Name*":"TargetUserName*", ""#text*":"", "", "", "@Name*":"" 0x180"", ""@Name*":"TargetUserName*", ""#text*":"", "", "", "@Name*":"" 0x180"", ""@Name*":""TargetUserName*", ""#text*":"", "", "", "@Name*":"" 0x180"", ""@Name*":""TargetUserName*", ""#text*":"", "", "", "@Name*":"" 0x180"", ""#text*":"", "", ", "@Name*":"", "", ", "@Name*":"" 0x180", "", ""#text*":"", "", ", ", "@Name*":"" 0x180", "", "", ", ", ", ", ", ", ", ", ", ",
2025-07-29T04:54:47+0000	157,157,2025-07-29 04:54:47.5993818,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,1,A new process has been created,-\-, "Parent process: ",PID: 0x164,Parent PID: 0x4 ,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, "C:\Windows\System32\smss.exe", False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Q Name"":""SubjectUserSid"",""#text":""-"", ""@ Name":""SubjectUserName":""#text":""-"", ""@ Name":""SubjectUserName":""#text":""-"", ""@ Name":""SubjectUserName":""#text":""-"", ""@ Name":""Name":""\"",""@ Name":""\"",""@ Name":""\"",""@ Name":""\"",""@ Name":""\"",""@ Name":""\"",""\"", "\"@ Name":""\"\"", "\"@ Name":""\"\"", "\"@ Name":""\"""\", \"@ Name":""\"""\", \"""""\", \""""""""



Time	Event
2025-07-29T04:54:47+0000	154,154,2025-07-29 04:54:47.5743079,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,DESKTOP -5A3QN5S,1,,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:Users\VM\Desktop\Security.evtx,Audit success,0."(""EventData":"[""Data":"[(""@Name"::""SubjectUserSid"",""#textt"::""S-1 -5-18""],(""@Name"::"SubjectUserName"",""#textt"::"""],"("@Name"::""SubjectDomainName",""#textt"::""],"("@Name"::""SubjectLogonId","#textt"::"0x3E7""),{ ""@Name"::"NewProcessId",""#textt":"0x6C""},(""@Name"::"NewProcessName",""#textt"": ""Registry""},(""@Name"::"TokenElevationType"","#text"::"%\1936""),(""@Name"::"TargetUserSid"", ""#textt":""S-1-0-0"),{ ""#text":""S-1-0-0"},{ ""#text":""S-1-0-0",(""@Name"::"TargetUserName",""#text":"",""),(""@Name":""TargetUserSid"", ""#text":""S-1-1-0-1",(""@Name"::"TargetUserName",""#text":"",""),(""@Name":"""] ""TargetDomainName",""#text":"",(""@Name"::""ArgetUserOgonId",""#text":""0x0"),("""@Name":""""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":"""),(""@Name":""),(""@Name":"""),(""@Name":""),(""@
2025-07-29T04:51:52+0000	14,14,2025-07-29 04:51:52.5896285,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128,WIN-N0IRN1T9IF6,0,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe,PID: 0x2AC,Parent PID: 0x210,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\wininit.exe,PID: 0x240,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\wininit.exe,"c:\windows\System32\wininit.exe,"c:\windows\System32\wininit.exe,"\",""Enabeta (""") at """ at
2025-07-29T04:51:52+0000	13,13,2025-07-29 04:51:52.5029430,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-N0IRN1T9IF6,0,,A new process has been created,-\-,.Parent process: C:Windows\System32\wininit.exe,PID: 0x29C,Parent PID: 0x210,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":["Data" ":[""@Name":""SubjectUserSid"".""#ext":""S-1-5-18""],(""@Name":""SubjectUserName"" ""#ext"":""-""),(""@Name":""SubjectUserName"" ""#ext"":""-"",(""@Name":""SubjectUserName"" ""#ext"":""-"",(""@Name":""WewProcessId"",""#ext":""0x29C""),("""@Name":""SubjectUserName"" ""#ext"":""",(""@Name":"""),(""@Name":"""0x29C""),("""#ext":""0x29C""),(""#ext":""0x29C""),("""#ext":""0x29C""),(""#ext":""0x29C"")
2025-07-29T04:51:52+0000	12,12,2025-07-29 04:51:52.3917041,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-NOIRN179IF6,0,,A new process has been created,-\-,-,Parent process: C:Windows\System32\smss.exe,PID: 0x274,Parent PID: 0x208,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sminogon.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data" ":"{\text\circle*{\text\c
2025-07-29T04:51:52+0000	11,11,2025-07-29 04:51:52.2702895,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-N0IRN1T9IF6,0,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe,PID: 0x218,Parent PID: 0x208,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"": ""Data"": ""SubjectUserSid"",""#text":""S-1-5-18"",{""@Name":""SubjectUserName""," "#text":""""]-\-,{""@Name":""SubjectUserSid"",""#text":"""",{""@Name":""0x218""},{""@Name":""SubjectLogonId"","#text":""0x218""},{""@Name":""NewProcessId",""#text":""0x218""},{""@Name":""TokenElevationType",""#text":""S-1-0-0"",{""@Name":""TokenElevationType",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""@Name":""TargetUserName"",""#text":""S-1-0-0"",{""#text":""S-1-0-0"",{""#text":""","","","@Name":""TargetUserName",""#text":""","","","@Name":""TargetUserName",""#text":""","","","@Name":""","","","@Name":""MandatoryLabel",""#text":"" S-1-16-16384"*]}}



Time	Event
2025-07-29T04:51:52+0000	10,10,2025-07-29 04:51:52.2699294,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-N0IRN1T9IF6,0,,A new process has been created,-\-,,Parent process: C:Windows\System32\smss.exe,PID: 0x210,Parent PID: 0x1BC,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows \System32\smininit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"\""EventData"":\""Data"":\"\""Data"":\"\"""Data"":\"\""""SubjectUserSubjectUserSame"",\"""#cx""",\""" @Name"":\""SubjectUserName"",\"""#text"":\""",\""" @Name"\":\"""",\""" @Name\"":\"""\""" \SubjectUserName\"",\""" \SubjectUserName\"",\""" \SubjectLogonId\"\""#text\":\"\"0x3E7\"\"\"" @Name\"\:\"\""\"\""\"\""\"\"\"\"\"\"\"\"\"\"
2025-07-29T04:51:52+0000	9,9,2025-07-29 04:51:52.2518688,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-NOIRN179IF6,0,A new process has been created,-\r.,Parent process: C:\Windows\System32\smss.exe,PID: 0x208,Parent PID: 0x15C,Mandatory label: SECURITy_MANDATORY_SYSTEM_RID; arrayet User: -\r.,"C:\Windows\System32\smss.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"": ""Data"": ""Data"": """Data"": """SubjectUserSid", ""#text":""S-1-5-18""},{""@Name":""SubjectUserSid"", "#text":""S-1-5-18""},{""@Name":""SubjectUserName", ""#text":""","",{""@Name":""SubjectUserName", ""#text":""","",{""@Name":""SubjectUserName", ""#text":""","",{""@Name":""SubjectUserName", ""#text":"","",{""@Name":""SubjectUserName", ""#text":"","",{""@Name":""SubjectUserName", ""#text":"","",{""@Name":""NewProcessId","#text":""0x208"",{""@Name":"""",""@Name":"""",""@Name":""","",""@Name":""","",""@Name":"","","",""@Name":"","","",""@Name":"","",","","@Name":"","",",",",",",",",",",",",,,,,,,,,,
2025-07-29T04:51:51+0000	8,8,2025-07-29 04:51:51.8583750,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,92,WIN-NoIRN179IF6,0,,A new process has been created,-\-,-,Parent process: C:Windows\System32\smss.exe,PID: 0x1C8,Parent PID: 0x1BC,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows \System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data""
2025-07-29T04:51:51+0000	7,7,2025-07-29 04:51:51.2518534,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,300,WIN-NOIRN179IF6,0,,A new process has been created,-\-,,Parent process: C:Windows\System32\smss.exe,PID: 0x1BC,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\smss.exe,"False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data""
2025-07-29T04:51:51+0000	6,6,2025-07-29 04:51:51.0082255,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,300,WIN-NOIRN1T9IF6,0,,A new process has been created,-\-,,Parent process: C:Windows\System32\smss.exe,PID: 0x148,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\setupcl.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0," (""EventIbata"": (""Data" ";""#ext"": """)," (""@Name"": ""SubjectUserSid"", ""#text": """-")," (""@Name"": ""SubjectUserName"" ""#text"": """-""," (""@Name": ""SubjectUserSid"", ""#text": ""-"")," (""@Name": """)," (""),"



Time	Event
2025-07-29T04:51:49+0000	5,5,2025-07-29 04:51:49.4893916,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,320,WIN-NOIRN1T9IF6,0,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe,PID: 0x170,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sutochk.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"\"EventData"":\"\"Data"":\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\\
2025-07-29T04:51:47+0000	4,4,2025-07-29 04:51:47.5654947,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-NOIRN1T9IF6,0,,A new process has been created,-\-,,"Parent process: ",PID: 0x15C,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\smss.exe ", False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData":-{"Data"::{\"Data"::{\"Data"::{\"Name"::""}} \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \ \
2025-07-29T04:51:47+0000	1,1,2025-07-29 04:51:47.5411715,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32,WIN-NOIRN179IF6,0,,A new process has been created,-\-, "Parent process: ",PID: 0x70,Parent PID: 0x4, Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-, ,"Registry ",False,C:\Users\VM\Desktop \Security.evtx,Audit success,0,"(""EventData":"{""a} Name":""subjectUserSid"",""#text*": ""s-5-18"),{""@Name":""SubjectUserName" ",""#text*":""s",""@Name":""SubjectUserSid"",""#text*": ""s-5-18"",{""@Name":""SubjectUserName",""#text*":""subjectLogonId"","#text*":"0x3E7"*],{ ""@Name":"NewProcessId"","#text*":""0x70"",{"@Name":"NewProcessName","#text*" :""Registry"",{"@Name":"TokenElevationType",""#text*":""%41936""},{""@Name":"TargetUserSid"",""#text*":""S-1-0-0"},{"@Name":"TargetUserName","#text*":""-"",{"@Name":"TargetUserSid"",""#text*":""s-1-0-0"},{"@Name":""TargetUserName","#text*":""-"",{"@Name":""TargetUserSid"",""#text*":""0x0"",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""TargetUserSid"",""#text*":""0x1",{""@Name":""""""""],{""@Name":"""""""""""""""""""""""""""""""""""
2025-07-29T03:44:31+0000	6383,6383,2025-07-29 03:44:31.9535012,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,,Parent process: C:Windows\System32\wininit.exe ,PID: 0x2D0,Parent PID: 0x230,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\ Windows\System32\sass.exe ",False,C:\Users\VMDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{\""@Name"":""SubjectUserSid",""#text"":""S-1-5-18"],{""@Name":""SubjectUserName"",""#text"":""SubjectUserName"",""#text":"""SubjectLogonId",""#text":""SubjectLogonId",""#text":""SubjectLogonId",""#text":""C:\\Windows\System32\\sass.exe"),{ ""@Name":""SubjectLogonId",""#text":""C:\\Windows\\System32\\sass.exe"),{ ""@Name":""TokenElevationType",""#text":""%4136"",\""@Name":""ProcessId",""#text "":""0x230"},\{\"@Name":"CommandLine"},\(\"@Name":"TargetUserSid",""#text":""S- 1-0-0"),\(\"@Name":"TargetUserName","#text":""-"),\(\"@Name":"TargetDomainName "",""#text":""-"",\(\"@Name":""TargetLogonId",""#text":""Ox0"'},\(\"@Name":""TargetDomainName "",""#text":""C:\\Windows\\System32\\wininit.exe"),\(\"@Name":""TargetDomainName "",""#text":""C:\\Windows\\System32\\wininit.exe"),\(\"@Name":""TargetDomainName "",""#text":""C:\\Windows\\System32\\wininit.exe"),\(\"@Name":""TargetDomainName "",""#text":""C:\\Windows\\System32\\wininit.exe"),\(\"@Name":""TargetDomainName "",""#text":""S-1-16-16384"")]}}
2025-07-29T03:44:31+0000	G382,6382,2025-07-29 03:44:31.8852626,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\\winninit.exe ,PlD: 0x2A8,Parent PlD: 0x230,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,*C:\ Windows\System32\\services.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,*(""EventData"":{ ""Data"*:{{""@Name"*:""SubjectUserSid"",""#ext*":"">-1-5-18""},{""@Name"*:""SubjectUserSid";""#ext*":"">-1-5-18""},{""@Name"*:""SubjectUserSid";"#ext*":"">-1"},{""@Name"*:""SubjectUserSid";"#ext*":""0x3E7""},{""@Name"*:""NewProcessId","#text*":""" ""Data"*:""SubjectLognolid"","#text*":""0x3E7""},{""@Name"*:""NewProcessId"",""#text*":"" ""0x2A8""},{""@Name"*:""NewProcessName",""#text*":""C:\Windows\\System32\\services.exe""}, {""@Name"*:""TokenElevationType",""#text*":""%41936""},{""@Name"*:""ProcessId"",""#text*":"" S-1-0-0"},{""@Name"*:"TargetUserName",""#text*":"">-1",{""@Name"*:""TargetUserSid"",""#text*":"" TargetDomainName",""#text*":""",{""@Name"*:""TargetUserName",""#text*":""0x0""},{""@Name"*:""TargetUserName",""#text*":""0x0""},{""@Name"*:""TargetUserName",""#text*":""0x0""},{""@Name"*:""TargetUserName",""#text*":""0x0""},{""@Name"*:""""","#text*":""0x0""},{""@Name"*:"""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:"","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:""","#text*":""0x0""},{""@Name"*:"","#text*":""0x0""},{""@Name"*:"","#text*":""0x0""},{""@Name"*:"","#text*":""0x0""},{""@Name"*:"","#text*":"","","#text*":"","","#text*":"","",","#text*":"","","#text*":"","","#text*":"",","","#text*":"",",","#text*":"",",","#text*":"",",","#text*":"",",","#text*":"",",","#text*":""



Time	Event
2025-07-29T03:44:31+0000	6381,6381,2025-07-29 03:44:31.8387518,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,128, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x294,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\windo
2025-07-29T03:44:31+0000	6380,6380,2025-07-29 03:44:31.7420302,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x238,Parent PID: 0x228,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,"C:\Windows\System32\csrss.exe ",False,C:\Users\UMnDesktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{{\textit{"}.000000000000000000000000000000000000
2025-07-29T03:44:31+0000	6379,6379,2025-07-29 03:44:31.7263999,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x230,Parent PID: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\wininit.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":{""@Name":""SubjectUserSid",""#text*":""S-1-5-18""},{""@Name":""SubjectUserSid",""#text*":""SubjectUserSid",""#text*":""S",{""@Name":""SubjectUserSid",""#text*":""SubjectUserSid",""#text*":""SubjectLogonld"",""#text*":""Ox3E7""},{""@Name":""NewProcessId"",""#text*":"""SubjectLogonld"",""#text*":""C:\\Windows\\System32\\wininit.exe*"\;{""@Name":""TokenElevationType",""#text*":""C:\\Windows\\System32\\wininit.exe*"\;{""@Name":""TokenElevationType",""#text*":""SubjectUserSid",""#text*":""S-1-0-0""\;{""@Name":""TargetUserName",""#text*":""S-1-10-0""\;{""@Name":""TargetUserName",""#text*":""S-1-10-0""\;{""@Name":""TargetUserName",""#text*":""S-1-10-16384""\;{\""@Name":""TargetUserName",""#text*":""S-1-10-16384""\;{\""@Name":""TargetUserName",""#text*":""S-1-10-16384""\;{\""@Name":""C:\\Windows\\System32\\smss.exe*"\;{\""@Name":""MandatoryLabel"",""#text*":""S-1-10-16-16384""\;{\""}}\;{\""@Name":""TargetUserName":""SubjectUserSid",""#text*":""S-1-10-16-16384""\;{\""}}\;{\""@Name":""TargetUserName":"""""""TargetUserName":""TargetUserName":"""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":""TargetUserName":"""""""""""""""""""
2025-07-29T03:44:31+0000	6378,6378,2025-07-29 03:44:31.7263961,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,116, DESKTOP-5A3QN5S,76,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x228,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\ Windows\System32\smss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""} Data"":{{"@Name"":""SubjectUserSid"",""#text*":""S-1-5-18*"},{""@Name*":""},{""} subjectUserName"",""#text*":""-"",{""@Name*":""SubjectDomainName"",""#text*":""-"",{""} "@Name*":""SubjectLogonId"","#text*":""Ox3E7""),{""@Name*":""NewProcessId"","#text*":"" "0x228""},{""@Name*":""NewProcessName*",""#text*":""C:\\Windows\\System32\\smss.exe*"},{""} "@Name*":""TokenElevationType*",""#text*":""6%%1936""},{""@Name*":""ProcessId*",""#text*":""S-1 -0-0""),{""@Name*":""TargetUserName*",""#text*":""S-1 -0-0""},{""@Name*":""TargetUserName*",""#text*":""0x0*"},{""@Name*":""TargetDomainName*" ",""#text*":"""],{""@Name*":""MandatoryLabel "",""#text*":""S-1-16-16384""]]})*
2025-07-29T03:44:31+0000	6377,6377,2025-07-29 03:44:31.0938882,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,324, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x1E4,Parent PID: 0x1D4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,C:\Windows\System32\csrss.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{\"@Name"":"SubjectUserSid"" ""#text"":""5-1-5-18""},{\"@Name"":""SubjectUserSid"" ""#text":""-""},{\"@Name"":"SubjectLognolld"","#text":""-""},{\"@Name"":"NewProcessId"","#text":""""","\"@Name"":""NewProcessId"","#text":"""","\"@Name":""TokenElevationType",""#text":""C:\Windows\System32\csrss.exe"{\""@Name":""TokenElevationType",\""@Name":"TargetUserSid"",""#text":""S-1-0-0"\""@Name":"TargetUserName",""#text":""",\""@Name":"TargetUserSid",""#text":""S-1-16-16384"\"""#text":""TargetLogonId",\""#text":""\"",\""@Name":""TargetUserSid",\""#text":""S-1-16-16384"\"\""#text":""C:\Windows\System32\\smss.exe"\""@Name":""MandatoryLabel



Time	Event
2025-07-29T03:44:30+0000	6376,6376,2025-07-29 03:44:30.8184718,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,308, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe, PID: 0x1D4,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\UMDesktop\Security.evtx,Audit success,0,"{""EventData"":{"" Data"":{{""@Name":-""SubjectUserSidi",""#text*":""S-1-5-18"],{""@Name":-""},{""EventData"":{"" SubjectUserSidi",""#text*":""SubjectUserSidi",""#text*":""" SubjectLogonId",""#text*":"" "0x1D4""),{""@Name":-""NewProcessId",""#text*":"" "0x1D4""),{""@Name":-""NewProcessId",""#text*":"" "0x1D4""),{""@Name":-""TokenElevationType",""#text*":""C:\\Windows\\System32\\smss.exe""},{""@Name:-":""S-1-0-0"",{""@Name":-""TargetUserName":""TargetUserSidi",""#text*":""S-1-0-0"",{""@Name":-""TargetUserName":""TargetUserSidi",""#text*":""S-1-10-10"3,{""@Name":-""TargetDomainName":-""TargetDomainName":-""TargetDomainName":-""#text*":""","",""@Name":-""TargetDomainName":-""TargetDomainName":-""#text*":""","","#text*":""","","",""@Name":-"""""","",""@Name":-""""""","",""@Name":-""""""""","",""@Name":-"""""""""","",""@Name":-""""""""""",""""""""""""""""""""""""
2025-07-29T03:44:22+0000	6375,6375,2025-07-29 03:44:22.0018272,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,332, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,Parent process: C:\Windows\System32\smss.exe, PID: 0x19C,Parent PID: 0x180,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\sutochk.exe ",False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"(""EventData"":(" @Name"::"\$ubjectUserSid"","#text*":""S-1-5-18"",(" @Name"::"\$ubjectUserSid"","#text*":"""""""""""""""""""""""""""""""""""
2025-07-29T03:44:12+0000	6374,6374,2025-07-29 03:44:12.3447689,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,"Parent process: ",PID: 0x180,Parent PID: 0x4,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"C:\Windows\System32\smss.exe ",False,C:\Users\WMDesktop\Security.evtx,Audit success,0,"\""EventData"":\""\""\"@\Name":\"""\"""\"""\"""\"""\"""\"""\"""\"""\
2025-07-29T03:44:12+0000	6371,6371,2025-07-29 03:44:12.3395993,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,32, DESKTOP-5A3QN5S,76,,A new process has been created,-\-,-,"Parent process: ",PID: 0x6C,Parent PID: 0x4 ,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,-,"Registry ",False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"(""EventData":((""Data":((""Data":":""S-1)-5-18"",""S-1)-5-18"",""@Name":""S-1)-5-18"",(""@Name":""S-1)-5-18"",(""@Name":"""S-1)-5-18"",(""@Name":""""),"(""@Name":""""),"(""@Name":""""),"(""@Name":""""),"(""@Name":"""),"(""@Name":"""),"(""@Name":"""),"(""@Name":"""),"(""@Name":"""),"(""@Name":"""),"(""@Name":"""),"(""@Name":""TargetUserSid"",""#text"":"""),"(""@Name":""TargetUserSid"",""#text":""-""),"(""@Name":""TargetUserSid"",""#text":""-""),"(""@Name":""TargetUserSid"","""*text":""-""),"(""@Name":""""),"(""@Name":""""],"(""@Name":""""],"(""@Name":""""],"(""@Name":""""],"(""@Name":""],"(""],"(""@Name":""],"(""@Name":""],"(""@Name":""],"(""],"(""@Name":""],"(""],"(""@Name":""],"(""]



New Services Installed

Time	Event	
2025-07-29T17:58:06+0000	1138,1138,2025-07-29 17:58:06.7537896,7045,Info,Service Control Manager,System,696,2432,DESKTOP-5A3QN5S, 8,S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,Name: PsExec ,StartType: demand start,Account: LocalSystem,,,%SystemRoot%NPSEXESVC.EXE,False,C:\Users\VM\Desktop\ System.evtx,"Audit success, classic",0,"\"EventData"":\"Evata"":\"ServiceName"\"""\"#text"":\"ServiceName"\"\""\"#text"\":\"%SystemRoot%\PSEXESVC.EXE\"\},\\\"\@\Name\"\"\"#text\":\"\"\@\Name\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"\"	
2025-07-29T07:14:17+0000	483,483,2025-07-29 07:14:17.9192753,7045,Info,Service Control Manager,System,676,760,DESKTOP-5A3QN5S,3, S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,,Name: VirtualBox Shared Folders,StartType: system start,"Account: ",,,,\SystemRoot\System32\drivers\VBoxSF.sys,False,C:\Users \VMDesktop\System.evtx, "Audit success, classic",0,"(""EventData"":(""@Name"":""@Name"":"" ServiceName"",""#text"::"\'\trutalBox Shared Folders""),{""@Name"":""ImagePath","#text"::"\\ SystemRoot\\System32\\drivers\\VBoxSF.sys""),{""@Name"":"ServiceType"","#text"":"\kernel mode driver"\},{""@Name"":"StartType"",""#text":"\system start""},{""@Name"::"AccountName""	
2025-07-29T07:14:17+0000	482,482,2025-07-29 07:14:17.6351039,7045,Info,Service Control Manager,System,676,760,DESKTOP-5A3QN5S,3, S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,,Name: VirtualBox Guest Additions Service,StartType: auto start,Account: LocalSystem,,,,%SystemRoot%\System32\VBoxService.exe, False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0."(""EventData"":(""Data"":[(""@ Name"":""@ Name"":""WirtualBox Guest Additions Service"),(""@ Name"":""ImagePath" ",""#text"":""%SystemRoot%\\System32\\VBoxService.exe=""},(""@ Name":""ServiceType"",""#text"":""serviceType"",""#text"":""auto start"},(""@ Name"":""""""""""""""""""""""""""""""""""	
2025-07-29T07:14:15+0000	481,481,2025-07-29 07:14:15.9153801,7045,Info,Service Control Manager,System,676,4408,DESKTOP-5A3QN5S,3, S-1-5-18,A new service was installed in the system,,,Name: VirtualBox Guest Mouse Service,StartType: demand start,"Account: ",,,,\SystemRoot\System32\drivers\\VBoxMouse.sys,False,C:\Users\VM\Desktop\System.evtx," Audit success, classic',0,*(""EventData":(""Data":(""@Name":""ServiceName","#text":"" VirtualBox Guest Mouse Service"},(""@Name":""ImagePath*","*#text*":*"\SystemRoot\System32\\drivers\\VBoxMouse.sys\"},(\text{""@Name"}",\text{"""\kernel mode driver\"},\{\text{""@Name"}\text{""},\text{""}\kernel mode driver\"},\{\text{""@Name"}\text{""}\tex	
2025-07-29T07:14:13+0000	480,480,2025-07-29 07:14:13.4707112,7045,Info,Service Control Manager,System,676,2152,DESKTOP-5A3QN5S,3, S-1-5-18,A new service was installed in the system,,,Name: VBoxWddm,StartType: demand start,"Account: ", ,,,\SystemRoot\System32\drivers\VBoxWddm.sys,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic" ,0,"{""EventData"":{""@Name":"ServiceName"","#text"":"VBoxWddm":},{""@Name":""\MoxWddm:System32\drivers\VBoxWddm.sys"),{""@Name"":"ServiceType",""#text":""\SystemRoot\System32\drivers\VBoxWddm.sys"),{""@Name"":"demand start""},{"@Name":""AccountName""}}}"	
2025-07-29T07:14:09+0000	478,478,2025-07-29 07:14:09.3919026,7045,Info,Service Control Manager,System,676,2152,DESKTOP-5A3QN5S,3, S-1-5-18,A new service was installed in the system,,,Name: VirtualBox Guest Driver,StartType: boot start," Account: ",,,system32\DRIVERS\VBoxGuest.sys,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic ",0,"\"EventData"":\""Data"":\""@Name"":""ServiceName"",""#text"":""VirtualBox Guest Driver ",\",\"@Name"":""ImagePath"",""#text"":""system32\\DRIVERS\\VBoxGuest.sys"],\"@Name"" :""ServiceType"",""#text"":""kernel mode driver"],\""@Name"":""StartType"",""#text"":""boot start""],\""@Name"":""AccountName""]}}\"	
2025-07-29T06:50:28+0000	418,418,2025-07-29 06:50:28.5928202,7045,Info,Service Control Manager,System,672,1852,DESKTOP-5A3QN5S,3, S-1-5-18,A new service was installed in the system,,,Name: KslD,StartType: demand start,"Account: ",,,, system32\drivers\wd\KslD.sys,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData "":(""Data"":{(""@Name"":""ServiceName"", ""#text"":""ServiceType"",""#text"":"" kernel mode driver"),{""@Name":""ServiceType"",""#text":"" kernel mode driver"),{""@Name":""" kernel mode driver"),{""@Name":""" kernel mode driver"}]};""@Name"":"" kernel mode driver"),{""@Name":""ServiceType",""#text":"" kernel mode driver"),{""@Name":"" kernel mode driver"}]};"	
2025-07-29T06:50:24+0000	416,416,2025-07-29 06:50:24.7740996,7045,Info,Service Control Manager,System,672,1852,DESKTOP-5A3QN5S,3, S-1-5-18,A new service was installed in the system,,,Name: Microsoft Defender Core Service,StartType: auto start,Account: LocalSystem,,,,"""C:\ProgramData\Microsoft\Windows Defender\platform\4.18.25060.7-0\ MpDefenderCoreService.exe"",False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{f"} EventData"":{f"@Name"":""ServiceName"",""#text"":""Wicrosoft Defender Core Service""},{f"@Name"":""UserviceName*",""#text"":""\c:\\ProgramData\Microsoft\Windows Defender\platform\\4.18.25060.7-0\\MpDefenderCoreService.exe\""",\f"@Name*":""ServiceType*","#text*":""user mode service"",\{""@Name":""StartType"",""#text*":"auto start*"},\f"@Name*":""#text*":""auto start*"},\f"@Name*":""#text*":""AccountName*",\f"@Name*":""LocalSystem*")}}})	
2025-07-29T04:54:21+0000	159,159,2025-07-29 04:54:21.2074655,7045,Info,Service Control Manager,System,668,2284,WIN-NoIRN1T9IF6,1,S -1-5-18,A new service was installed in the system,,,Name: Printer Extensions and Notifications,StartType: demand start,Account: LocalSystem,,,,%SystemRoot%\system32\svchost.exe -k print,False,C:\Users\VM\Desktop\System. evtx,"Audit success, classic",0,"\f""EventData"":\f""Data"":\f""Bara"":\f""ServiceName"",\f""\serviceName"\f""\serviceName"\f""\serviceName\f"\f""\serviceName\f"\f""\serviceName\f"\f"\f"\f" \end{array} \text\f"\f" \f" \f" \f" \f" \f" \f" \f" \f" \	



Dashboard for the privilege escalation attack

Time	Event
2025-07-29T04:52:21+0000	86,86,2025-07-29 04:52:21.8480315,7045,Info,Service Control Manager,System,668,2360,WIN-NOIRN1T9IF6,0,S-1 -5-18,A new service was installed in the system,,,Name: Microsoft Edge Elevation Service (MicrosoftEdgeElevationService),StartType: demand start,Account: LocalSystem,,,,"""C:\Program Files (x86)\ MicrosoftEdgeApplication\92.0.902.67\elevation_service.exe"",False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"(""EventData"":(""@Name"::"ServiceName"","#text":": Microsoft Edge Elevation Service (MicrosoftEdgeElevationService)""),{""@Name"":"ImagePath"",""#text":": "\""C:\\Program Files (x86)\\Microsoft\\Edge\Application\\92.0.902.67\\elevation_service.exe\\""""},{"" @Name"":"StartType"",""#text":"" @Name"":"StartType"",""#text":"#text":""#text":"#tex
2025-07-29T04:52:09+0000	61,61,2025-07-29 04:52:09.0669226,7045,Info,Service Control Manager,System,668,2284,WIN-N0IRN1T9IF6,0,S-1 -5-18,A new service was installed in the system,,Name: Intel(R) PRO/1000 NDIS 6 Adapter Driver,StartType: demand start,"Account: ",,,,'SystemRoot\System32\drivers\E166032E.sys,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"(""EventData"":{""Data"":{""@Name"":""ServiceName"",""#text"":""Hete(R) PRO/1000 NDIS 6 Adapter Driver"),{""@Name"::""ImagePath"",""#text"":""\ SystemRoot\System32\drivers\E166032E.sys""),{""@Name":""ServiceType"",""#text"":""kernel mode driver"},{\""@Name":""ServiceType"",""#text"":""kernel mode driver"},{\""@Name":""ServiceType"",""#text"":""kernel mode driver"}},{\""@Name":""StartType"",""#text"":""demand start""},{\""@Name":""
2025-07-29T00:53:39+0000	560,560,2025-07-29 00:53:39.6787974,7045,Info,Service Control Manager,System,700,6108,DESKTOP-5A3QN5S,4, S-1-5-18,A new service was installed in the system,,,Name: Microsoft Update Health Service,StartType: disabled, Account: LocalSystem,,,,"""C:\Program Files\Microsoft Update Health Tools\underseten Service,StartType: disabled, Account: LocalSystem,,,,"""C:\Program Files\Microsoft Update Health Tools\underseten ServiceName",""#text":"Microsoft Update Health Service"),{""@Name":"ImagePath",""#text": ""\"C:\Program Files\Microsoft Update Health Tools\underseten Service\underseten,"\""@Name\underseten ServiceType\underseten \underseten Service\underseten,\underseten Service\underseten Se
2025-07-28T22:29:35+0000	546,546,2025-07-28 22:29:35.9750988,7045,Info,Service Control Manager,System,700,4220,DESKTOP-5A3QN5S,4, S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,Name: SysmonDrv ,StartType: boot start,"Account: ",,,,C:\Windows\SysmonDrv.sys,False,C:\Users\VM\Desktop\System.evtx," Audit success, classic",0,"(""EventData":",(""@Name":",""ServiceName",","#text":"" SysmonDrv.sys,[""@Name":",""#text":"" SysmonDrv.sys"],{""@Name":","#text":"" was a construction of the constr
2025-07-28T22:29:35+0000	545,545,2025-07-28 22:29:35.9609784,7045,Info,Service Control Manager,System,700,4220,DESKTOP-5A3QN5S,4, S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,,Name: Sysmon, StartType: auto start,Account: LocalSystem,,,,C:\Windows\Sysmon.exe,False,C:\Users\VM\Desktop\System.evtx, "Audit success, classic",0,1(""EventData":!(""Data":!(""@Name":""ServiceName"",""#text"": "Sysmon"),{""@Name":""ImpagePath",""#text":""C:\Windows\\Sysmon.exe"),{""@Name":""auto start"},{""@Name":""auto start"},{""@Name":""auto start"],{""@Name":""auto start"],{""auto start"],{""auto start
2025-07-28T21:09:11+0000	278,278,2025-07-28 21:09:11.6400388,7045,Info,Service Control Manager,System,676,5280,DESKTOP-5A3QN5S,2, S-1-5-21-3151804214-3226339955-2188200191-1001,A new service was installed in the system,,,Name: Mozilla Maintenance Service,StartType: demand start,Account: LocalSystem,,,,,"""C:\Program Files (x86)\Mozilla Maintenance Service\maintenanceservice.exe"",False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0 ,"\""EventData":\""\Desktop\System.evtx,"Audit success, classic",0 ,\"\""EventData":\""\Desktop\System.evtx,"Audit success, classic",0 ,\"\""EventData":\""\Desktop\System.evtx,"Audit success, classic",0 ,\"\""EventData":\"\"Desktop\System.evtx,"Audit success, classic",0 ,\"\""EventData":\"\"Desktop\System.evtx,"Audit success, classic",0 ,\"\""EventData":\"\"Desktop\System.evtx,"Audit success, classic",0 ,\"\""#texti":\""service\Nazilla Maintenance Service ""\",\""\"B\Name"\"\""\"""\""\""\""\""\""\""\""\""\""\"

