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, 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""}]}}"
2025-07-30 02:40:17.798	14262,14262,2025-07-30 02:40:17.7983761,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,760, DESKTOP-5A3QN5S,169,,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, SeImpersonatePrivilege""}]}}"
2025-07-30 02:40:17.793	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, 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""}]}}"
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-5A3QN5S,169,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0xDA08,,,,,,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"":""0xDA08""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"
2025-07-30 02:40:17.763	14257,14257,2025-07-30 02:40:17.7637041,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, 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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xD9EF""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
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, 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
2025-07-30 02:40:17.730	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, 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""}]}} "
2025-07-30 02:40:17.444	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"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}]}}"
2025-07-30 02:40:17.196	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, 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""}]}} "
2025-07-30 02:21:43.866	14106,14106,2025-07-30 02:21:43.8662566,4672,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""}]}} "
2025-07-30 02:21:43.586	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""},{""@Name"":""SubjectUserName"",""#text"":""LOCAL SERVICE""},{""@ Name"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""# text"":""0x3E5""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}]}}"
2025-07-30 02:21:43.584	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, 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""}]}} "
2025-07-30 02:21:43.556	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: 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 ""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName"" ,""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xD837""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"

_time	_raw
2025-07-30 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"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
2025-07-30 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"":{""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""}]}} "
2025-07-30 02:21:43.534	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, 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""}]}} "
2025-07-30 02:21:43.180	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""}]}}"
2025-07-30 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, 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""}]}} "
2025-07-30 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, 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""}]}} "

_time	_raw
2025-07-30 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, 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""}}}} "
2025-07-30 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",LogonId: 0xDC7B,,,,,,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"":""0xDC7B""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}}}}"
2025-07-30 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"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name" ":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"" :""0xDC67""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}}}}"
2025-07-30 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"":[{""@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""}}}}"
2025-07-30 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, 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""}}}} "
2025-07-30 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"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""# text"":""0x3E4""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}}}}"
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"":""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
2025-07-30 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, 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""}}}} "
2025-07-30 02:16:04.298	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, 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""}}}} "
2025-07-30 02:16:04.277	13890,13890,2025-07-30 02:16:04.2775060,4672,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",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"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xDB75""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}}}}"
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, SeImpersonatePrivilege",LogonId: 0xDB42,,,,,,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"" :""0xDB42""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}}}}"
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"":{""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 , 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: 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""}}}} "
2025-07-30 02:16:03.745	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, 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""}}}}"

_time	_raw
2025-07-30 02:16:03.544	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, 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""}]}} "
2025-07-30 02:07:46.794	13583,13583,2025-07-30 02:07:46.7943930,4672,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""}]}} "
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"":""SubjectDomainName"",""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""# text"":""0x3E5""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}]}}"
2025-07-30 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, 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""}]}} "
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\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"":""0xD5FF""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"
2025-07-30 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"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name" ":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"" :""0xD541""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
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, 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""}]}} "

_time	_raw
2025-07-30 02:07:46.579	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: 0x3E7,,,,,,False,C:\Users\VM\Desktop\ Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"" ""S-1-5-18""},{""@Name"":""SubjectUserName"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-30 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 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"","":""NETWORK SERVICE""},{""@ Name"":""SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""# text"":""0x3E4""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}]}}"
2025-07-30 02:07:45.897	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 18:02:45.989	14360,14360,2025-07-29 18:02:45.9899822,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,720,804, DESKTOP-5A3QN5S,170,,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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:57:50.704	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:50:46.925	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-29 17:42:22.010	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, 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""}]}} "
2025-07-29 17:41:42.973	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,"{""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 17:40:43.727	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, 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""}]}} "
2025-07-29 17:40:31.129	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, 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""}]}} "
2025-07-29 17:40:28.205	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, 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""}]}} "
2025-07-29 17:40:23.717	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, 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""}]}} "

_time	_raw
2025-07-29 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, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x38CE6,,,,,,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"":""0x38CE6""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 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"":{""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 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"":""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 17:40:20.645	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, 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""}]}}"
2025-07-29 17:40:20.069	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, 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""}]}}"
2025-07-29 17:40:19.868	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, 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""}]}}"

_time	_raw
2025-07-29 17:37:57.093	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, 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""}]}} "
2025-07-29 17:23:50.689	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, 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""}]}} "
2025-07-29 17:22:11.522	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, 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""}]}} "
2025-07-29 17:21:58.782	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"":{""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 17:21:55.597	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",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 17:21:50.429	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: 0x3B50C,,,,,,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"":""0x3B50C""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"

_time	_raw
2025-07-29 17:21:50.214	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""}]}} "
2025-07-29 17:21:46.443	14121,14121,2025-07-29 17:21:46.4434194,4672,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""}]}} "
2025-07-29 17:21:46.384	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, 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""}]}} "
2025-07-29 17:21:46.378	14117,14117,2025-07-29 17:21:46.3789671,4672,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""}]}} "
2025-07-29 17:21:45.751	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"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:21:45.575	14112,14112,2025-07-29 17:21:45.5758868,4672,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"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-29 17:18:28.775	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, 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""}]}} "
2025-07-29 17:18:16.318	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""}]}} "
2025-07-29 17:18:13.069	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, 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""}]}} "
2025-07-29 17:18:10.067	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, 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""}]}} "
2025-07-29 17:18:07.948	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, 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""}]}} "
2025-07-29 17:18:07.941	14021,14021,2025-07-29 17:18:07.9415716,4672,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""}]}} "

_time	_raw
2025-07-29 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",LogonId: 0x1EE05,,,,,,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"":""0x1EE05""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 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, 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""}]}}"
2025-07-29 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"":{""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 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, 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""}]}}"
2025-07-29 17:18:04.629	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, 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 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, 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""}]}}"

_time	_raw
2025-07-29 17:16:38.217	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"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:16:25.198	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""}]}} "
2025-07-29 17:16:17.994	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""}]}} "
2025-07-29 17:16:14.894	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, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 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"":"" 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 17:16:10.980	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, 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""}]}} "

_time	_raw
2025-07-29 17:16:07.961	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, 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""}]}} "
2025-07-29 17:16:07.892	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, 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""}]}} "
2025-07-29 17:16:07.887	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, 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""}]}} "
2025-07-29 17:16:07.181	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:16:07.066	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, 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""}]}} "
2025-07-29 17:16:06.189	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, 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""}]}} "

_time	_raw
2025-07-29 17:13:42.806	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"":{""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 17:13:42.673	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 17:13:24.390	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, 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""}]}} "
2025-07-29 17:10:25.055	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, 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""}]}} "
2025-07-29 17:09:51.312	13640,13640,2025-07-29 17:09:51.3126369,4672,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",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 17:08:13.630	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, 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""}]}} "

_time	_raw
2025-07-29 17:08:01.308	13628,13628,2025-07-29 17:08:01.3081570,4672,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, 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""}]}} "
2025-07-29 17:07:55.271	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\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""}]}} "
2025-07-29 17:07:53.629	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, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3FB99,,,,,,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"":""0x3FB99""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 17:07:52.874	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, 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""}]}} "
2025-07-29 17:07:49.537	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",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 17:07:49.506	13598,13598,2025-07-29 17:07:49.5068686,4672,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",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 17:07:49.504	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, 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""}]}} "
2025-07-29 17:07:48.998	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, 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""}]}} "
2025-07-29 17:07:48.837	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, 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""}]}} "
2025-07-29 17:07:48.177	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""}]}} "
2025-07-29 17:03:02.206	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, 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""}]}} "
2025-07-29 17:02:59.995	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, 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""}]}} "

_time	_raw
2025-07-29 16:50:57.870	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, 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""}]}} "
2025-07-29 16:50:56.296	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"":{""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 16:48:08.689	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"":{""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 16:48:08.570	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, 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""}]}} "
2025-07-29 16:42:45.085	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, SeImpersonatePrivilege, 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""}]}} "
2025-07-29 16:41:22.530	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, 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""}]}} "

_time	_raw
2025-07-29 16:41:22.357	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, 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""}]}} "
2025-07-29 16:41:20.292	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 16:39:20.475	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, 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""}]}} "
2025-07-29 16:39:19.263	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 16:22:09.912	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, 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""}]}} "
2025-07-29 16:13:04.010	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"":{""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 16:06:06.249	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, 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""}]}} "
2025-07-29 16:06:06.073	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, 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""}]}} "
2025-07-29 16:06:03.843	13505,13505,2025-07-29 16:06:03.8430288,4672,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, 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""}]}} "
2025-07-29 16:00:01.648	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, 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""}]}} "
2025-07-29 16:00:01.389	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, 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""}]}} "
2025-07-29 15:38:16.643	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, 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""}]}} "

_time	_raw
2025-07-29 15:38:15.324	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""}]}} "
2025-07-29 15:38:15.014	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"":{""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 15:15:57.191	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 15:11:56.229	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"",""#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 15:11:55.394	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, 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""}]}} "
2025-07-29 15:08:07.376	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, 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""}]}} "

_time	_raw
2025-07-29 15:00:06.517	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, 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""}}}} "
2025-07-29 15:00:06.089	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"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} "
2025-07-29 14:00:17.630	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, 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""}}}} "
2025-07-29 14:00:12.833	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, 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""}}}} "
2025-07-29 13:57:34.683	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, 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""}}}} "
2025-07-29 13:43:14.580	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, SeImpersonatePrivilege, 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""}}}} "

_time	_raw
2025-07-29 13:30:46.762	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, 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""}]}} "
2025-07-29 13:12:43.968	13467,13467,2025-07-29 13:12:43.9686243,4672,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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 13:05:04.663	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, 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""}]}} "
2025-07-29 12:42:45.075	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, 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""}]}} "
2025-07-29 12:42:44.916	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, 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""}]}} "
2025-07-29 12:40:57.997	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),,"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""}]}} "

_time	_raw
2025-07-29 12:05:32.772	13457,13457,2025-07-29 12:05:32.7726764,4672,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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 12:05:32.537	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, 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""}]}} "
2025-07-29 12:05:29.445	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: 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"":{""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 11:42:28.493	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, 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""}]}} "
2025-07-29 11:42:28.194	13449,13449,2025-07-29 11:42:28.1947396,4672,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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 11:12:29.871	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, 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""}]}} "

_time	_raw
2025-07-29 10:57:20.332	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, 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""}]}} "
2025-07-29 10:57:09.728	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, 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""}]}} "
2025-07-29 10:56:56.059	13433,13433,2025-07-29 10:56:56.0595586,4672,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, 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""}]}} "
2025-07-29 10:44:08.479	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 10:42:24.379	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, 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""}]}} "
2025-07-29 10:42:24.130	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, 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""}]}} "

_time	_raw
2025-07-29 10:12:48.244	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, 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""}]}} "
2025-07-29 09:42:50.476	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, 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""}]}} "
2025-07-29 09:42:38.987	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, 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""}]}} "
2025-07-29 09:42:38.786	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, 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""}]}} "
2025-07-29 09:30:40.149	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, 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""}]}} "
2025-07-29 09:29:06.523	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, 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""}]}} "

_time	_raw
2025-07-29 09:29:04.932	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""}]}} "
2025-07-29 09:27:52.660	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""}]}} "
2025-07-29 09:27:45.788	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, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 09:27:44.765	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""}]}} "
2025-07-29 09:22:13.115	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, 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""}]}} "
2025-07-29 09:22:12.947	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, 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""}]}} "

_time	_raw
2025-07-29 09:16:19.197	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"":{""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 09:13:22.061	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, 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""}}}} "
2025-07-29 09:07:08.698	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, 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""}}}} "
2025-07-29 08:05:56.115	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"":{""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 08:04:55.709	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, 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""}}}} "
2025-07-29 08:04:22.786	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 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 07:50:22.058	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, 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""}]}} "
2025-07-29 07:49:36.964	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, 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""}]}} "
2025-07-29 07:48:38.353	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: 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""}]}} "
2025-07-29 07:43:08.397	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"":{""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 07:42:17.793	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, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:42:15.292	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, 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""}]}} "

_time	_raw
2025-07-29 07:42:11.940	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""}}}} "
2025-07-29 07:31:53.189	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""}}}} "
2025-07-29 07:31:41.737	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, 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""}}}} "
2025-07-29 07:31:31.270	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""}}}} "
2025-07-29 07:31:29.170	13193,13193,2025-07-29 07:31:29.1701863,4672,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""}}}} "
2025-07-29 07:26:40.781	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, 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""}}}} "

_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, 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""}]}} "
2025-07-29 07:22:35.202	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, 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""}]}} "
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, 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""}]}} "
2025-07-29 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),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x199241,,,,,,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"":""0x199241""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 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"":{""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 07:20:43.411	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, 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 07:19:51.226	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, 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""}}}} "
2025-07-29 07:19:51.199	13076,13076,2025-07-29 07:19:51.1996480,4672,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""}}}} "
2025-07-29 07:19:46.161	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} "
2025-07-29 07:19:46.063	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""}}}} "
2025-07-29 07:19:46.020	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, 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""}}}} "
2025-07-29 07:19:45.030	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, 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""}}}} "

_time	_raw
2025-07-29 07:19:44.834	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, 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""}}}} "
2025-07-29 07:19:43.505	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"":{""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 07:19:43.022	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"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}}}} "
2025-07-29 07:19:42.734	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, 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""}}}} "
2025-07-29 07:19:42.704	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, 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 , SeImpersonatePrivilege""}}}"
2025-07-29 07:19:42.683	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"" ,""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xDC44""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}}}"
2025-07-29 07:19:42.683	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"":{""Data"":[{""@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, SeImpersonatePrivilege""}}}"

_time	_raw
2025-07-29 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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":"" ""S-1-5-18""},{""@Name"":""SubjectUserName"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:19:41.928	13044,13044,2025-07-29 07:19:41.9289059,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,736,824, DESKTOP-5A3QN5S,153,,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"","":""NETWORK SERVICE""},{""@ Name"":""SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""# text"":""0x3E4""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege , SeImpersonatePrivilege""}]}}"
2025-07-29 07:19:41.616	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:19:12.150	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:19:06.987	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, 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"","":""SYSTEM""},{""@Name"":"" SubjectDomainName"","":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","":""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"","":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-29 07:19:06.909	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"":{""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 07:19:06.904	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"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:19:06.046	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""}]}} "
2025-07-29 07:19:05.552	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, 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""}]}} "
2025-07-29 07:14:47.926	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, 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""}]}} "
2025-07-29 07:14:47.700	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, 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""}]}} "

_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 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, 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, 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""}]}} "
2025-07-29 07:14:47.438	1109,1109,2025-07-29 07:14:47.4383603,4672,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",LogonId: 0xC128,,,,,,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"":""0xC128""},{""@ Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"
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, SeImpersonatePrivilege",LogonId: 0xC0FF,,,,,,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"" :""0xC0FF""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
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"":{""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""}]}}"
2025-07-29 07:14:47.072	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, 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""}]}} "
2025-07-29 07:12:09.571	2093,2093,2025-07-29 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, 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""}]}} "

_time	_raw
2025-07-29 07:11:38.770	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, 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""}]}} "
2025-07-29 07:10:51.200	1071,1071,2025-07-29 07:10:51.2009458,4672,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, 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""}]}} "
2025-07-29 07:10:04.477	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"":{""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 07:10:00.591	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, 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""}]}} "
2025-07-29 07:09:49.604	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"":{""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 07:09:44.258	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, 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""}]}} "

_time	_raw
2025-07-29 07:09:42.016	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, 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""}]}} "
2025-07-29 07:09:40.110	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, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 07:09:39.233	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, 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""}]}} "
2025-07-29 07:09:39.181	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"":""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 07:09:38.763	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"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 07:09:37.509	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, 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""}]}} "

_time	_raw
2025-07-29 07:09:37.408	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, 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""}]}} "
2025-07-29 07:09:37.388	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, 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""}]}} "
2025-07-29 07:09:36.808	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, 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""}]}} "
2025-07-29 07:09:36.807	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, 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""}]}} "
2025-07-29 07:09:35.647	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, 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""}]}} "
2025-07-29 07:09:35.438	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, 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""}]}} "

_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 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 , SeImpersonatePrivilege""}]}}"
2025-07-29 07:09:35.401	1009,1009,2025-07-29 07:09:35.4014722,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,696,744, DESKTOP-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""}]}} "
2025-07-29 07:09:35.165	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"":"" 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, SeImpersonatePrivilege",LogonId: 0xBBB8,,,,,,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"" :""0xBBB8""},{""@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"":""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""}]}}"
2025-07-29 07:09:34.660	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, 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 06:57:01.552	2089,2089,2025-07-29 06:57:01.5521678,4672,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, 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""}]}} "

_time	_raw
2025-07-29 06:50:24.781	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, 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""}]}} "
2025-07-29 06:49:55.957	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 06:49:47.817	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""}]}} "
2025-07-29 06:49:22.932	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""}]}} "
2025-07-29 06:48:52.996	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 06:48:52.697	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, 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""}]}} "

_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",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 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, 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""}]}}"
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, 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""}]}} "
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",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 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",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 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, 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 06:38:59.218	939,939,2025-07-29 06:38:59.2181783,4672,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"","""#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 06:38:53.582	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",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 06:38:48.834	933,933,2025-07-29 06:38:48.8347267,4672,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",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 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, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x2F930,,,,,,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"":""0x2F930""},{""@Name"":"" PrivilegeList"","""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 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, 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 06:38:44.515	912,912,2025-07-29 06:38:44.5157100,4672,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"":""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 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, 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 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"":""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 06:38:40.479	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"":[{""@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 06:38:40.440	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"":{""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 06:38:39.419	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, 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 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"","",""#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 06:38:39.166	897,897,2025-07-29 06:38:39.1661993,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,728,DESKTOP -5A3QN5S,10,,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 , SeImpersonatePrivilege""}]}}"

_time	_raw
2025-07-29 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, 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 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"":""DWM-1""},{""@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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xBE1D""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
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"":{""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""}]}}"
2025-07-29 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"":[{""@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 06:34:36.148	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, 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""}]}}"
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,,,,,,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 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, SeAuditPrivilege, 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, 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""}]}}"
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, 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""}]}}"
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-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, 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, 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""}]}}"
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, 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""}]}}"

_time	_raw
2025-07-29 06:29:54.024	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, 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""}]}}"
2025-07-29 06:29:49.497	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, 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""}]}}"
2025-07-29 06:29:45.961	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, 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""}]}}"
2025-07-29 06:29:44.298	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 (S-1-5-21-3151804214-3226339955-2188200191-1001),,"PrivilegeList: SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x3D45B,,,,,,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"":""0x3D45B""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 06:29:38.757	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, 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 06:29:38.745	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, 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""}]}}"

_time	_raw
2025-07-29 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, 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""}]}}"
2025-07-29 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, 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""}]}}"
2025-07-29 06:29:36.193	777,777,2025-07-29 06:29:36.1938915,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP-5A3QN5S,8,,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""}]}}"
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, 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""}]}}"
2025-07-29 06:29:35.344	773,773,2025-07-29 06:29:35.3446355,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP-5A3QN5S,8,,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""}]}}"
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, 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""}]}}"
2025-07-29 06:29:35.137	769,769,2025-07-29 06:29:35.1370519,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,688,788,DESKTOP-5A3QN5S,8,,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, SeImpersonatePrivilege""}]}}"

_time	_raw
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, 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""}]}}"
2025-07-29 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"",""#text"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0xC1EE""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"
2025-07-29 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"":{""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""}]}}"
2025-07-29 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, 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""}]}}"
2025-07-29 05:48:32.053	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"":[{""@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 05:14:58.607	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, 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""}]}}"

_time	_raw
2025-07-29 04:59:26.736	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, 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""}]}} "
2025-07-29 04:55:02.544	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, 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""}]}}"
2025-07-29 04:55:02.306	296,296,2025-07-29 04:55:02.3061776,4672,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\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 04:55:01.324	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\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 04:55:00.829	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, 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""}]}}"
2025-07-29 04:55:00.461	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, 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""}]}}"

_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, 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""}]}}"
2025-07-29 04:55:00.000	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"":""defaultuser0""},{""@Name"":""SubjectDomainName"","""#text"":""DESKTOP-5A3QN5S""},{""@Name"":""SubjectLogonId"","""#text"":""0x148CD""},{""@Name"":""PrivilegeList"","""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
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, 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 04:54:52.354	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"":""SubjectUserName"","""#text"":""LOCAL SERVICE""},{""@Name"":""SubjectDomainName"","""#text"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"","""#text"":""0x3E5""},{""@Name"":""PrivilegeList"","""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
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, 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""}]}}"
2025-07-29 04:54:51.992	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"":""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, SeImpersonatePrivilege",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"":""Window Manager""},{""@Name"":""SubjectLogonId"","""#text"":""0xBDCD""},{""@Name"":""PrivilegeList"","""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"

_time	_raw
2025-07-29 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, 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""}]}}"
2025-07-29 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, 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""}]}}"
2025-07-29 04:54:14.102	150,150,2025-07-29 04:54:14.1026895,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,440,WIN-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"":""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-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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-29 04:54:10.560	146,146,2025-07-29 04:54:10.5602005,4672,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"":""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 04:54:10.076	144,144,2025-07-29 04:54:10.0764677,4672,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"":""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 04:54:09.427	142,142,2025-07-29 04:54:09.4279984,4672,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"":""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 04:54:08.966	140,140,2025-07-29 04:54:08.9667855,4672,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"":""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 04:54:08.560	138,138,2025-07-29 04:54:08.5603119,4672,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"":""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 04:54:07.604	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, 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""}]}}"
2025-07-29 04:54:07.126	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"":{""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 04:54:06.721	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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"

_time	_raw
2025-07-29 04:54:06.385	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, 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""}]}} "
2025-07-29 04:54:06.084	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"":{""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 04:54:05.504	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"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:54:04.251	124,124,2025-07-29 04:54:04.2517870,4672,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:53:53.797	121,121,2025-07-29 04:53:53.7973497,4672,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:53:52.287	119,119,2025-07-29 04:53:52.2870930,4672,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-29 04:52:27.343	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, 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""}]}} "
2025-07-29 04:52:12.208	111,111,2025-07-29 04:52:12.2088576,4672,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"":""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 04:52:10.356	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"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:52:08.979	107,107,2025-07-29 04:52:08.9795905,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,736,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:52:08.026	104,104,2025-07-29 04:52:08.0268001,4672,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 04:52:07.944	102,102,2025-07-29 04:52:07.9440968,4672,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"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-29 04:52:06.862	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, 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 04:52:05.907	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"":""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 04:52:05.665	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"":""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 04:52:05.516	91,91,2025-07-29 04:52:05.5165202,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,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"":""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 04:51:55.368	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, SeImpersonatePrivilege""}]}}"
2025-07-29 04:51:55.116	61,61,2025-07-29 04:51:55.1168919,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN1T9IF6,0,,Administrative logon,Window Manager\DWM-1 (S-1-5-90-0-1),,"PrivilegeList: SeAssignPrimaryTokenPrivilege, SeAuditPrivilege",LogonId: 0x12BE7,,,,,,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"":""0x12BE7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]}}"
2025-07-29 04:51:55.116	60,60,2025-07-29 04:51:55.1168901,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,816,WIN-N0IRN1T9IF6,0,,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"":""SubjectUserSid"",""#text"":""S-1-5-90-0-1""},{""@Name"":""SubjectUserName"",""#text"":""DWM-1""},{""@Name"":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":""0x12BD5""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"

_time	_raw
2025-07-29 04:51:54.941	56,56,2025-07-29 04:51:54.9417969,4672,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"":""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 04:51:54.016	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, 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""}]}}"
2025-07-29 04:51:53.603	48,48,2025-07-29 04:51:53.6036654,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,736,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"":""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 04:48:21.008	2066,2066,2025-07-29 04:48:21.0088680,4672,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, 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""}]}}"
2025-07-29 04:14:41.165	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, 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""}]}}"
2025-07-29 03:59:21.626	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, 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""}]}}"

_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, 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""}]}} "
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, 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""}]}} "
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, 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""}]}} "
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, 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""}]}} "
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,"{""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 , SeImpersonatePrivilege""}]}}"
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"":{""Data"":[{""@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 03:44:32.816	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, SeImpersonatePrivilege",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
2025-07-29 03:44:32.528	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 , SeImpersonatePrivilege""}]}}"
2025-07-29 03:44:32.310	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, 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""}]}} "
2025-07-29 03:14:21.194	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"":{""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 02:48:00.674	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"":{""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 01:59:23.347	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"":{""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 01:48:30.583	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, 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""}]}} "

_time	_raw
2025-07-29 01:16:02.452	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, 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""}]}} "
2025-07-29 01:16:02.314	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, 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""}]}} "
2025-07-29 01:15:27.449	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, 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""}]}} "
2025-07-29 01:09:52.492	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, 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""}]}} "
2025-07-29 01:06:23.424	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, 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""}]}} "
2025-07-29 00:53:43.881	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, 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""}]}} "

_time	_raw
2025-07-29 00:53:28.981	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, 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""}]}} "
2025-07-29 00:51:59.715	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"":{""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 00:51:55.301	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, 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""}]}} "
2025-07-29 00:51:55.044	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"":[{""@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 00:48:06.909	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"":{""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 00:48:05.763	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, 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""}]}} "

_time	_raw
2025-07-29 00:48:05.696	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, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 00:45:05.058	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, 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""}]}} "
2025-07-29 00:29:30.586	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 , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-29 00:15:47.987	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, 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""}]}} "
2025-07-29 00:15:47.909	1205,1205,2025-07-29 00:15:47.9094949,4672,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, 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""}]}} "
2025-07-29 00:15:05.132	1203,1203,2025-07-29 00:15:05.1325168,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,712,6468, 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""}]}} "

_time	_raw
2025-07-28 23:59:14.260	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"":{""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""}]}} "
2025-07-28 23:48:09.284	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"":{""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""}]}} "
2025-07-28 23:14:50.121	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, 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""}]}} "
2025-07-28 22:57:23.162	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, 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""}]}} "
2025-07-28 22:45:11.558	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, 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""}]}} "
2025-07-28 22:34:57.681	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"":""NT AUTHORITY""},{""@Name"":""SubjectLogonId"",""#text"":"" 0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeTcbPrivilege, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "

_time	_raw
2025-07-28 22:31:42.752	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""}]}} "
2025-07-28 22:29:53.764	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, 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""}]}} "
2025-07-28 22:16:54.539	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, 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""}]}} "
2025-07-28 22:15:15.087	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, 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""}]}} "
2025-07-28 22:15:04.535	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""}]}} "
2025-07-28 22:14:58.639	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, 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""}]}} "

_time	_raw
2025-07-28 22:14:56.257	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"":{""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""}]}}"
2025-07-28 22:14:53.623	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, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-28 22:14:52.636	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"":{""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""}]}}"
2025-07-28 22:14:52.608	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, 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""}]}}"
2025-07-28 22:14:51.404	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, 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""}]}}"
2025-07-28 22:14:51.363	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, 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""}]}}"

_time	_raw
2025-07-28 22:14:51.338	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, 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""}]}} "
2025-07-28 22:14:50.612	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, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-28 22:14:50.587	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"":{""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""}]}} "
2025-07-28 21:07:32.334	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"":{""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""}]}} "
2025-07-28 20:56:31.811	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, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-28 20:54:12.473	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",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
2025-07-28 20:45:13.382	669,669,2025-07-28 20:45:13.3826076,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,1864, DESKTOP-5A3QN5S,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, SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege , SeAuditPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}} "
2025-07-28 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"":""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 20:37:36.728	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",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""}]}}"
2025-07-28 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, 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""}]}} "
2025-07-28 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, 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""}]}} "
2025-07-28 20:25:36.919	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, 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""}]}} "

_time	_raw
2025-07-28 20:22:15.685	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, 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""}]}}"
2025-07-28 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, 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""}]}}"
2025-07-28 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, 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""}]}}"
2025-07-28 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, 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""}]}}"
2025-07-28 20:12:25.935	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",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""}]}}"
2025-07-28 20:11:14.416	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, 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""}]}}"

_time	_raw
2025-07-28 20:10:35.848	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, 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""}]}} "
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, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege",LogonId: 0x2671DB,,,,,,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"":""0x2671DB""},{""@Name"":"" PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-28 20:10:34.329	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",LogonId: 0x26549A,,,,,,False,C:\Users\VM\Desktop\Security.evtx, Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-90- 0-2""},{""@Name"":""SubjectUserName"",""#text"":""DWM-2""},{""@Name"":"" SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"":"" 0x26549A""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege""}]} }"
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, SeImpersonatePrivilege",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"",""#text"":""DWM-2""},{""@Name" ":""SubjectDomainName"",""#text"":""Window Manager""},{""@Name"":""SubjectLogonId"",""#text"" :""0x26547D""},{""@Name"":""PrivilegeList"",""#text"":""SeAssignPrimaryTokenPrivilege, SeAuditPrivilege, SeImpersonatePrivilege""}]}}"
2025-07-28 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",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""}]}}"
2025-07-28 20:03:24.473	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: 0x23D57D,,,,,,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"":""0x23D57D""},{""@Name"":""PrivilegeList"",""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
2025-07-28 19:58:28.129	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",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
2025-07-28 19:57:58.633	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:\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""}]}}"
2025-07-28 19:57:58.499	445,445,2025-07-28 19:57:58.4995838,4672,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:\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""}]}}"
2025-07-28 19:57:54.071	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, 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""}]}}"
2025-07-28 19:57:11.462	441,441,2025-07-28 19:57:11.4626590,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,796,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:\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""}]}}"
2025-07-28 19:56:12.607	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, 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""}]}}"
2025-07-28 19:55:45.888	368,368,2025-07-28 19:55:45.8880090,4672,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,752,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"":[{""@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
2025-07-28 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"":[{""@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 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",LogonId: 0x3BDD5,,,,,,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"":""defaultuser0""},{""@Name"":""SubjectDomainName"","""#text"":""DESKTOP-5A3QN5S""},{""@Name"":""SubjectLogonId"","""#text"":""0x3BDD5""},{""@Name"":""PrivilegeList"","""#text"":""SeSecurityPrivilege, SeTakeOwnershipPrivilege, SeLoadDriverPrivilege, SeBackupPrivilege, SeRestorePrivilege, SeDebugPrivilege, SeSystemEnvironmentPrivilege, SeImpersonatePrivilege, SeDelegateSessionUserImpersonatePrivilege""}]}}"
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, 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""}]}}"
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, 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""}]}}"
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, 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""}]}}"

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-N0IRN1T9IF6$ (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"":{""Data"":[{""@Name"":""TargetUserName"" ,""#text"":""defaultuser0""},{""@Name"":""TargetDomainName"",""#text"":""DESKTOP-5A3QN5S"" },{""@Name"":""TargetSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-1000""},{"" @Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text "":""WIN-N0IRN1T9IF6$""},{""@Name"":""SubjectDomainName"",""#text"":""WORKGROUP""},{"" @Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""- ""},{""@Name"":""SamAccountName"",""#text"":""defaultuser0""},{""@Name"":""DisplayName"" ,""#text"":""%%1793""},{""@Name"":""UserPrincipalName"",""#text"":""-""},{""@Name"" :""HomeDirectory"",""#text"":""%%1793""},{""@Name"":""HomePath"",""#text"":""%%1793"" },{""@Name"":""ScriptPath"",""#text"":""%%1793""},{""@Name"":""ProfilePath"",""#text"" :""%%1793""},{""@Name"":""UserWorkstations"",""#text"":""%%1793""},{""@Name"":"" PasswordLastSet"",""#text"":""%%1794""},{""@Name"":""AccountExpires"",""#text"":""%% 1794""},{""@Name"":""PrimaryGroupId"",""#text"":""513""},{""@Name"":""AllowedToDelegateTo"" ,""#text"":""-""},{""@Name"":""OldUacValue"",""#text"":""0x0""},{""@Name"":"" NewUacValue"",""#text"":""0x15""},{""@Name"":""UserAccountControl"",""#text"":"", %%2080, %%2082, %%2084""},{""@Name"":""UserParameters"",""#text"":""%%1793""},{""@Name"" :""SidHistory"",""#text"":""-""},{""@Name"":""LogonHours"",""#text"":""%%1797""}]}} "
2025-07-29T04:51:53+0000	43,43,2025-07-29 04:51:53.4850959,4720,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,688,WIN- N0IRN1T9IF6,0,,A new account was created,\MINWINPC$ (S-1-5-18),,Target: MINWINPC\WDAGUtilityAccount (S-1-5-21-3151804214-3226339955-2188200191-504),,,,,,,,False,C:\Users\VM\Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""TargetUserName"",""#text"":"" WDAGUtilityAccount""},{""@Name"":""TargetDomainName"",""#text"":""MINWINPC""},{""@Name"": ""TargetSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-504""},{""@Name"":"" SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"" MINWINPC$""},{""@Name"":""SubjectDomainName""},{""@Name"":""SubjectLogonId"",""#text"":" "0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""-""},{""@Name"":""SamAccountName"", ""#text"":""WDAGUtilityAccount""},{""@Name"":""DisplayName"",""#text"":""%%1793""},{""@ Name"":""UserPrincipalName"",""#text"":""-""},{""@Name"":""HomeDirectory"",""#text"":""%% %1793""},{""@Name"":""HomePath"",""#text"":""%%1793""},{""@Name"":""ScriptPath""," "#text"":""%%1793""},{""@Name"":""ProfilePath"",""#text"":""%%1793""},{""@Name"": ""UserWorkstations"",""#text"":""%%1793""},{""@Name"":""PasswordLastSet"",""#text"":""% %1794""},{""@Name"":""AccountExpires"",""#text"":""%%1794""},{""@Name"":"" PrimaryGroupId"",""#text"":""513""},{""@Name"":""AllowedToDelegateTo"",""#text"":""-""},{" "@Name"":""OldUacValue"",""#text"":""0x0""},{""@Name"":""NewUacValue"",""#text"":"" 0x15""},{""@Name"":""UserAccountControl"",""#text"":"", %%2080, %%2082, %%2084""},{" "@Name"":""UserParameters"",""#text"":""%%1793""},{""@Name"":""SidHistory"",""#text"": ""-""},{""@Name"":""LogonHours"",""#text"":""%%1797""}]}}"
2025-07-28T20:03:23+0000	466,466,2025-07-28 20:03:23.8707345,4720,LogAlways,Microsoft-Windows-Security-Auditing,Security,684,4868, DESKTOP-5A3QN5S,5,,A new account was created,WORKGROUP\WIN-N0IRN1T9IF6$ (S-1-5-18),,Target: DESKTOP-5A3QN5S\VM (S-1-5-21-3151804214-3226339955-2188200191-1001),,,,,,,,False,C:\Users\VM\ Desktop\Security.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":""TargetUserName"","" #text"":""VM""},{""@Name"":""TargetDomainName"",""#text"":""DESKTOP-5A3QN5S""},{""@ Name"":""TargetSid"",""#text"":""S-1-5-21-3151804214-3226339955-2188200191-1001""},{""@Name"" :""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":"" WIN-N0IRN1T9IF6$""},{""@Name"":""SubjectDomainName"",""#text"":""WORKGROUP""},{""@ Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""PrivilegeList"",""#text"":""-"" },{""@Name"":""SamAccountName"",""#text"":""VM""},{""@Name"":""DisplayName"",""#text "":""%%1793""},{""@Name"":""UserPrincipalName"",""#text"":""-""},{""@Name"":"" HomeDirectory"",""#text"":""%%1793""},{""@Name"":""HomePath"",""#text"":""%%1793""}, {""@Name"":""ScriptPath"",""#text"":""%%1793""},{""@Name"":""ProfilePath"",""#text"":"" ""%%1793""},{""@Name"":""UserWorkstations"",""#text"":""%%1793""},{""@Name"":"" PasswordLastSet"",""#text"":""%%1794""},{""@Name"":""AccountExpires"",""#text"":""%% 1794""},{""@Name"":""PrimaryGroupId"",""#text"":""513""},{""@Name"":""AllowedToDelegateTo"" ,""#text"":""-""},{""@Name"":""OldUacValue"",""#text"":""0x0""},{""@Name"":"" NewUacValue"",""#text"":""0x15""},{""@Name"":""UserAccountControl"",""#text"":"", %%2080, %%2082, %%2084""},{""@Name"":""UserParameters"",""#text"":""%%1793""},{""@Name"" :""SidHistory"",""#text"":""-""},{""@Name"":""LogonHours"",""#text"":""%%1797""}]}} "

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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2D0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text """:""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#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\wininit. 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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2B8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-5A3QN5S,168,,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x274""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x224""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x234""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x224""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x22C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text """:""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"

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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x224""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#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 ,PID: 0x1E0,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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1E0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1D4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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.evtx,Audit success,0,"{""EventData"":{"" "Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x198""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" "S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\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 "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x17C""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"
	""0x2D4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{
	""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text
	"":""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-
	1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName
	"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""
	ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""
	MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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: 0x2BC,Parent PID: 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"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x2BC""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x290""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
2025-07-30T02:21:42+0000	14077,14077,2025-07-30 02:21:42.0031000,4688,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x238""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{"@Name":"TargetLogonId","#text":"0x0"},{"@Name":" ParentProcessName","#text":"C:\\Windows\\System32\\smss.exe"},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"

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\wininit.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x230""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1DC""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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 ",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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x228""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x174""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1E4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1DC""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1DC""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x174""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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: 0x1A0,Parent PID: 0x174,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"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1A0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x174""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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"":{""Data"":[{""@Name"":" "SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""} ,{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x174""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" ""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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
	:\Windows\System32\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""
	0x2D8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{
	""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text
	"":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-
	1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName
	"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""
	ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""
	MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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-5A3QN5S,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" 0x2C4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" 0x27C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x23C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x234""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1D8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x22C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1E8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1D8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1D8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"

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 ,PID: 0x1A0,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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1A0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":"" SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""} ,{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x180""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""
	"0x2E0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{
	""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text
	"":""0x23C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-
	1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName
	"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""
	ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""
	MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x2C8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x23C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x284""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x244""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x23C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1E0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x234""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1F0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1E0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"

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 ",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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x1E0""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text "":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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\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"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x1A8""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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\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 "":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":""0x180""},{""@Name"":"" NewProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName"","",""#text"":"" -""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"","",""#text"":""-""},{""@Name"":"" SubjectDomainName"","",""#text"":""-""},{""@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"","",""#text"":""0x6C""},{""@Name"":""NewProcessName"","",""#text"" :""Registry""},{""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":"" ProcessId"","",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":" "TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"","",""#text"":""S-1-16-16384""}] }}"
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 :\Windows\System32\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x2D4""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text """:""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":"" MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"

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: 0x2BC,Parent PID: 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"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2BC""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x278""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x238""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x230""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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-5A3QN5S,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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x228""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"

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\csrss.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1E4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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 ,PID: 0x1D4,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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1D4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x19C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-5A3QN5S,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\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 "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x180""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" "TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"
	"0x2E0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{
	""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text
	"":""0x23C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-
	1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName
	"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""
	ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""
	MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2C4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x23C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2A0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x244""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x234""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\wininit.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x23C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1E0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"

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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x234""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"" :""0x184""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"" ,""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1F0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1E0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1E0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x184""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1A8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x184""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\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 "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x184""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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,"{""EventData"":{""Data"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"
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-5A3QN5S,12,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe ,PID: 0x2C8,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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x2C8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x2BC""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x22C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x274""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x224""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" ""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" ""0x234""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x224""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" 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: 0x22C,Parent PID: 0x1D0,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"":"" SubjectUserName"","""#text"":""-""},{""@Name"":""SubjectDomainName"","""#text"":""-""},{" "@Name"":""SubjectLogonId"","""#text"":""0x3E7""},{""@Name"":""NewProcessId"","""#text"":" "0x22C""},{""@Name"":""NewProcessName"","""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"","""#text"":""%%1936""},{""@Name"":""ProcessId"","""#text """:""0x1D0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","""#text"":""-""},{""@Name"":""TargetDomainName "","""#text"":""-""},{""@Name"":""TargetLogonId"","""#text"":""0x0""},{""@Name"":"" ParentProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"","""#text"":" "0x224""},{""@Name"":""NewProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"","""#text"":""%%1936""},{""@Name"":""ProcessId"","""#text" ":""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","""#text"":""-""},{""@Name"":""TargetDomainName" "","""#text"":""-""},{""@Name"":""TargetLogonId"","""#text"":""0x0""},{""@Name"":"" ParentProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"","""#text"":""-""},{""@Name"":""SubjectDomainName"","""#text"":""-""},{" "@Name"":""SubjectLogonId"","""#text"":""0x3E7""},{""@Name"":""NewProcessId"","""#text"":" "0x1E0""},{""@Name"":""NewProcessName"","""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"","""#text"":""%%1936""},{""@Name"":""ProcessId"","""#text """:""0x1D0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","""#text"":""-""},{""@Name"":""TargetDomainName "","""#text"":""-""},{""@Name"":""TargetLogonId"","""#text"":""0x0""},{""@Name"":"" ParentProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"","""#text"":" "0x1D0""},{""@Name"":""NewProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"","""#text"":""%%1936""},{""@Name"":""ProcessId"","""#text """:""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","""#text"":""-""},{""@Name"":""TargetDomainName "","""#text"":""-""},{""@Name"":""TargetLogonId"","""#text"":""0x0""},{""@Name"":"" ParentProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","""#text"":""S-1-16-16384""}]}}"
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"":""SubjectDomainName"","""#text"":""-""},{" "@Name"":""SubjectLogonId"","""#text"":""0x3E7""},{""@Name"":""NewProcessId"","""#text"":" "0x198""},{""@Name"":""NewProcessName"","""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"","""#text"":""%%1936""},{""@Name"":""ProcessId"","""# text"":""0x17C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"","""#text"":""-""},{""@Name"":"" TargetDomainName"","""#text"":""-""},{""@Name"":""TargetLogonId"","""#text"":""0x0""},{"" @Name"":""ParentProcessName"","""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"","""#text"":""S-1-16-16384""}]}}"

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.evtx,Audit success,0,"{""EventData"":{""Data"":[{""@Name"":" "SubjectUserSid","#text":"S-1-5-18"},{"@Name":"SubjectUserName","#text":"-"} ,{"@Name":"SubjectDomainName","#text":"-"},{"@Name":"SubjectLogonId","#text ":"0x3E7"},{"@Name":"NewProcessId","#text":"0x17C"},{"@Name":" NewProcessName","#text":"C:\\Windows\\System32\\smss.exe"},{"@Name":" TokenElevationType","#text":"%%1936"},{"@Name":"ProcessId","#text":"0x4"},{ "@Name":"CommandLine"},{"@Name":"TargetUserSid","#text":"S-1-0-0"},{"@ Name":"TargetUserName","#text":"-"},{"@Name":"TargetDomainName","#text":" -"},{"@Name":"TargetLogonId","#text":"0x0"},{"@Name":"ParentProcessName"}, {"@Name":"MandatoryLabel","#text":"S-1-16-16384"}]}}"
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":"S-1-5-18"},{"@Name":"SubjectUserName","#text":"-"},{"@Name":" SubjectDomainName","#text":"-"},{"@Name":"SubjectLogonId","#text":"0x3E7"},{ "@Name":"NewProcessId","#text":"0x6C"},{"@Name":"NewProcessName","#text" :"Registry"},{"@Name":"TokenElevationType","#text":"%%1936"},{"@Name":" ProcessId","#text":"0x4"},{"@Name":"CommandLine"},{"@Name":"TargetUserSid", "#text":"S-1-0-0"},{"@Name":"TargetUserName","#text":"-"},{"@Name":" "TargetDomainName","#text":"-"},{"@Name":"TargetLogonId","#text":"0x0"},{" @Name":"ParentProcessName"},{"@Name":"MandatoryLabel","#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\lsass.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":"0x3E7"},{"@Name":"NewProcessId","#text":" "0x2B8"},{"@Name":"NewProcessName","#text":"C:\\Windows\\System32\\lsass.exe"},{ "@Name":"TokenElevationType","#text":"%%1936"},{"@Name":"ProcessId","#text ":"0x22C"},{"@Name":"CommandLine"},{"@Name":"TargetUserSid","#text":"S- 1-0-0"},{"@Name":"TargetUserName","#text":"-"},{"@Name":"TargetDomainName ","#text":"-"},{"@Name":"TargetLogonId","#text":"0x0"},{"@Name":" ParentProcessName","#text":"C:\\Windows\\System32\\wininit.exe"},{"@Name":" MandatoryLabel","#text":"S-1-16-16384"}]}}"
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":" SubjectUserName","#text":"-"},{"@Name":"SubjectDomainName","#text":"-"},{" "@Name":"SubjectLogonId","#text":"0x3E7"},{"@Name":"NewProcessId","#text":" "0x2A4"},{"@Name":"NewProcessName","#text":"C:\\Windows\\System32\\services.exe"}, {"@Name":"TokenElevationType","#text":"%%1936"},{"@Name":"ProcessId","# text":"0x22C"},{"@Name":"CommandLine"},{"@Name":"TargetUserSid","#text":" "S-1-0-0"},{"@Name":"TargetUserName","#text":"-"},{"@Name":" TargetDomainName","#text":"-"},{"@Name":"TargetLogonId","#text":"0x0"},{" @Name":"ParentProcessName","#text":"C:\\Windows\\System32\\wininit.exe"},{"@Name": "MandatoryLabel","#text":"S-1-16-16384"}]}}"
2025-07-29T07:09:33+0000	989,989,2025-07-29 07:09:33.9248664,4688,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: 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","#text":"S-1-5-18"},{"@Name":" SubjectUserName","#text":"-"},{"@Name":"SubjectDomainName","#text":"-"},{" "@Name":"SubjectLogonId","#text":"0x3E7"},{"@Name":"NewProcessId","#text":" "0x25C"},{"@Name":"NewProcessName","#text":"C:\\Windows\\System32\\winlogon.exe"}, {"@Name":"TokenElevationType","#text":"%%1936"},{"@Name":"ProcessId","# text":"0x20C"},{"@Name":"CommandLine"},{"@Name":"TargetUserSid","#text":" "S-1-0-0"},{"@Name":"TargetUserName","#text":"-"},{"@Name":" TargetDomainName","#text":"-"},{"@Name":"TargetLogonId","#text":"0x0"},{" @Name":"ParentProcessName","#text":"C:\\Windows\\System32\\smss.exe"},{"@Name":" "MandatoryLabel","#text":"S-1-16-16384"}]}}"

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: 0x22C,Parent PID: 0x1C0,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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x22C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1C0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x214""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x20C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x20C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1C8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1C0""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1C0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"

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: 0x184,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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x184""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}}}"
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"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""}, {""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text" ":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x164""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}}}"
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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"" :""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" "TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2B0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}}}"
2025-07-29T06:38:36+0000	876,876,2025-07-29 06:38:36.7780046,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,260, DESKTOP-5A3QN5S,9,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe, PID: 0x2A0,Parent PID: 0x228,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"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x2A0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"",""#text"":""S-1-16-16384""}}}"

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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x258""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x208""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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: 0x1B8,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"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x228""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text """:""0x1B8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" 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,"{""EventData"":{"" Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x210""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text" ":""0x208""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x208""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text" ":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x1C4""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text """:""0x1B8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"

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 ",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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1B8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x17C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" "S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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 -5A3QN5S,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\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" ":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x15C""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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 -5A3QN5S,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1 -5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" "TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"
2025-07-29T06:29:34+0000	749,749,2025-07-29 06:29:34.1754098,4688,LogAlways,Microsoft-Windows-Security-Auditing,Security,4,304, DESKTOP-5A3QN5S,8,,A new process has been created,-\-,,Parent process: C:\Windows\System32\wininit.exe, PID: 0x2B0,Parent PID: 0x20C,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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x2B0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x20C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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.evtx,Audit success,0,"{""EventData"":{ ""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x29C""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x20C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x270""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x204""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x218""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text" ":""0x204""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x20C""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text ":""0x1B4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x204""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text" ":""0x150""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"

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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1C0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1B4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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: 0x1B4,Parent PID: 0x150,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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1B4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x150""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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 -5A3QN5S,8,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe,PID: 0x178,Parent PID: 0x150,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"":""SubjectDomainName"",""#text"":""-""},{""@Name"":"" SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x178""},{" "@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""},{""@Name"": ""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x150"" },{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{" "@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"": ""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"" ,""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":"" "S-1-16-16384""}]}}"
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 -5A3QN5S,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\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" ":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x150""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1 -5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" "TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x2AC""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\lsass.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text """:""0x21C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":"" MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x2A4""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\services.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x21C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"": ""MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x25C""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""# text"":""0x20C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":" "S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":" "MandatoryLabel"","",""#text"":""S-1-16-16384""}]}}"
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\wininit.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x21C""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text """:""0x1B8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName "","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"
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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"","",""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{" "@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":" "0x214""},{""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text" ":""0x20C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName" ","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":"" ParentProcessName"","",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","",""#text"":""S-1-16-16384""}]}}"

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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x20C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1C8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x1B8""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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: 0x1B8,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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x1B8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":"" "0x180""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x164""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" "MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":{""Data"":[{""@Name"":"" SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""}, {""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text" ":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x164""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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"",""#text"":""S-1 -5-18""},{""@Name"":""SubjectUserName"","",""#text"":""-""},{""@Name"":"" SubjectDomainName"","",""#text"":""-""},{""@Name"":""SubjectLogonId"","",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"","",""#text"":""0x6C""},{""@Name"":""NewProcessName"","",""#text"" :""Registry""},{""@Name"":""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":"" ProcessId"","",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":"" TargetDomainName"","",""#text"":""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"","",""#text"":""S-1-16-16384""}] }}"
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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":""0x2AC""},{" ""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\lsass.exe""},{""@Name"":"" TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text"":""0x210""} ,{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1-0-0""},{"" @Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName"","",""#text"":"" -""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":""ParentProcessName"", ""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""MandatoryLabel"","",""#text"":"" S-1-16-16384""}]}}"
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"","",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"" ,""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{""@Name"":"" SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":""0x29C""},{" ""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\services.exe""},{""@Name"" :""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text"":""0x210" "},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1-0-0""},{ ""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName"","",""#text"" :""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":""ParentProcessName"" ,""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""MandatoryLabel"","",""#text"": ""S-1-16-16384""}]}}"
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- N0IRN1T9IF6,0,,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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":""0x274""},{" ""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\winlogon.exe""},{""@Name"" :""TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text"":""0x208"" "},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1-0-0""},{ ""@Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName"","",""#text"" :""-""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":""ParentProcessName"" ,""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"","",""#text"": ""S-1-16-16384""}]}}"
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"": [{""@Name"":""SubjectUserSid"","",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName""," ""#text"":""-""},{""@Name"":""SubjectDomainName"","",""#text"":""-""},{""@Name"":"" SubjectLogonId"","",""#text"":""0x3E7""},{""@Name"":""NewProcessId"","",""#text"":""0x218""},{" ""@Name"":""NewProcessName"","",""#text"":""C:\\Windows\\System32\\csrss.exe""},{""@Name"":"" TokenElevationType"","",""#text"":""%%1936""},{""@Name"":""ProcessId"","",""#text"":""0x208""} ,{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"","",""#text"":""S-1-0-0""},{"" @Name"":""TargetUserName"","",""#text"":""-""},{""@Name"":""TargetDomainName"","",""#text"":"" -""},{""@Name"":""TargetLogonId"","",""#text"":""0x0""},{""@Name"":""ParentProcessName"", ""#text"":""C:\\Windows\\System32\\smss.exe""},{""@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\wininit.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x210""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x1BC""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x208""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x1C8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x1BC""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x1BC""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,A new process has been created,-\-,,Parent process: C:\Windows\System32\smss.exe,PID: 0x1A8,Parent PID: 0x15C,Mandatory label: SECURITY_MANDATORY_SYSTEM_RID,Target User: -\-,,"C:\Windows\System32\setupcl.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x1A8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\setupcl.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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-N0IRN1T9IF6,0,,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\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"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x170""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x15C""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,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"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x15C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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-N0IRN1T9IF6,0,,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"":{""Data"":[{""@Name"":""SubjectUserSid"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x70""},{""@Name"":""NewProcessName"",""#text"":""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\lsass.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x2D0""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\lsass.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
2025-07-29T03:44:31+0000	6382,6382,2025-07-29 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\wininit.exe,PID: 0x2A8,Parent PID: 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"",""#text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x2A8""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\services.exe""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x230""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"

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\winlogon.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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x294""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\winlogon.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x238""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x228""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"
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"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x230""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\wininit.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text ":""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"
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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x228""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{" "@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text" ":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1 -0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName" ","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@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"":""S-1-5-18""},{""@Name"":"" SubjectUserName"",""#text"":""-""},{""@Name"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1E4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\csrss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text ":""0x1D4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "","#text":"-"},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "","#text":"S-1-16-16384""}]}}"

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\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"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x1D4""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{ ""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text "":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S- 1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName "",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":"" ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":""MandatoryLabel "",""#text"":""S-1-16-16384""}]}}"
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\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"":""SubjectDomainName"",""#text"":""-""},{" "@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":" "0x19C""},{""@Name"":""NewProcessName"",""#text"":""C:\\Windows\\System32\\autochk.exe""}, {""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""# text"":""0x180""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":"" S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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\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 "":""0x3E7""},{""@Name"":""NewProcessId"",""#text"":""0x180""},{""@Name"":"" NewProcessName"",""#text"":""C:\\Windows\\System32\\smss.exe""},{""@Name"":"" TokenElevationType"",""#text"":""%%1936""},{""@Name"":""ProcessId"",""#text"":""0x4""},{ ""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"",""#text"":""S-1-0-0""},{""@ Name"":""TargetUserName"",""#text"":""-""},{""@Name"":""TargetDomainName"",""#text"":"" -""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{""@Name"":""ParentProcessName""}, {""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}]}}"
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"":[{""@Name"":""SubjectUserSid"","" #text"":""S-1-5-18""},{""@Name"":""SubjectUserName"",""#text"":""-""},{""@Name"":"" SubjectDomainName"",""#text"":""-""},{""@Name"":""SubjectLogonId"",""#text"":""0x3E7""},{ ""@Name"":""NewProcessId"",""#text"":""0x6C""},{""@Name"":""NewProcessName"",""#text"" :""Registry""},{""@Name"":""TokenElevationType"",""#text"":""%%1936""},{""@Name"":"" ProcessId"",""#text"":""0x4""},{""@Name"":""CommandLine""},{""@Name"":""TargetUserSid"", ""#text"":""S-1-0-0""},{""@Name"":""TargetUserName"",""#text"":""-""},{""@Name"":"" TargetDomainName"",""#text"":""-""},{""@Name"":""TargetLogonId"",""#text"":""0x0""},{"" @Name"":""ParentProcessName""},{""@Name"":""MandatoryLabel"",""#text"":""S-1-16-16384""}] }}"

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%\PSEXESVC.EXE,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"",""#text"":""PsExec""},{""@Name"":""ImagePath"",""#text"":""%SystemRoot%\\PSEXESVC.EXE""},{""@Name"":""ServiceType"",""#text"":""user mode service""},{""@Name"":""StartType"",""#text"":""demand start""},{""@Name"":""AccountName"",""#text"":""LocalSystem""}]}}"
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\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"",""#text"":""VirtualBox 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"":""ServiceName"",""#text"":""VirtualBox Guest Additions Service""},{""@Name"":""ImagePath"",""#text"":""%SystemRoot%\\System32\\VBoxService.exe""},{""@Name"":""ServiceType"",""#text"":""user mode service""},{""@Name"":""StartType"",""#text"":""auto start""},{""@Name"":""AccountName"",""#text"":""LocalSystem""}]}}"
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""},{""@Name"":""ServiceType"",""#text"":""kernel mode driver""},{""@Name"":""StartType"",""#text"":""demand start""},{""@Name"":""AccountName""}]}}"
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"":{""Data"":[{""@Name"":""ServiceName"",""#text"":""VBoxWddm""},{""@Name"":""ImagePath"",""#text"":""\\SystemRoot\\System32\\drivers\\VBoxWddm.sys""},{""@Name"":""ServiceType"",""#text"":""kernel mode driver""},{""@Name"":""StartType"",""#text"":""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"":""KslD""},{""@Name"":""ImagePath"",""#text"":""system32\\drivers\\wd\\KslD.sys""},{""@Name"":""ServiceType"",""#text"":""kernel mode driver""},{""@Name"":""StartType"",""#text"":""demand start""},{""@Name"":""AccountName""}]}}"
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,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"",""#text"":""Microsoft Defender Core Service""},{""@Name"":""ImagePath"",""#text"":""\""C:\\ProgramData\\Microsoft\\Windows Defender\\platform\\4.18.25060.7-0\\MpDefenderCoreService.exe\""""},{""@Name"":""ServiceType"",""#text"":""user mode service""},{""@Name"":""StartType"",""#text"":""auto start""},{""@Name"":""AccountName"",""#text"":""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-N0IRN1T9IF6,1,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,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"",""#text"":""Printer Extensions and Notifications""},{""@Name"":""ImagePath"",""#text"":""%SystemRoot%\\system32\\svchost.exe -k print""},{""@Name"":""ServiceType"",""#text"":""user mode service""},{""@Name"":""StartType"",""#text"":""demand start""},{""@Name"":""AccountName"",""#text"":""LocalSystem""}]}}"

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-N0IRN1T9IF6,0,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)\Microsoft\Edge\Application\92.0.902.67\elevation_service.exe""",False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData"":{""Data"":[{""@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"":""ServiceType"","":""#text"":""user mode service""},{""@Name"":""StartType"","":""#text"":""demand start""},{""@Name"":""AccountName"","":""#text"":""LocalSystem""}]}}"
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\E1G6032E.sys,False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"","":""#text"":""Intel(R) PRO/1000 NDIS 6 Adapter Driver""},{""@Name"":""ImagePath"","":""#text"":""\\SystemRoot\\System32\\drivers\\E1G6032E.sys""},{""@Name"":""ServiceType"","":""#text"":""kernel mode driver""},{""@Name"":""StartType"","":""#text"":""demand start""},{""@Name"":""AccountName""}]}}"
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\uhssvc.exe""",False,C:\Users\VM\Desktop\System.evtx,"Audit success, classic",0,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"","":""#text"":""Microsoft Update Health Service""},{""@Name"":""ImagePath"","":""#text"":""\""C:\\Program Files\\Microsoft Update Health Tools\\uhssvc.exe\""""},{""@Name"":""ServiceType"","":""#text"":""user mode service""},{""@Name"":""StartType"","":""#text"":""disabled""},{""@Name"":""AccountName"","":""#text"":""LocalSystem""}]}}"
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"":{""Data"":[{""@Name"":""ServiceName"","":""#text"":""SysmonDrv""},{""@Name"":""ImagePath"","":""#text"":""C:\\Windows\\SysmonDrv.sys""},{""@Name"":""ServiceType"","":""#text"":""kernel mode driver""},{""@Name"":""StartType"","":""#text"":""boot start""},{""@Name"":""AccountName""}]}}"
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,"{""EventData"":{""Data"":[{""@Name"":""ServiceName"","":""#text"":""Sysmon""},{""@Name"":""ImagePath"","":""#text"":""C:\\Windows\\Sysmon.exe""},{""@Name"":""ServiceType"","":""#text"":""user mode service""},{""@Name"":""StartType"","":""#text"":""auto start""},{""@Name"":""AccountName"","":""#text"":""LocalSystem""}]}}"
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"":{""Data"":[{""@Name"":""ServiceName"","":""#text"":""Mozilla Maintenance Service""},{""@Name"":""ImagePath"","":""#text"":""\""C:\\Program Files (x86)\\Mozilla Maintenance Service\\maintenanceservice.exe\""""},{""@Name"":""ServiceType"","":""#text"":""user mode service""},{""@Name"":""StartType"","":""#text"":""demand start""},{""@Name"":""AccountName"","":""#text"":""LocalSystem""}]}}"