Event ID Quick Reference

SIMSPACE

Log Name	Event ID	Event Summary
Sysmon	1	Process create
Sysmon	2	File creation time
Sysmon	3	Network connection detected
Sysmon	4	Sysmon service state changed
Sysmon	5	Process terminated
Sysmon	6	Driver loaded
Sysmon	7	Image Loaded
Sysmon	8	Create Remote Thread
Sysmon	9	Raw Access Read
Sysmon	10	Process accessed
Sysmon	11	File created
Sysmon	12	Registry object added or deleted
Sysmon	13	Registry value set
Sysmon	14	Registry object renamed
Sysmon	15	File stream created
Sysmon	16	Sysmon configuration changed
Sysmon	17	Named pipe created
Sysmon	18	Named pipe connected
Sysmon	19	WMI filter
Sysmon	20	WMI consumer
Sysmon	21	WMI consumer
Sysmon	22	DNS Query
Sysmon	23	File Delete
Sysmon	24	Clipboard Changed
Security	1102	Audit log cleared
Security	4614	Security System Extension
Security	4624	Account successfully logged on

Log Name	Event ID	Event Summary
Security	4625	Account failed to log on
Security	4625	A user account failed to log on
Security	4634	Account successfully logged off
Security	4648	A logon was attempted using explicit credentials
Security	4672	Special privileges assigned to new logon
Security	4688	A new process has been created
Security	4697	Service Installation
Security	4698	Scheduled Task Creation
Security	4699	Scheduled Task Deleted
Security	4700	Scheduled Task Enabled
Security	4701	Scheduled Task Disabled
Security	4702	Scheduled Task Modified
Security	4720	Account created
Security	4722	Account enabled
Security	4723	User changed password
Security	4724	Password reset
Security	4732	Account added to a group
Security	4733	Account removed from a group
Security	4736	Account deleted
Security	4738	User account change
Security	4740	A user account was locked out
Security	4767	A user account was unlocked
Security	4776	The domain controller attempted to validate credentials for an account
Security	4778	Remote Desktop session reconnected
Security	4779	Remote desktop session disconnected
Security	4781	Account renamed