sourcetype	EventCod	comments	remove	Comments2	URL
WinEventLog:Application	100	start up	Remove		
WinEventLog:Application	10000	Failed to engage a Terminal Services session on a Windows 2k3 server	Remove	Arguably this setting could be useful for intrusion attempts on Win 2k3 devices but these log messages can be sourced from elsewhere.	
WinEventLog:Application	10032	Updates failed	Keep	This message has some usefulness in terms of alerting when the WSUS service side update fails, but overall if a patch installation has failed, it will be apparent from interrogation of the SCOM or WSUS UI	https://nitishkumar.net/tag/event-id-10032/
WinEventLog:Application	101	task scheduler failed to start a scheduled job	remove	This event arguably could have some bearing on security as it could alert to the presence of APTs - but we are stretching the imagination with this	https://social.technet.microsoft.com/Forums/windows/en-US/cdf859c2-e9a7-4795-9ad2-18b29ff5e920/task-scheduler-event-id-101-error-value?forum=winserver8gen
WinEventLog:Application	116	Microsoft Exchange OLEDB was unable to initialize event system cor	remove		https://www.experts-exchange.com/questions/26286141/Exchange-2003-Event-116.html
WinEventLog:Application	12344	File Server Resource Manager finished syncing claims from Active Directory and encountered errors during the sync, there is no such object on the server	remove		

WinEventLog:Application	1517	Windows saved user <user name> registry while an application or service was still using the registry during log off. The memory used by the user's registry has not been freed. The registry will be unloaded when it is no longer in use. This is often caused by services running as a user account, try configuring the services to run in either the LocalService or NetworkService account.	remove		http://www.eventid.net/display-eventid-1517-source-Userenv-eventno-1206-phase-1.htm
WinEventLog:Application	15268	hyper-v failed to get disk information	remove		
WinEventLog:Application	15281	SQL Server blocked access to procedure 'dbo.sp_get_sqlagent_properties' of component 'Agent XPs' because this component is turned off as part of the security configuration for this server	remove		
WinEventLog:Application	16385	Failed to schedule Software Protection service for re-start	remove	service added as a scheduled job but fails to start or restart - usually fixed by just removing it	
WinEventLog:Application	17069	This event is logged whenever SQL server starts up. If you're trying to correlate the end of an outage with an SQL instance starting up, this is the event you're looking for	remove		
WinEventLog:Application	17101		remove		
WinEventLog:Application	17103		remove		
WinEventLog:Application	17104		remove		
WinEventLog:Application	17111		remove		
WinEventLog:Application	17183	notice of recycling logs locally	remove		
WinEventLog:Application	17184	reinitialisation of local logging process	remove		
WinEventLog:Application	17202		remove		

WinEventLog:Application	17203	invalid trace directory	remove	https://community.dynamics.com/crm/f/117/t/265705
WinEventLog:Application	18210	backup failed	remove	
WinEventLog:Application	18264	SQL server database backup	remove	
WinEventLog:Application	18496		remove	
WinEventLog:Application	18950		remove	
WinEventLog:Application	20226	VPN / remote connection terminated	remove	
WinEventLog:Application	20249	Lost contact with a Sandbox Client.	remove	
WinEventLog:Application	2362	Related to a deprecated feature of SQL server	remove	
WinEventLog:Application	3421		remove	
WinEventLog:Application	4097	Event ID 4097 is produced on joining a Windows 2012 Server to a SBS 2003 domain for the first time.	remove	
WinEventLog:Application	4610	a security subsystem such as kerberos was started	remove	
WinEventLog:Application	49904		remove	
WinEventLog:Application	49916		remove	
WinEventLog:Application	49917		remove	
WinEventLog:Application	5		remove	
WinEventLog:Application	6701		remove	
WinEventLog:Application	6702		remove	
WinEventLog:Application	6704		remove	
WinEventLog:Application	6705		remove	
WinEventLog:Application	8198		remove	
WinEventLog:Application	8311		remove	
WinEventLog:Application	10311		remove	
WinEventLog:Application	12299		remove	
WinEventLog:Application	18960		remove	
WinEventLog:Application	20246		remove	
WinEventLog:Application	20248		remove	
WinEventLog:Application	216		remove	

WinEventLog:Application	24589	remove	
WinEventLog:Application	34	remove	
WinEventLog:Application	6290	remove	
WinEventLog:Application	6299	remove	
WinEventLog:Application	7886	remove	
WinEventLog:Application	8356	remove	
WinEventLog:Application	9666	remove	
WinEventLog:Application	1023	remove	
WinEventLog:Application	12309	remove	
WinEventLog:Application	1314	remove	
WinEventLog:Application	17890	remove	
WinEventLog:Application	2004	remove	
WinEventLog:Application	2159	remove	
WinEventLog:Application	218	remove	
WinEventLog:Application	4101	remove	
WinEventLog:Application	9003	remove	
WinEventLog:Application	1026	remove	
WinEventLog:Application	1101	remove	
WinEventLog:Application	1104	remove	
WinEventLog:Application	18267	remove	
WinEventLog:Application	20227	remove	
WinEventLog:Application	2370	remove	
WinEventLog:Application	325	remove	
WinEventLog:Application	326	remove	
WinEventLog:Application	3355	remove	
WinEventLog:Application	3402	remove	
WinEventLog:Application	3406	remove	
WinEventLog:Application	3407	remove	
WinEventLog:Application	3760	remove	
WinEventLog:Application	4356	remove	
WinEventLog:Application	6000	remove	
WinEventLog:Application	1010	remove	

WinEventLog:Application	1022	remove	
WinEventLog:Application	3014	remove	
WinEventLog:Application	327	remove	
WinEventLog:Application	8224	remove	
WinEventLog:Application	108	remove	
WinEventLog:Application	2	remove	
WinEventLog:Application	5084	remove	
WinEventLog:Application	103	remove	
WinEventLog:Application	18944	remove	
WinEventLog:Application	18957	remove	
WinEventLog:Application	102	remove	
WinEventLog:Application	105	remove	
WinEventLog:Application	17420	remove	
WinEventLog:Application	201	remove	
WinEventLog:Application	2138	remove	
WinEventLog:Application	23379	remove	
WinEventLog:Application	24591	remove	
WinEventLog:Application	26090	remove	
WinEventLog:Application	5401	remove	
WinEventLog:Application	912	remove	
WinEventLog:Application	17573	remove	
WinEventLog:Application	65	remove	
WinEventLog:Application	17192	remove	
WinEventLog:Application	2017	remove	
WinEventLog:Application	17972	remove	
WinEventLog:Application	2137	remove	
WinEventLog:Application	50	remove	
WinEventLog:Application	833	remove	
WinEventLog:Application	17189	remove	
WinEventLog:Application	528	remove	
WinEventLog:Application	906	remove	
WinEventLog:Application	2080	remove	

WinEventLog:Application	64	remove		
WinEventLog:Application	18204	remove		
WinEventLog:Application	18959	remove		
WinEventLog:Application	1035	remove		
WinEventLog:Application	700	remove		
WinEventLog:Application	1033	remove		
WinEventLog:Application	1034	remove		
WinEventLog:Application	1530	remove		
WinEventLog:Application	701	remove		
WinEventLog:Application	8313	remove		
WinEventLog:Application	6003	remove		
WinEventLog:Application	3041	remove		
WinEventLog:Application	12291	remove		
WinEventLog:Application	28673	remove		
WinEventLog:Application	18732	remove		
WinEventLog:Application	18832	remove		
WinEventLog:Application	2163	remove		
WinEventLog:Application	5586	remove		
WinEventLog:Application	8197	remove		
WinEventLog:Application	2003	remove		
WinEventLog:Application	1008	remove		
WinEventLog:Application	3	remove		
WinEventLog:Application	1315	remove		
WinEventLog:Application	12014	remove		
WinEventLog:Application	18702	remove		
WinEventLog:Application	4354	remove		
WinEventLog:Application	259	remove		
WinEventLog:Application	8230	remove		
WinEventLog:Application	18454	keep	failed SQL logins	https://gallery.technet.microsoft.com/SQL-Server-Login-Failure-8252820b
WinEventLog:Application	17137	remove		

WinEventLog:Application	1309	remove	
WinEventLog:Application	113	remove	
WinEventLog:Application	12289	remove	
WinEventLog:Application	9009	remove	
WinEventLog:Application	2330	remove	
WinEventLog:Application	8210	remove	
WinEventLog:Application	12288	remove	
WinEventLog:Application	2158	remove	
WinEventLog:Application	12293	remove	
WinEventLog:Application	257	remove	
WinEventLog:Application	4	remove	
WinEventLog:Application	705	remove	
WinEventLog:Application	208	remove	
WinEventLog:Application	1704	remove	
WinEventLog:Application	512	remove	
WinEventLog:Application	1001	remove	
WinEventLog:Application	18845	remove	
WinEventLog:Application	510	remove	
WinEventLog:Application	502	remove	
WinEventLog:Application	17418	remove	
WinEventLog:Application	1000	remove	
WinEventLog:Application	3006	remove	
WinEventLog:Application	10031	remove	
WinEventLog:Application	8306	remove	
WinEventLog:Application	0	remove	
WinEventLog:Application	18949	remove	
WinEventLog:Application	256	remove	
WinEventLog:Application	258	remove	
WinEventLog:Application	18689	remove	
WinEventLog:Application	6398	remove	
WinEventLog:Application	3005	remove	
WinEventLog:Application	978	remove	

WinEventLog:Application	121		remove	
WinEventLog:Application	6482		remove	
WinEventLog:Application	18265		remove	
WinEventLog:Application	1041		remove	
WinEventLog:Application	16384		remove	
WinEventLog:Application	903		remove	
WinEventLog:Application	1066		remove	
WinEventLog:Application	900		remove	
WinEventLog:Application	902		remove	
WinEventLog:Application	1003		remove	
WinEventLog:Application	9002		remove	
WinEventLog:Application	18456		investigate	needs some investigation - its about failed token based logins to SQL Server
WinEventLog:Application	18453		remove	this is for a successful login on SQL Server
WinEventLog:Directory-Servi	1083		remove	
WinEventLog:Directory-Servi	1955	Active Directory encountered a write conflict when applying replicated changes to an object.	remove	
WinEventLog:Directory-Servi	1162		remove	related to compaq and sNMP values
WinEventLog:Directory-Servi	2041	duplication of error messages was suppressed -	remove	
WinEventLog:Directory-Servi	2887	A SASL (Negotiate Kerberos NTLM or Digest) LDAP connection attempt was made without a valid signature	keep	attempts were made in the previous 24 hours to make clear text LDAP binds or unsigned binds - an event of this nature is worth some initial analysis
WinEventLog:Directory-Servi	700		remove	Online defragmentation
WinEventLog:Directory-Servi	701		remove	insufficient memory

WinEventLog:Directory-Servi	1226	remove	duplicate objects	
WinEventLog:Security	1105	remove	Event log automatic backup	
WinEventLog:Security	4720	keep	A user account was created	
WinEventLog:Security	4722	keep	user account was enabled	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4722
WinEventLog:Security	4724	keep	password reset attempted	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4724
WinEventLog:Security	4754	keep	just means a group other than a distribution group was created.	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4754
WinEventLog:Security	5378	keep	Can't imagine a case where this event would be reported, even if we see 2 of them here.	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5378
WinEventLog:Security	683	keep	tells us when a RDP session is disconnected as opposed to logged off, could be useful on rare occasions	
WinEventLog:Security	4663	remove	Surprised there's not more of these. The messages could be useful but MS has over-engineered things. These messages are useful for developers perhaps.	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4663

WinEventLog:Security	4695		remove	the chances of this message leading to potential malware or other unauthorised actions being detected are low. More likely there will be lots of false positives	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4695
WinEventLog:Security	4700		trial	worth keeping this, although be aware that there are likely to be some false positives. Suggest to trial and see how it goes.	
WinEventLog:Security	4701	scheduled task disabled	keep	fairly un-noisy, so probably worth keeping	
WinEventLog:Security	4755		keep	a group was changed	
WinEventLog:Security	4825	A user was denied the access to Remote Desktop. By default, users are allowed to connect only if they are members of the Remote Desktop Users group or Administrators group	keep		
WinEventLog:Security	4692	Backup of data protection master key was attempted	remove	Noise. Not what it says on the tin.	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4692
WinEventLog:Security	4697	A service was installed in the system	keep	Worth keeping - starting up a new service can be a malware indicator	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4697
WinEventLog:Security	4728	A member was added to a security-enabled global group	keep		https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4728
WinEventLog:Security	4733	A member was removed from a group	remove		
WinEventLog:Security	4735	A security-enabled local group was changed	keep		

WinEventLog:Security	4737	A security-enabled global group was changed	keep		
WinEventLog:Security	551	User initiated logoff	keep		
WinEventLog:Security	4627	Group membership information	keep	Identifies the account that requested the logon - NOT the user who just logged on.	
WinEventLog:Security	4756	A member was added to a security-enabled universal group	keep		
WinEventLog:Security	4954	Windows Firewall Group Policy settings has changed. The new settings have been applied	keep	Keep, but not if local firewalls are not being used. May as well keep - its not too noisy.	
WinEventLog:Security	4718	System security access was removed from an account	remove		
WinEventLog:Security	5141	documents the revokation of logon rights such as "Access this computer from the network" or "Logon as a service".	keep		
WinEventLog:Security	680	Account Used for Logon by	keep	Its not clear on the designed usage purpose of this message - it appears when a user tries to logon with no domain membership, so you'll see it with some brute force attempts	http://forum.ultimatewindowssecurity.com/Topic778-129-1.aspx
WinEventLog:Security	5137	A directory service object was created	keep		
WinEventLog:Security	5031	The Windows Firewall Service blocked an application from accepting incoming connections on the network	remove	count of 24 tells us that Windows Firewall isn't in extensive usage or its poorly configured	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=5031
WinEventLog:Security	4740	A user account was locked out	keep	expected low volume of traffic - can be useful in some investigations	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4740

WinEventLog:Security	4693	Recovery of data protection master key was attempted	remove		
WinEventLog:Security	4702	A scheduled task was updated	keep		
WinEventLog:Security	4723	An attempt was made to change an account's password	keep		
WinEventLog:Security	601	Attempt to install service	keep		https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=601
WinEventLog:Security	4801	Workstation unlocked	remove		https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4801
WinEventLog:Security	4647	User initiated logoff	keep	This event seems to be in place of 4634 in the case of Interactive and RemoteInteractive (remote desktop) logons. This is a plus since it makes it easier to distinguish between logoffs resulting from an idle network session and logoffs where the user actually logs off with from his console.	
WinEventLog:Security	4738	A user account was changed	keep		
WinEventLog:Security	4798	A user's local group membership was enumerated	keep	classic indicator of malware activity	
WinEventLog:Security	4904	an attempt was made to register an events source	keep	potential unauthorised activity indicator, although quite unlikely, aside from attenmpts to obscure logs by filling them with drivel	
WinEventLog:Security	4905	An attempt was made to unregister a security event source	keep		

WinEventLog:Security	4931	An Active Directory replica destination naming context was modified	remove		
WinEventLog:Security	4742	A computer account was changed	keep	not clear at the actual usefulness of this	
WinEventLog:Security	4767	A user account was unlocked	keep	could be useful - for example - a dormant JML account is unlocked	
WinEventLog:Security	515	A trusted logon process has registered with the Local Security Authority	keep	An occurrence of event 515 is logged at startup and occasionally afterwards for each logon process on the system.	
WinEventLog:Security	4800	The workstation was locked	keep	When either a user manually locks his workstation or the workstation automatically locks its console after a period of inactivity this event is logged.	
WinEventLog:Security	4779	A session was disconnected from a Window Station	keep	more particular to a RDP logoff	
WinEventLog:Security	4778	A session was reconnected to a Window Station	keep	RDP	
WinEventLog:Security	528	Successful Network Logon	keep	Event 528 is logged whenever an account logs on to the local computer, except for in the event of network logons	
WinEventLog:Security	598	Failed to release memory allocation	keep		https://kb.eventtracker.com/evtpass/evtPages/EventId_598_WDSMC_63244.asp

WinEventLog:Security	4653		investigate	not clear how useful this is - if it is generated in response to failed VPN connections then its probably worth keeping	
WinEventLog:Security	4770	A Kerberos service ticket was renewed	keep	Kerberos limits how long a ticket is valid. If a ticket expires when the user is still logged on, Windows automatically contacts the domain controller to renew the ticket which triggers this event.	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4770
WinEventLog:Security	4793	The Password Policy Checking API was called	remove	Looks like a legacy code, should have been removed years ago but wasn't	
WinEventLog:Security	552	Logon attempt using explicit credentials	keep	Another type of login message, this one is useful for tracking user account switching	
WinEventLog:Security	6416	A new external device was recognized by the system	keep	seems like this message is generated whenever any device is inserted, not just USBs	
WinEventLog:Security	4696	A primary token was assigned to process	keep		
WinEventLog:Security	578	Privileged object operation	remove	this about use of rights as opposed to assgning of rights - likely to be very noisy with little security value	

WinEventLog:Security	577	unable to load registry	remove	This message can cover a whole plethora of problems, mostly operational, and mostly not security. There is a chance that malware can corrupt registries, however other layers of security can deal with this issue
WinEventLog:Security	4933	Synchronization of a replica of an Active Directory naming context has ended	remove	word on the street is its not so useful
WinEventLog:Security	4932	Synchronization of a replica of an Active Directory naming context has begun	remove	
WinEventLog:Security	599	Unprotection of auditable protected data	investigate	A program used the CryptUnprotectData function to read data encrypted by Data Protection API (DPAPI). The name of the encrypted data is provided in the event message, but because this name is determined by the program that originally created the encrypted data, it might not be recognizable. This type of event can be a result of unauthorised access to encrypted passwords - but exactly how useful is it? needs some investigation
WinEventLog:Security	5059	Key migration operation	remove	

WinEventLog:Security	5154	The Windows Filtering Platform has permitted an application or service to listen on a port for incoming connections	remove	remove for servers because use of local packet filters is hard ot justify based on TCO v risk - apart from mobile users/EUDs
WinEventLog:Security	4611	A trusted logon process has been registered with the Local Security Authority	remove	lots of noise, little value
WinEventLog:Security	4771	Kerberos pre-authentication failed	keep	In Windows Kerberos, password verification takes place during pre-authentication, so in a kerberos enviornment one can expect to see this for all password fails
WinEventLog:Security	4658	The handle to an object was closed	remove	extremely noisy. If you can match it with a corresponding event 4656
WinEventLog:Security	600	A process was assigned a primary token	remove	Very noisy - remote chance of being able to detect unauthorised behaviour
WinEventLog:Security	4661	A handle to an object was requested	remove	Very noisy - remote chance of being able to detect unauthorised behaviour
WinEventLog:Security	4675	SIDs were filtered	investigate	why are there so many of these?
WinEventLog:Security	4985		remove	Microsoft cryptic message that even they don't understand
WinEventLog:Security	5157		remove	Windows firewall dropped a packet

WinEventLog:Security	4656		remove	object based events - only useful in cases where fine grained access to files or folders has to be logged
WinEventLog:Security	4625	Failed local logon	keep	
WinEventLog:Security	576	Privileges assigned to logon account	remove	these privileges are usefu to know but this standard for your IDAM config - you have to know this basically, and telling the user about privileges for logon isn't so helpful
WinEventLog:Security	540	Successful network logon	keep	
WinEventLog:Security	538	user logoff	keep	for any type of connection
WinEventLog:Security	5140	network share was accessed	keep	lots of windows attacks involve exploiting open shares such as $ADMIN and default hidden shares such as $C
WinEventLog:Security	4768	kerberos ticket requested	remove	This event is logged on domain controllers only and both success and failure instances of this event are logged - remove because you only need logon and logoff events, not this. you already know you have Kerberos
WinEventLog:Security	4957	windows firewall did not apply the following rule	remove	
WinEventLog:Security	5136	A directory service object was modified	keep	

WinEventLog:Security	4648	A logon was attempted using explicit credentials	keep	captures lots of useful events - e.g. a user maps a drive to a server but specifies a different user's credentials
WinEventLog:Security	4673		remove	flags use of privileges. I would say can this one because operationally priivleges need to be known anyway and the noise doesn't' justify the benefit coming from it
WinEventLog:Security	4670	Windows logs this event when someone changes the access control list on an object.	keep	
WinEventLog:Security	4674	An operation was attempted on a privileged object	remove	
WinEventLog:Security	4769	A Kerberos service ticket was requested	keep	This is different from 4768. Service tickets are obtained whenever a user or computer accesses a server on the network. For example, when a user maps a drive to a file server, the resulting service ticket request generates event ID 4769 on the DC.

WinEventLog:Security	4776		keep	Despite what this event says, the computer is not necessarily a domain controller; member servers and workstations also log this event for logon attempts with local SAM accounts.
WinEventLog:Security	593		Remove	process exited - arguably can help in incident investigation but not so useful on the whole
WinEventLog:Security	592		remove	
WinEventLog:Security	4672	This event lets you know whenever an account assigned any "administrator equivalent" user rights logs on.	Keep	
WinEventLog:Security	5447		Remove	
WinEventLog:Security	4662		Remove	Use 5136 if this event is of interest - better info, more useful
WinEventLog:Security	4703		Remove	generally whenever nobody can explain what an event means, its probably not so useful
WinEventLog:Security	5158		Remove	Too noisy with little return in terms of benefits
WinEventLog:Security	5061		Remove	Vague info on this but enough to know its not so valuable

WinEventLog:Security	5058		Remove	again - little info on the purpose of this apart from intuitive reading of the description -	
WinEventLog:Security	521		Keep	Useful for alerting on event logging failures	
WinEventLog:Security	4689		Remove	No so useful for security, especially not at this cost	
WinEventLog:Security	4688		Remove		
WinEventLog:Security	5156		Investigate	Some of these can be interesting but most are not.	
WinEventLog:Security	4634		Keep		
WinEventLog:Security	4624	An account was successfully logged on	keep	there is a "logon type" field in the message body - this is useful for correlation against different login types	https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventid=4624
WinEventLog:System	10005		remove		
WinEventLog:System	1004		remove		
WinEventLog:System	1074		remove		
WinEventLog:System	129		remove		
WinEventLog:System	4000		remove		
WinEventLog:System	4006		remove		
WinEventLog:System	44		remove		
WinEventLog:System	7000		remove		
WinEventLog:System	7009		remove		
WinEventLog:System	7031		remove		
WinEventLog:System	10010		remove		
WinEventLog:System	10029		remove		
WinEventLog:System	2		remove		
WinEventLog:System	35		remove		
WinEventLog:System	5807		remove		
WinEventLog:System	1500		remove		

WinEventLog:System	5823	remove	
WinEventLog:System	6038	remove	
WinEventLog:System	1150	remove	
WinEventLog:System	12294	remove	
WinEventLog:System	1502	remove	
WinEventLog:System	45056	remove	
WinEventLog:System	5722	remove	
WinEventLog:System	7011	remove	
WinEventLog:System	1020	remove	
WinEventLog:System	15	remove	
WinEventLog:System	2001	remove	
WinEventLog:System	153	remove	
WinEventLog:System	5723	remove	
WinEventLog:System	1	remove	
WinEventLog:System	20001	remove	
WinEventLog:System	32	remove	
WinEventLog:System	37	remove	
WinEventLog:System	4200	remove	
WinEventLog:System	4201	remove	
WinEventLog:System	7002	remove	
WinEventLog:System	7042	remove	
WinEventLog:System	27	remove	
WinEventLog:System	1064	remove	
WinEventLog:System	98	remove	
WinEventLog:System	1085	remove	
WinEventLog:System	10028	remove	
WinEventLog:System	1503	remove	
WinEventLog:System	16	remove	
WinEventLog:System	5805	remove	
WinEventLog:System	36882	remove	
WinEventLog:System	1030	remove	
WinEventLog:System	1111	remove	

WinEventLog:System	36888	remove	
WinEventLog:System	5186	remove	
WinEventLog:System	4	remove	
WinEventLog:System	14554	remove	
WinEventLog:System	7001	remove	
WinEventLog:System	12503	remove	
WinEventLog:System	12517	remove	
WinEventLog:System	3	remove	
WinEventLog:System	7035	remove	
WinEventLog:System	101	remove	
WinEventLog:System	103	remove	
WinEventLog:System	108	remove	
WinEventLog:System	7040	remove	
WinEventLog:System	26	remove	
WinEventLog:System	7045	remove	
WinEventLog:System	1112	remove	
WinEventLog:System	6013	remove	
WinEventLog:System	10016	remove	
WinEventLog:System	11	remove	
WinEventLog:System	10009	remove	
WinEventLog:System	36887	remove	
WinEventLog:System	7036	remove	
