

Normal Date	Priority	Classification	Common Event	Vendor Message	Origin Login	Origin Host	Impacted Host	Log Message	Object
04/08/08 06:39:3...		Access Failure	Failed Object Open	560	local service	Jupiter	Jupiter	4/8/2008 6:39 PM TYPE=FailureAudit USER=NT AUTHORITY\LOCAL SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetbiosSmb Handle ID:- Operation ID:{0,101100738} Process ID: 800 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:LOCAL SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\Device\NetbiosSmb
04/08/08 05:52:4...		Other Audit	Failed Object Open	560	system	Jupiter	Jupiter	4/8/2008 5:52 PM TYPE=FailureAudit USER=NT AUTHORITY\SYSTEM COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:Mutant Object Name:\BaseNamedObjects\RasPbFile Handle ID:- Operation ID:{0,100856213} Process ID:720 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:JUPITER Primary Domain:SA...	\BaseNamedObjects\RasPbFile
04/08/08 06:48:3...	30	Access Failure	Failed Object Open	560	local service	Jupiter	Jupiter	4/8/2008 6:48 PM TYPE=FailureAudit USER=NT AUTHORITY\LOCAL SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetbiosSmb Handle ID:- Operation ID:{0,101143989} Process ID: 800 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:LOCAL SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\Device\NetbiosSmb
04/08/08 02:11:3...	30	Access Failure	Failed Object Open	560	local service	Jupiter	Jupiter	4/8/2008 2:11 PM TYPE=FailureAudit USER=NT AUTHORITY\LOCAL SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetbiosSmb Handle ID:- Operation ID:{0,93766959} Process ID:800 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:LOCAL SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\Device\NetbiosSmb
04/21/08 12:12:4...	30	Access Failure	Failed Object Open	560	local service	Jupiter	Jupiter	4/21/2008 12:12 PM TYPE=FailureAudit USER=NT AUTHORITY\LOCAL SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetbiosSmb Handle ID:- Operation ID:{0,366245} Process ID:808 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:LOCAL SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\Device\NetbiosSmb
04/08/08 08:02:3...	30	Access Failure	Failed Object Open	560	local service	Jupiter	Jupiter	4/8/2008 8:02 PM TYPE=FailureAudit USER=NT AUTHORITY\LOCAL SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetbiosSmb Handle ID:- Operation ID:{0,101482990} Process ID: 800 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:LOCAL SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\Device\NetbiosSmb
04/08/08 10:13:2...	30	Access Failure	Failed Object Open	560	system	Jupiter	Jupiter	4/8/2008 10:13 PM TYPE=FailureAudit USER=NT AUTHORITY\SYSTEM COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:Mutant Object Name:\BaseNamedObjects\RasPbFile Handle ID:- Operation ID:{0,102082631} Process ID:1492 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:JUPITER Primary Domain:SA...	\BaseNamedObjects\RasPbFile
04/21/08 11:23:5...	30	Access Failure	Failed Object Open	560	network service	Jupiter	Jupiter	4/21/2008 11:23 AM TYPE=FailureAudit USER=NT AUTHORITY\NETWORK SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:Event Object Name:\BaseNamedObjects\DINPUTWINMM Handle ID:- Operation ID:{0,53908} Process ID:1056 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:NETWORK SERVICE Primary Domain:NT AUTHORITY Primary Logon I...	\BaseNamedObjects\DINPUTWIN...
04/21/08 11:59:5...	30	Access Failure	Failed Object Open	560	network service	Jupiter	Jupiter	4/21/2008 11:59 AM TYPE=FailureAudit USER=NT AUTHORITY\NETWORK SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetBT_Tcpip_{42CA64E4-4977-463B-B167-EC8770D0E5F} Handle ID:- Operation ID:{0,348131} Process ID:768 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:NETWORK SERV...	\Device\NetBT_Tcpip_{42CA64E4...
04/08/08 08:14:3...	30	Access Failure	Failed Object Open	560	system	Jupiter	Jupiter	4/8/2008 8:14 PM TYPE=FailureAudit USER=NT AUTHORITY\SYSTEM COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:Mutant Object Name:\BaseNamedObjects\RasPbFile Handle ID:- Operation ID:{0,101536211} Process ID:200 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:JUPITER Primary Domain:SA...	\BaseNamedObjects\RasPbFile
04/08/08 03:32:2...	30	Access Failure	Failed Object Open	560	network service	Jupiter	Jupiter	4/8/2008 3:32 PM TYPE=FailureAudit USER=NT AUTHORITY\NETWORK SERVICE COMP=JUPITER SORC=Security CATG=Object Access EVID=560 MSG=Object Open: Object Server:Security Object Type:File Object Name:\Device\NetBT_Tcpip_{673E8F41-D9DF-48B2-956F-AF3E153107D4} Handle ID:- Operation ID:{0,100140369} Process ID:756 Image File Name:C:\WINDOWS\system32\svchost.exe Primary User Name:NETWORK SERV...	\Device\NetBT_Tcpip_{673E8F41...

LogRhythm users have on-demand access to normalized data, prioritized events and correlated information along with supporting raw log data all delivered in a single window for compliance assurance, forensic analysis and root-cause investigations.