

Investigator Wizard

Select Search Type

Search Types

- Event Manager Search**
Select this type of search to query the Event Manager. Events meeting your criteria will be displayed in Investigator.
- Log Manager Search**
Select this type of search to query Investigator. Only logs currently available in Investigator are displayed.
- LogMart Search**
Select this type of search to query LogMart.
- Include Raw Log**
Check this box to include the raw log text. This is more resource intensive and is only available when performing a low-level search.

Select Date Range to Query

- In the Last** Days
- Date is Before**
- Date is After**
- Date is Between**

Specify Event Selection

Operator: [v] Field: IP Address (Origin) Filter Mode: Is Filtered Values: 192.168.1.21

Buttons: Add New Field Filter, Edit Values, Delete

LogRhythm Console - [Investigator]

Log/Event Analyzer | Log Viewer

Aggregate Log/Event List (0 logs/events)

Drag a column header here to group by that column.

First Normal Date	Last Normal Date	Count	Priority	Entity	Direction	Classification	Common Event	Vendor Message	Origin Host	Impacted Host	Impacted Appl	TCP/UDP Port ID	TCP/UDP Port
03/24/08 01:59.1	03/24/08 07:12.0	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	server3			
03/24/08 01:59.1	03/24/08 07:11.5	2	0	LogRhythm Labs	External	Account Deleted	Group Deleted	0049	192.168.1.21	172.10.1.9			
03/24/08 01:59.0	03/24/08 07:11.5	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.26	111/TCP	40030	111
03/24/08 01:59.0	03/24/08 07:11.4	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.6			
03/24/08 01:58.5	03/24/08 07:11.4	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	server4			
03/24/08 01:58.5	03/24/08 07:11.4	2	0	LogRhythm Labs	Local	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.21	5800/ICMP	40057	5800
03/24/08 01:58.5	03/24/08 07:11.4	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.2	135/ICMP	40018	135
03/24/08 01:58.5	03/24/08 07:11.3	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.14	79/ICMP	40061	79
03/24/08 01:58.5	03/24/08 07:11.3	2	2	LogRhythm Labs	External	Information	Session Started	0039	192.168.1.21	172.10.1.14	BO0TP - Client	40049	68
03/24/08 01:58.5	03/24/08 07:11.3	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.5			
03/24/08 01:58.4	03/24/08 07:11.3	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.20			
03/24/08 01:58.4	03/24/08 07:11.3	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	server1			
03/24/08 01:58.4	03/24/08 07:11.3	2	0	LogRhythm Labs	External	Access Revoked	User Removed From Group	0046	192.168.1.21	172.10.1.20			
03/24/08 01:58.4	03/24/08 07:11.2	2	0	LogRhythm Labs	External	Authentication S...	Authentication	0004	192.168.1.21	172.10.1.20			
03/24/08 01:58.4	03/24/08 07:11.2	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.12			
03/24/08 01:58.3	03/24/08 07:11.1	2	2	LogRhythm Labs	External	Information	Session Started	0039	192.168.1.21	server4	Kazaa	40043	1214
03/24/08 01:58.3	03/24/08 07:11.1	3	0	LogRhythm Labs	External	Authentication S...	Authentication	0004	192.168.1.21	172.10.1.10			
03/24/08 01:58.3	03/24/08 07:11.1	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	usep14	110/UDP	40016	110
03/24/08 01:58.2	03/24/08 07:11.0	2	2	LogRhythm Labs	External	Information	Session Started	0039	192.168.1.21	172.10.1.6	X/Window System	40086	6000
03/24/08 01:58.2	03/24/08 07:11.0	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	usep14	5500/ICMP	40082	5500
03/24/08 01:58.1	03/24/08 07:11.0	2	10	LogRhythm Labs	External	Access Granted	User Added To Group	0045	192.168.1.21	172.10.1.5			
03/24/08 01:58.1	03/24/08 07:10.5	2	0	LogRhythm Labs	External	Access Revoked	User Removed From Group	0046	192.168.1.21	172.10.1.2			
03/24/08 01:58.0	03/24/08 07:10.4	2	0	LogRhythm Labs	External	Account Deleted	Group Deleted	0049	192.168.1.21	server2			
03/24/08 01:57.5	03/24/08 07:10.4	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.29	79/ICMP	40002	79
03/24/08 01:57.5	03/24/08 07:10.3	2	2	LogRhythm Labs	External	Information	Session Started	0039	192.168.1.21	172.10.1.20	Microsoft Directo...	40089	445
03/24/08 01:57.5	03/24/08 07:10.3	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.14			
03/24/08 01:57.4	03/24/08 07:10.2	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	usep7	PPTP - Point-to...	40025	1723
03/24/08 01:57.3	03/24/08 07:10.2	2	0	LogRhythm Labs	External	Access Revoked	User Removed From Group	0046	192.168.1.21	172.10.1.14			
03/24/08 01:57.3	03/24/08 07:10.2	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.5			
03/24/08 01:57.3	03/24/08 07:10.2	3	0	LogRhythm Labs	External	Authentication S...	Authentication	0004	192.168.1.21	172.10.1.17			
03/24/08 01:57.3	03/24/08 07:10.2	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	usep5	6000/ICMP	40090	6000
03/24/08 01:57.3	03/24/08 07:10.2	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.20	IMAP - Internet...	40059	143
03/24/08 01:57.3	03/24/08 07:10.1	2	0	LogRhythm Labs	External	Account Deleted	Group Deleted	0049	192.168.1.21	172.10.1.9			
03/24/08 01:57.2	03/24/08 07:10.1	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	server5			
03/24/08 01:57.2	03/24/08 07:10.1	2	0	LogRhythm Labs	External	Access Success	General Access Success	0012	192.168.1.21	172.10.1.12			
03/24/08 01:57.2	03/24/08 07:10.1	2	2	LogRhythm Labs	External	Account Deleted	Group Modified	0048	192.168.1.21	172.10.1.3			
03/24/08 01:57.2	03/24/08 07:10.0	2	0	LogRhythm Labs	External	Authentication S...	Authentication	0004	192.168.1.21	172.10.1.18			
03/24/08 01:57.2	03/24/08 07:10.0	2	0	LogRhythm Labs	External	Network Traffic	Netflow V5 Flow	0041	192.168.1.21	192.168.1.18	TFTP - Trivial FL	40002	69
03/24/08 01:57.2	03/24/08 07:10.0	2	14	LogRhythm Labs	External	Reconnaissance	General Reconnaissance	0018	192.168.1.21	172.10.1.6	DNS - Domain N...	40058	53

eDiscovery efforts can be cut down from days, weeks or even months to minutes with LogRhythm. In this example, with 3 simple clicks of the mouse an investigator gathers all activity logs for a specific server for the last 30 days. Similar retrievals can occur for logs associated with a specific employee, system, process and more.