

Auditing session activity on networks



Auditing session activity on networks

Session activity monitoring is one of the most basic but important ways administrators analyze network activity. Session details show when users are logged into the network, as well as a breakdown of users' specific network activities during each session. All of this helps to establish a solid baseline for explaining users' interactions with the network.

Uses of session information

Session information helps administrators understand the following aspects of their network:

Who's using the network: Know which users are actively using the network so it's easier to spot users who shouldn't be logged in.

How they log in: Differentiate between users logging in to a machine directly, and users logging in via a remote desktop or terminal services connection.

Where they log in from: Identify which machines are being used to establish remote connections.

What system they log in to: Discover which devices are used most frequently on the network.

When they log in and off: Analyze the duration of various sessions, and identify idle sessions as well as sessions which have not been logged out of. Looking at these statistics for a specific device can provide an idea of the level of engagement with that device.

The need for an auditing tool

Individual devices generate login and logoff logs, which provide session information; however, they don't offer native reporting and analysis capabilities for sessions in a holistic way. Using a dedicated, centralized auditing tool solves this problem and offers the following benefits:

A comprehensive network overview: Collate the session information from various network devices and present it in a unified manner.

Login patterns: Identify hosts and users with the highest number of logins to the network.

Anomalies: Identify any odd sessions, such as logins during non-working hours, logins by users without sufficient permissions, and the like.

Session activity monitoring with EventLog Analyzer

With EventLog Analyzer, tracking session activity across a network is quick and easy. The solution provides predefined reports that track entire user sessions from start to finish, including details of the user's activity during the session.

Where do I access these reports?

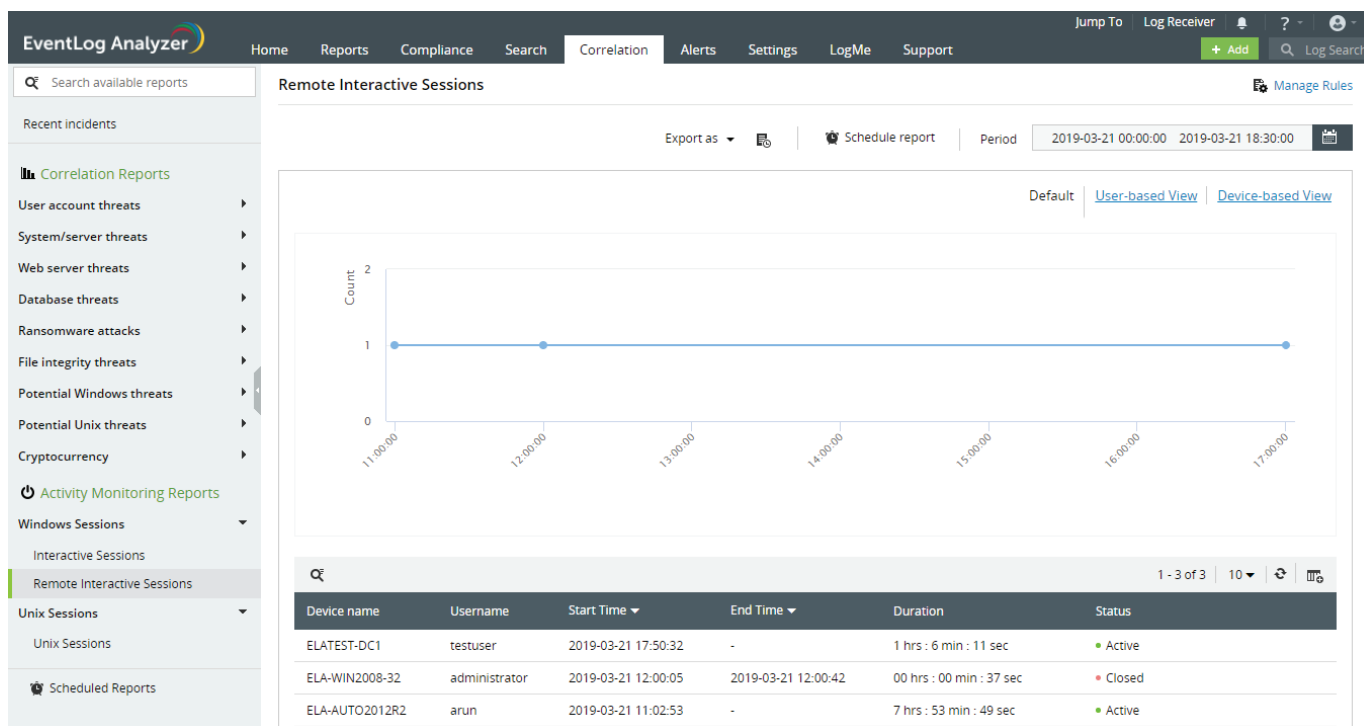
Access the session activity reports by going to the Correlation tab and clicking on the desired report under Activity Monitoring Reports in the left panel.

What do these reports provide information on?

Currently, the provided reports cover the following types of sessions:

- Windows interactive sessions
- Windows remote interactive sessions
- Windows Password Manager Pro sessions
- Unix sessions

Working with session activity reports



The screenshot displays the EventLog Analyzer interface. The top navigation bar includes Home, Reports, Compliance, Search, Correlation (selected), Alerts, Settings, LogMe, and Support. The left sidebar shows a search bar and a list of reports under 'Activity Monitoring Reports', with 'Remote Interactive Sessions' selected. The main content area shows the report title 'Remote Interactive Sessions' and a period selector set to '2019-03-21 00:00:00' to '2019-03-21 18:30:00'. Below the title is a line chart with 'Count' on the y-axis (0 to 2) and time on the x-axis. The chart shows a count of 1 for three time points: 11:00:00, 12:00:00, and 17:00:00. Below the chart is a table with columns: Device name, Username, Start Time, End Time, Duration, and Status. The table contains three rows of session data.

Device name	Username	Start Time	End Time	Duration	Status
ELATEST-DC1	testuser	2019-03-21 17:50:32	-	1 hrs : 6 min : 11 sec	Active
ELA-WIN2008-32	administrator	2019-03-21 12:00:05	2019-03-21 12:00:42	00 hrs : 00 min : 37 sec	Closed
ELA-AUTO2012R2	arun	2019-03-21 11:02:53	-	7 hrs : 53 min : 49 sec	Active

Session activity reports help to:

- Identify, in one glance, who's active on the network at a given moment.
- Pick out improperly ended sessions.
- Analyze how many sessions occur at various times, and identify abnormally active or idle periods.
- Drill down into sessions of interest and analyze exactly what occurred during each session.
- Identify the most active users and the devices they use. Similarly, you can also identify frequently used devices in the network, and the users who are active on them.

The default view of a session activity report provides you with the following information:

- The graph shows you the number of sessions started at various intervals during the selected time window.
- The table lists each session and specifies details such as the user and device names, start and end times, duration, and status of the session (active or ended).
- For sessions that have ended, the reason they ended is also given; for instance, whether the session was logged off or the device was shut down. For ongoing sessions, the duration column displays a live timer to show you how long the user has been active.
- To track a user's activity during a session, you can click View History on the respective session's entry in the table. The page that opens presents a timeline, which lists the user's various actions in chronological order.

You can also switch the report to a user-based or device-based view. You can do this by selecting the user-based view or device-based view links which appear when you hover your mouse over the graph.

User-based view: Tells you the number of sessions started by each user during the selected time window, and the devices they were active on.

Device-based view: Tells you the number of sessions started on each device during the selected time window, and the users active on those devices.

To view sessions from a particular user or device, you can either:

- Use the search bar in any of the reports.
- Navigate to the user or device-based view and click on the respective user/device name.

User-defined session rules

Normally, a session starts when a user logs in to a device, and it ends when the user logs off or the device is shut down. The predefined session activity reports described above provide you with information based on this definition of a session. However, typical sessions last for several hours, and if you're interested in a particular session, you might still have a lot of information to go through.

EventLog Analyzer takes you beyond the simple login/logoff model of a session and allows you to define the starting and ending conditions of a session—or activity rules. These activity rules consist of a sequence of network events. This way, when the events described by these rules occur, you can track all activities that occur in between them.

For example, you may want to monitor activity on one of your critical file servers. You wish to monitor users who log in remotely to the file server, and access a file after several failed attempts. You are also interested in tracking how they obtained this access. To monitor this, you can create an activity rule in the following way:

Activity starting rule: Remote login to the file server, followed by a few failed attempts at accessing a file.

Activity ending rule: Successful access of the file.

By creating a session activity rule this way, you not only monitor unauthorized accesses to confidential files, but also identify security loopholes in your file server which allow these accesses.

How to create activity rules

Session activity reports can be found in the Correlation tab. Create a new activity rule by going to:

Correlation > Manage Rules > Activity Rules > +Create Activity Rule

The screenshot displays the 'EventLog Analyzer' interface for creating an activity rule. The top navigation bar includes 'Home', 'Reports', 'Compliance', 'Search', 'Correlation', 'Alerts', 'Settings', 'LogMe', and 'Support'. The main content area is titled 'Unnamed rule' and shows a two-step process: '1 Activity Starting Rule' and '2 Activity Ending Rule'. The first step is active and shows a primary action: 'Action 1: An account successfully logs on to a device in the network.' with a green checkmark. Below this action is a criteria pattern: 'Device type' equals 'Any'. There is a 'Threshold Limit' checkbox which is unchecked. The second step is 'Action 2: An account successfully logs on to the database.' with a green checkmark. Below this action is a 'Threshold Limit' checkbox which is unchecked. Between the two sub-rules, there is a 'Followed by within' section with '10 Mins' selected. At the bottom, there is a prompt: 'Select one or more actions from left pane to build activity rule'. The left pane contains a search bar and a list of event categories: Logon events, Workstation events, Network device events, Database events, Webservice events, Windows logons, Windows file system, Windows account management, Windows group management, Windows Firewall, Windows Policies, and Windows software management.

The rule builder interface is the same as the correlation rule builder interface. You can learn how to use it in [this video](#). Session activity rules are similar to correlation rules, and the only differences are:

Session activity rules are split into two sub-rules: The activity starting rule and the activity ending rule define how a session starts and ends, respectively.

The use of a primary action: Each sub-rule of an activity rule has one primary action. By default, it's the first action of each sub-rule, but you can designate any action as primary by selecting the green check mark next to the required action. You can compare the fields of the primary actions of both rules using the Link to filter.

Conclusion

EventLog Analyzer is extremely effective in auditing user sessions on an organization's network. Session activity reports provide granular information regarding user activity and remain up-to-date with all activities on your network. These rules allow you to monitor custom defined sessions and track user activity with simple, straightforward reports. With EventLog Analyzer's easy-to-use interface and intuitive reports, it's easy to view all required session information and quickly identify patterns or anomalies.

ManageEngine EventLog Analyzer

EventLog Analyzer is a web-based, real-time log management and IT compliance solution that combats network security attacks. With comprehensive log management capabilities, EventLog Analyzer helps organizations meet their diverse auditing needs. It also offers out-of-the-box compliance reports and alerts that meet stringent IT regulatory mandate requirements with ease.

\$ Get Quote

↓ Download



Toll Free

+1 844 649 7766

Direct Dialing Number

US : +1-408-352-9254



eventlog-support@manageengine.com



www.eventloganalyzer.com