Logsign

Logsign Next-Gen SIEM Cluster Infrastructure

Datasheet

Cluster Big Data Infrastructure

What are Cluster Infrastructure and High Availability?

The cluster infrastructure model requires two or more servers called “nodes” to work together. With this working principle, a cluster of servers allows for more availability, more reliability, and more scalability compared to just one server.

High availability is the support provided to the service with more than one machine or device so that it is not interrupted for any reason.

Logsign SIEM’s Rapid, Flexible and Scalable Cluster Technology

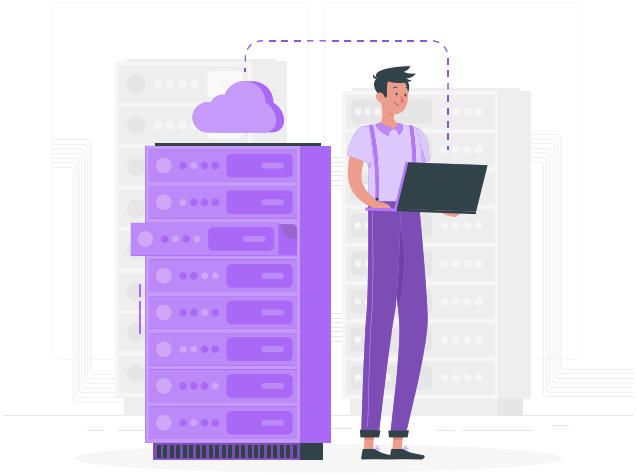
Depending on the size of the network it supports, Logsign may be installed on a cloud or on one or more physical servers. The services used on Logsign, which works as an active-active cluster, are activated on various servers in order to meet the performance requirements and optimization conditions. The cluster infrastructure enables both horizontal and vertical scalability.

Logsign SIEM Cluster infrastructure begins with minimum of three Nodes. The data redundancy capacity may rapidly increase by 3x, 4x, 5x, and Nx. If the number of logs in the institutions increase, a machine is rapidly added to expand the infrastructure, and the machine that was deactivated within the cluster infrastructure is automatically reactivated. The performance of the service processes among the machines in the cluster infrastructure may be discursively handled by increased service and load distribution.

When there is a service problem with one machine in the cluster infrastructure, the same service continues to automatically work on the other machine. The service uses self-optimization to enable enhancement and performance optimization as it continues to work on this machine in case the problematic machine is activated.

High Availability

Logsign’s cluster infrastructure allows the received data clones to be placed on more than one server. If one or more servers are damaged (depending on the number of servers that are simultaneously actively-actively working), the remaining servers and the system continue to function productively without losing any data. Logsign SIEM enables high usability with its automatic failover, load balancing, service discovery, terabyte live data capacity, as well as redundancy at any level and both online and offline storage and clustering.



Improved Layered Data and Service Redundancy Infrastructure

The multi-layer data and service redundancy capacity of Logsign provides a number of benefits. It allows you to store and backup live and offline data at the petabyte level and enables redundancy at every layer, storing your data centrally or dispersedly. In possible worst-case scenarios, it also protects your data safely and always makes them accessible with its features of automatic activation, service increase and failover, and self-recovery. These advantages provide you with flexibility, instant mobility, and opportunity to take actions.

Fault Tolerance

Logsign cluster’s fault tolerance ability allows the same data from another Data Node to be used when any Data Nodes are broken down. The cluster forms two or more working Name Nodes (active and passive) within the hot standby configuration.

If an active node fails, the passive node takes the responsibility of the active node. Therefore, the files are usable and accessible by the users even if the Name Node is down.

Cost-Effective

As the Logsign cluster is composed of flexible hardware nodes, it enables a cost-effective solution for storing and processing big data. Additionally, it does not create additional licensing costs since the open-source Hadoop is used for infrastructure.

Data Location

Hadoop's data location feature is important for the network structure. Logsign SIEM unicast has a conveyance structure and calculates the data on the traffic, which reduces bandwidth use.

More Rapid Data Processing

Hadoop stores data dispersedly, which allows the data to be processed quickly on a nod cluster.

Data Reliability

As the data in the cluster is increased in Hadoop, it is stored safely in cluster machines despite the machine errors. If a node or data included in the cluster is broken down, your data is protected and accessible from the other machine that includes a copy of the data.

Flexible Working Data Analysis Infrastructure

Contrary to the traditional system, Logsign SIEM processes unconfigured data. This enables feasibility for the users in analyzing data in any format and size.

Improved SOC Support and Big Data Management Model

With its big log data, Logsign SIEM enables admin and analyst users, who are dispersedly positioned, to work at their best performance levels with more users and more data. Within the framework of the Cyber Security Operations Center (SOC), it allows the access performances of the managerial roles to reach the highest level. During its first set-up stage, Logsign SIEM may allow various servers to be assigned to various roles, and dozens of server clusters with similar server roles may be created. Thanks to the Multicore and Multimachine features, more than one service and machine redundancy are enabled.

Logsign manages live and offline log data redundancy processes that are connected to the SOC network infrastructures with especially defined critical tasks, at any size and shape, and additional users and sources. It prevents the problems occurring from the addition and use of high-volume data structures, and meets the necessary extension requirements for growth by improving storage abilities.

About Us

Logsign was established in 2010 to enable cyber security practitioners to work more efficiently with smart, clutter-free and next-generation softwares. Securing the IT systems and managing cyber security operations should not be so complex, time consuming and over-priced. This is why we developed our smart and simple-to-use SIEM and SOAR softwares considering the market's current and future needs. Automation starts the new era in cybersecurity. We believe with this era, automation handles the manual workload of humans upto 98%. Thus, efficiency in cybersecurity operations is not a dream anymore. SOAR software is in the heart of operations enhancing security teams work in a smart, collaborative and effective environment. You can't protect before you see and detect. Collecting any data, visualizing and turning into actionable intelligence are possible via our infinitely scalable and cluster SIEM. With 10 years of experience, Logsign is a sincere team player for all internal & external parties, trusted by more than 500 enterprises, ministries and state agencies.

www.logsign.com

support.logsign.net

0 850 660 0 850