Juniper Secure Analytics Data Node

Product Overview

Juniper Secure Analytics Data Node, a member of the JSA Series Secure Analytics family of products, helps organizations increase their storage capacity and processing performance in a manner that is designed to be cost-effective, scalable, and flexible. Data Node allows users to scale their Juniper Secure Analytics deployments to store up to petabytes worth of information, improve query and search performance, and distribute data to optimize resource utilization.

Product Description

Today's attackers have become increasingly sophisticated and hide inside networks longer than in the past. As a result, analyzing historical data to determine normal, baseline behavior is critical in order to detect anomalies that could be signs of a breach. Security teams now need to conduct searches that go back months or even years, which means storing potentially hundreds of terabytes or even petabytes of information, a very expensive proposition. Fortunately, now organizations deploying Juniper Networks® JSA Series Secure Analytics Appliances have an option for increasing their storage capacity and processing performance that is designed to be cost-effective, scalable, and flexible—the Juniper Secure Analytics Data Node .

In JSA Series Secure Analytics portfolio deployments, data storage and searching is performed by an all-in-one appliance, event processors, flow processors, or event/flow processors. As more data is accumulated, additional storage capacity and processing power for queries often become needed, which normally requires the addition of more event and flow processors. Now there is a cost-effective alternative—the Juniper Secure Analytics Data Node. Data Nodes are highly scalable and can be attached directly to all-in-one JSA Series Secure Analytics Appliances, event processors, flow processors, or event/flow processors to add storage capacity and processing resources. And there is almost no limit to the number of Juniper Secure Analytics Data Nodes that can be added, making it possible to store and search up to petabytes of historical log, event, and flow data.

In addition to being scalable, Juniper Secure Analytics Data Nodes are also very flexible. They contain algorithms that automatically balance data among the Data Nodes when a new one is added, in a manner that helps optimize search performance and storage.

Data Nodes support high availability and clustering, and can be purchased in a hardware, software, or virtual format. Juniper Secure Analytics Data Nodes are also designed to be added on demand, without changes to system configurations, correlation rules, integrations, or user interfaces. In fact, they are plug-and-play, and can be added to an installation at any time. After the initial setup, Data Nodes seamlessly integrate with an existing deployment.

Architecture and Key Components

Juniper Secure Analytics Data Nodes are designed to deliver:

- Greater scalability and search performance
- On demand expansion without significant system configuration or deployment changes
- Data distribution designed for optimum resource utilization
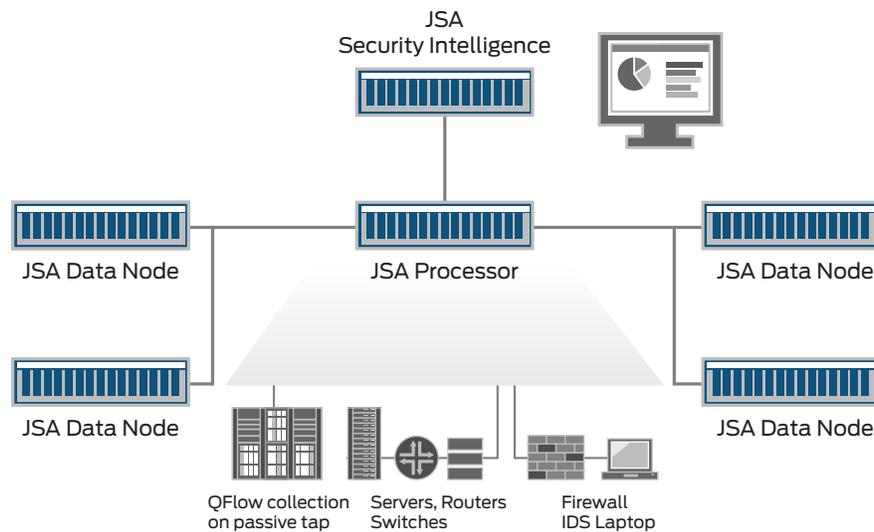
Your ideas. Connected.™

Figure 1. JSA Series Secure Analytics Appliances security intelligence architecture

Greater Scalability and Search Performance

Juniper Secure Analytics Data Nodes can be added directly to all-in-one JSA Series Secure Analytics Appliances, event processors, flow processors, and event/flow processors to add both lower cost storage and search processing capacity instead of adding event/flow processors. They receive and store events and flows, and can actively participate in query operations, providing additional processing power and increased search performance. Data Nodes also deliver real-time data interpretation, event correlation, and alerts. They are 100 percent dedicated to storage and search workloads, and are designed to transfer data at potentially millions of events per second without impacting normal operations.

Juniper Secure Analytics Data Nodes can be clustered around an event or flow processor, providing access to the space and processing capacity of each Data Node instance. Users are now capable of creating data storage deployments of potentially hundreds of terabytes to petabytes of data, while simultaneously adding the processing capacity to handle the queries on that data. Once in place, data distribution algorithms disperse all incoming data among the Data Node instances in a manner designed to be optimal for both query and storage.

Juniper Secure Analytics Data Nodes also provide flexibility, allowing storage to be added independent of requirements for events per second, or flows per minute, as is the case when adding event or flow processors. This can result in an overall system that has the appropriate storage capacity to meet the demands of day-to-day operations. It also allows more data to be maintained in an uncompressed and readily searchable form, which helps reduce search times and improves performance. Data Nodes add more I/O, CPU, and memory resources that can

be used by the query infrastructure when executing a search, and these resources do not have competing demands placed on them as is the case with event and flow processors.

On-Demand Expansion

With Juniper Secure Analytics Data Nodes, addition to a JSA Series Secure Analytics Appliances deployment is simple and straightforward. It does not require any reconfiguration or changes to log sources, correlation rules, reports and integrations, or the user interface. And Data Nodes can keep being added as more capacity is required. Juniper Secure Analytics Data Nodes are offered as hardware, software, and virtual appliances.

Data Distribution Designed for Optimized Resource Utilization

Juniper Secure Analytics Data Nodes contain algorithms that take data from JSA Series Secure Analytics Appliances, event processors, and flow processors, and distribute it across the Data Nodes in a manner that helps optimize search performance and storage utilization. This is done using a scattering algorithm that distributes data based on the amount of available space and the disk space utilization rates of the cluster members. As new Data Nodes are added, data is automatically distributed to them. If a Data Node is removed or taken offline, the cluster will resume write operations to it when it is returned to the network.

High availability (HA) is also available for Juniper Secure Analytics Data Nodes, where each node is paired with a second node for failover in order to provide coverage for the data stored in the cluster. Data retention policies are applied to Data Nodes in the same way as they are applied to an event processor, flow processor, or event/flow processor. These policies are evaluated on a node-by-node basis and criteria such as free space will be based on the individual node and not on the cluster as a whole.

Features and Benefits

- Scale deployments of JSA Series Secure Analytics Appliances to store up to petabytes of information

- Improve query and search performance

- Distribute data to help optimize resource utilization

Juniper Networks Services and Support

Juniper Networks is the leader in performance-enabling services that are designed to accelerate, extend, and optimize your high-performance network. Our services allow you to maximize operational efficiency while reducing costs and minimizing risk, achieving a faster time to value for your network. Juniper Networks ensures operational excellence by optimizing the network to maintain required levels of performance, reliability, and availability. For more details, please visit www.juniper.net/us/en/products-services.

Ordering Information

To learn more about how JSA Series Secure Analytics Appliances and Juniper Secure Analytics Data Nodes can benefit your organization, please contact your Juniper Networks representative and visit www.juniper.net.

About Juniper Networks

Juniper Networks is in the business of network innovation. From devices to data centers, from consumers to cloud providers, Juniper Networks delivers the software, silicon and systems that transform the experience and economics of networking. The company serves customers and partners worldwide. Additional information can be found at www.juniper.net.

Corporate and Sales Headquarters

Juniper Networks, Inc.

1133 Innovation Way

Sunnyvale, CA 94089 USA

Phone: 888.JUNIPER (888.586.4737)

or +1.408.745.2000

Fax: +1.408.745.2100

www.juniper.net

APAC and EMEA Headquarters

Juniper Networks International B.V.

Boeing Avenue 240

1119 PZ Schiphol-Rijk

Amsterdam, The Netherlands

Phone: +31.0.207.125.700

Fax: +31.0.207.125.701

1000542-001-EN   May 2016