ServiceNow Log Export Service

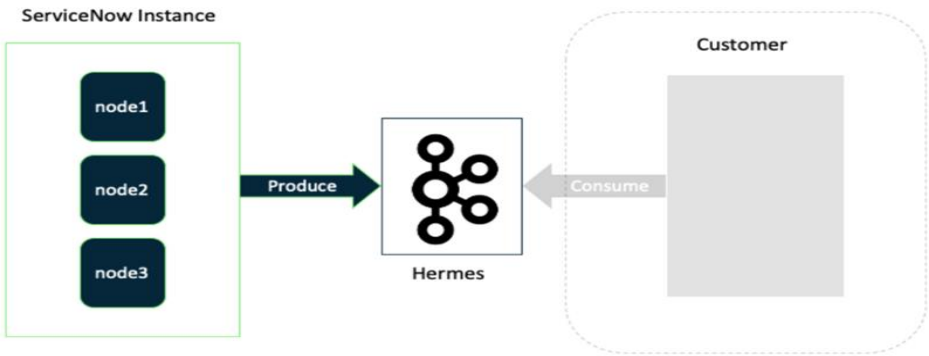
The business challenge

Organizations face increasing challenges in monitoring the performance of their digital platforms and the security of their sensitive data within them. Organizations have a myriad of systems, applications and cloud services deployed that generate large amount of log data (petabytes). These large amounts of log data are collected, aggregated, and analyzed using enterprise-wide log and security analytics solutions to avoid service disruptions and protect the infrastructure from potentially costly data breaches or cyberattacks. Security analytics solutions provide rapid threat detection and response, real-time risk assessments and security posture management by looking for anomalies and correlations within the large data sets collected from multiple sources. This provides organizations a comprehensive view of their environment with in-depth insights about the state of their risk as well as real-time actionable insights. Organizations can also use log analytics to monitor system performance and perform IT troubleshooting across their enterprise.

Gathering logs from individual sources can be a very laborious process. The process requires resources with expert scripting skills, additional dedicated infrastructure to support the collection, processing and storage of the data along with regular ongoing maintenance. Without the log data, organizations can find themselves with a weaker security posture. They cannot proactively identify threats; they cannot ensure consistent performance monitoring and ultimately, they can fall short on their regulatory compliance with government and industry mandates leading to negative brand reputation and possibly paying fines and penalties.

The ServiceNow Solution

ServiceNow Log Export Service is a turn-key service that organizations can subscribe to either as a standalone offering or as part of the ServiceNow Vault product. Log Export Service enables organizations to easily integrate their ServiceNow system and applications logs into their enterprise security analytics solution with minimal effort and complete control.



ServiceNow Log Export Service

Benefits

Highly scalable and near real-time native integration with Kafka-based analytics systems using Kafka connector.
Sidebar Content

Easy setup with no additional coding needed

Control cost and improve efficiency by exporting only the data needed for your ServiceNow instances

Increase threat detection, improve user experience and compliance monitoring and simplify IT troubleshooting.

As shown in the diagram above, Now Platform system administrators can selectively configure and forward their system and applications logs for their ServiceNow instances to Hermes Messaging Service and then pull those logs into their enterprise-wide log and security analytics.

Customers can use Kafka-connectors to integrate and export their ServiceNow system logs into their Kafka-based enterprise security analytics platform. This Kafka connector solution provides organizations the speed, reliability, and scalability to address the real-time analysis of large volumes of log data from the Now Platform to provide efficient end-to-end visibility and correlation of security anomalies and IT performance related issues.

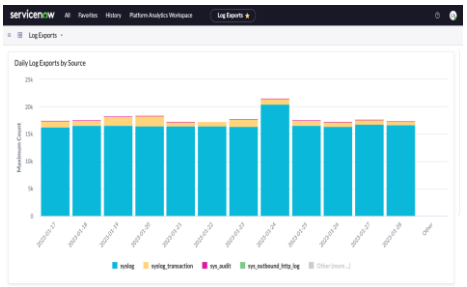
To regulate the logs that need to be forwarded, users can use the Log Export Service to create a configuration to identify the specific logs. Once the logs are forwarded, they can be consumed from Hermes to the required destination.

Real-time and highly scalable architecture

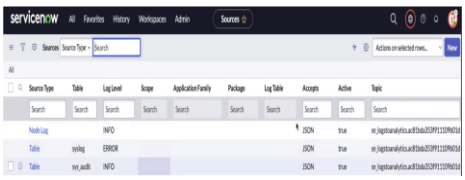
Log Export Service is built upon an Apache Kafka platform. Kafka is an open source, distributed and real-time data streaming technology capable of handling trillions of events per day. Examples include continuous analyzing of log files generated by systems and applications, monitoring, and responding to customer behaviors and responding to telemetry and performance-related data.

ServiceNow Log Export Service comes as part of the ServiceNow Vault product or can be ordered separately. The product comes for free for the first 500 GB. If customers need more capacity, they can order additional bandwidth in 1000 GB increments for an additional charge.

By integrating their ServiceNow logs into their enterprise security analytics tools, organizations can improve their security, minimize workflow interruptions and performance issues, and resolve incidents quickly and effectively for their ServiceNow deployments. To learn more about ServiceNow Log Export Service please visit: **www.servicenow.com/products/vault.html**



Daily Log Exports Summary



Active Systems Logs

servicenow

© 2022 ServiceNow, Inc. All rights reserved. ServiceNow, the ServiceNow logo, Now, Now Platform, and other ServiceNow marks are trademarks and/or registered trademarks of ServiceNow, Inc. in the United States and/or other countries. Other company names, product names, and logos may be trademarks of the respective companies with which they are associated.
SN-DataSheet-Name-01012022