TECHNICAL WHITE PAPER: High Availability for Log Collection in RSA Netwitness®

JULY 2020

ProtectedIT

Elevating & Unifying Security Technologies

High Availability for Log Collection in RSA Netwitness®

July 2020

A White Paper exclusively produced and presented by the ProtectedIT Engineering Department

Modern IT operations can be compared to a well-planned robust factory working and serving us nonstop 24x7x365. These entities, that we have come to highly depend on for keeping our lives going, are constantly under attack and are struggling hard to fend off a throng of cyber attackers who are trying to compromise the holy trinity of cybersecurity which are:

Confidentiality – protecting information from being accessed by unauthorized parties.

Integrity – maintaining and assuring the accuracy and completeness of data over its entire lifecycle.

Availability – refers to authorized users that can freely access the systems, networks, and data needed to perform their daily tasks

Although all three of the above listed aspects are equally important, we will keep our focus only on **availability** for this article.

Need for High Availability in a SIEM solution

A SIEM application provides an extremely high level of detailed view to the SOC team members and allows them to understand exactly what is going on in a clients' environment be it on a Server or any network component like Switch, Firewall, Proxy etc. A SIEM application accordingly is required to provide high level of availability to its respective stakeholders or end users.

What type of downtime can your SIEM application be subjected to?

Based on the functionality, a SIEM system can have two types of downtime –

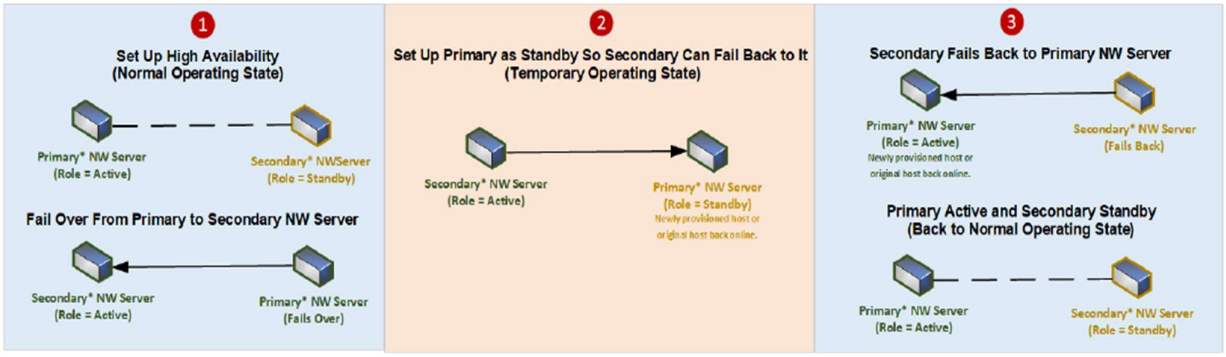
- Monitoring Downtime
- Log Collection Downtime

While both the above listed downtimes are equally catastrophic and should not be acceptable to the stakeholders involved, the latter causes a far more dreadful impact on clients environment as losing event source logs causes a delay in Log Collection (when Log Collection is restored) or worse a Log loss situation which can severely hamper abilities of teams to paint a detailed picture of the network in case of a breach.

How has RSA® addressed this in their Netwitness platform?

Monitoring Downtime

RSA® has addressed the monitoring downtime aspect from Netwitness 11.3 onwards by introducing a Warm Standby Netwitness Server host. The Warm Standby Netwitness Server duplicates the critical components and configurations of the Active Netwitness Server Host to increase reliability. A secondary Netwitness Server remains in the standby role and when configured, receives backups of the primary Netwitness Server in the active role at regular intervals. If the primary Netwitness Server fails (goes offline), the fail-over procedure must be executed allowing the secondary Netwitness Server to assume the active role.



Log Collection Method Types

By default, the log collection methods available in RSA Netwitness® can be classified into Push or Pull Method

- Push – Syslog and File
- Pull – Checkpoint, Netflow, ODBC, plugins, SDEE, SNMP, Windows (using WinRM), VMWare

Impact of Downtime on Log Collection Methods

Pull Method

Log collection relying on the Pull Method can survive the downtime (caused due to a fault in log collection) as it can pick up the collection from the last collected point. This can cause some significant delay in monitoring, reporting and alerting but will not result in any log loss.

Push Method

Push Method (particularly syslog) is very susceptible to such an event since many critical devices in the network like firewalls, switches, routers, proxy etc. send logs using the syslog method. As per the current design, RSA Netwitness® provides a failover model for forwarding the logs once collected using a Virtual Log Collector as per the below diagram

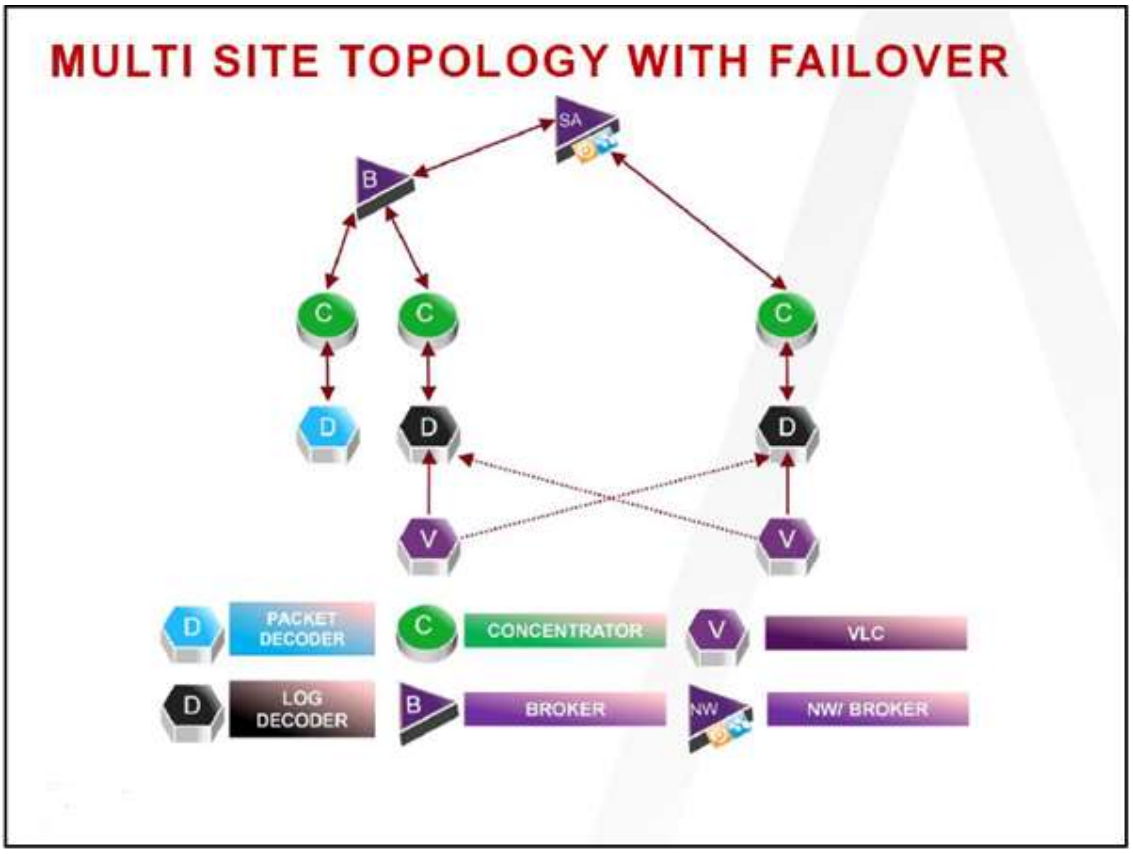


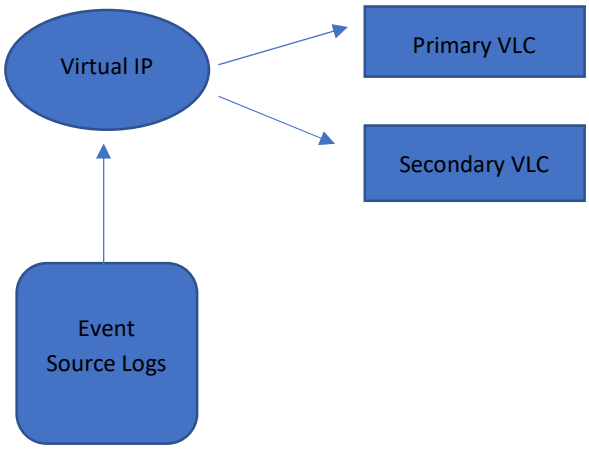
Image Source: RSA®

But this design does not address the High Availability on Log Collection layer for both Virtual Log Collectors and Local log Collectors.

The solution

The solution is simple and can be achieved using Linux concepts as we know the base OS for RSA Netwitness® is CentOS 7. The HA can be achieved on log collection layer for syslog collection and file collection using Virtual IP, Corosync and Pacemaker.

In this scenario Push Method logs will send Logs to a Virtual IP instead of VLC'S actual IP – this is pictorially represented below



Recommendation - It is good to integrate all your syslog collection on RLC at the very start of the implementation so that the HA will be effective from the initial stages itself.

Readers are urged to reach out to ProtectedIT in case they need further and detailed information. Please contact sales@protectedit.net