Hadoop Platform Centralized Logging System

Date: [Publish Date]

Revision: 0.1

Revision History

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Date | Version | Status | Prepared by | Comments |
| 12-06-2016 | 0.1 | Draft | Prashant Bhalesain | Initial Draft |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |
|  |  |  |  |  |

Table of Contents

[1 Document Purpose 4](#_Toc458172939)

[2 Business Requirements 5](#_Toc458172940)

[3 Approach 6](#_Toc458172941)

[4 Data Repository 8](#_Toc458172942)

[5 Roll Out Approach 11](#_Toc458172943)

[6 Expected outcome 12](#_Toc458172944)

[7 Key Performance Index for Hadoop Monitoring 13](#_Toc458172945)

[8 Planned Deliverables 14](#_Toc458172946)

# Document Purpose

Currently HSBC has ten Hadoop Clusters that host production data. Recently an independent assessment exercise was carried to identify risks associated with the ‘Data Lakes’ mainly to avoid any data leakage or system compromise.

The assessment exercise identified few issues and recommended best practices to avoid them.

Following were the recommendations made:

The following recommendations address the deficiency of controls:

1. As a matter of urgency the detective controls such as Daily Logs reviews, alerting and auditing must be developed, documented and deployed. These must be in place, tested and proven to be effective.
2. The separation of the management of the Encryption Keys, Operating Systems, and Hadoop must be maintained.
   1. Separation of duties between the various and different Privileged Accounts must be maintained. Combining these roles could give someone the ability to gain unauthorised access to data.
   2. The number of staff with Root or Privileged access must be strictly controlled
3. A preventative control that will stop privileged accounts from having unauthorised access to data must be incorporated into the design, tested and deployed. The risk of unauthorised access to data and the potential for subsequent data leakage remains without this control.

This document proposes a plan to implement these recommendation, if there are cases where it is not possible to put together a solution, this plan identifies reasons for them, risk associated with it and mitigation plan.

# Business Requirements

In order to achieve above mentioned goals, we analysed our current systems and data architecture. We currently collect multiple types of logs in various systems. Those logs remain in silos and serve specific purposes to create a view of actions performed in distributed systems. A need was identified to collect these logs centrally so that a single usage view could be built to identify pattern of usage and find anomalies if and when they occur. Systems that were identified to be useful are as followed.

1. Rsyslog
2. Ranger Logs
3. PAR logs
4. Direct logs (Centrify)
5. AD
6. GSD Logs
7. Data Clinic

The system envisioned for the described purpose would be able to acquire data from various sources, ingest it to a centralized repository. The file and data types used by these systems should be processed with minimum efforts required to transform and manage the data. Once the data is in central repository tools need to be put together to enrich the data with other external data sources. Initially, a single view needs to be built using visualization technologies to actively view and act, should there be any anomalies identified. The system should also alert when such anomalies occur.

To cater the immediate needs, the solution could be put together in two phases.

1. Tactical solution:

In this phase a central repository would be built with available resources and tools so the data can manually be pulled into it and processed. The data could be periodically collected from the servers and brought central repository using tools such as sftp. The anomaly detection could be done manually using simple data aggregation methods.

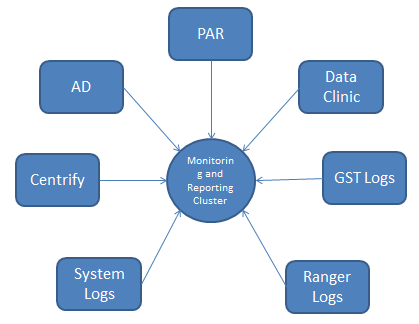
1. Longer Term Solution:

A long term solution would be a system where data could be pulled from multiple clusters automatically using real time data processing techniques. It would also use more intelligent algorithm to detect anomalies and generate alerts.

# Approach

In order to achieve above mentioned goals we plan to build a single log repository, where logs, initially only access logs, from all the systems would be brought to. This would facilitate HSBC to put together appropriate tooling, make use of the logs in understanding the intention behind the actions performed and whether those actions pose any risks. It would give an insight into the usage of the cluster and detect possible breaches/compromise to the systems. This will also provide a single view of the authentication usage and associated incident reports with it.

We identified following main systems that could provide necessary information that could be analysed and used for the purpose.



The systems are :

1. Centrify – outside firewall
2. Syslog
3. Ranger Logs
4. PAR Release Logs
5. AD
6. GST logs
7. Data Clinic

Once the data is collected from these system to a log analysis mechanism and graph will be built to link the activities user preformed on various clusters, the datasets s/he on which actions were performed, whether appropriate authentication was used to perform such action and there is valid reason provided/documented in our records.

.

**Centrify:**

Centrify is an identity management tool which is planned to use to provide Secure Remote Access, Shared Password Management and Single sign on.

**Syslog**:

Previously we had a system call envision which is no longer in use and we do not have any licenses. We have rsyslog installed on every machine which is collecting the data which can be used to collect system logs for Audit purposes.

**Ranger**:

Ranger is a framework to enable, monitor and manage comprehensive data security across the Hadoop platform. Since this is part of HDP platform, every cluster is enabled with ranger.

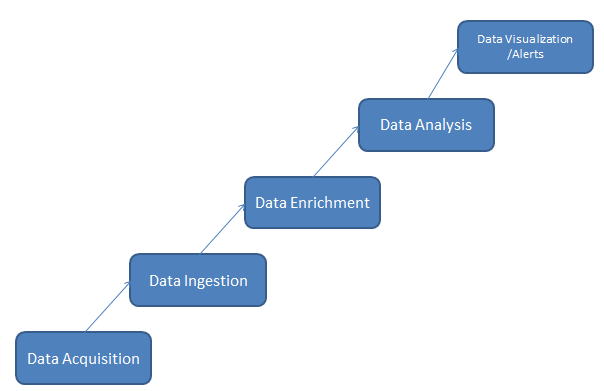
**PAR:**

The Password Auto-Repository (PAR) provides secure control of administrative accounts. The PAR is a repository where these account passwords are stored until needed, and released only to authorized persons

# Data Repository

In order to collect data from multiple clusters and other data sources a small cluster of Search engine technology will be built either using search engines such as Solr and Elastic Search. The log data will initially be brought in semi-automatically to this repository. More automation could be built using near real time logging mechanisms such as NiFi, Solr and Banana.

Following diagram depicts the data journey that will be used to process the data.



1. Data Acquisition

From the seven systems that were described above, clients will be installed/used to transfer the data to a central location either to the repository or a gateway.

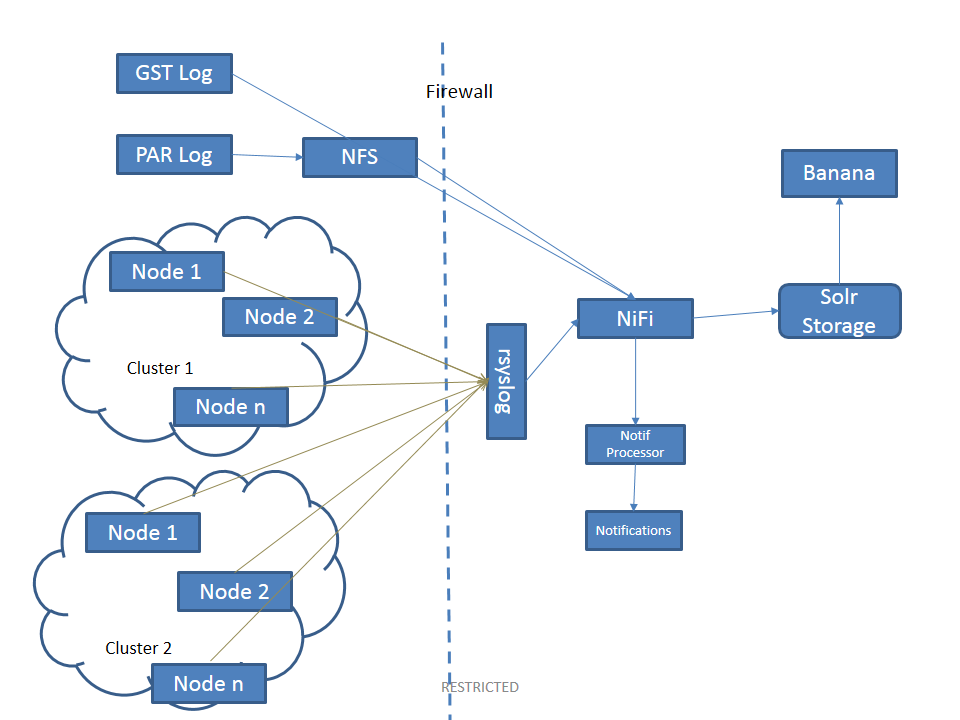
* 1. Ranger – a mysql client will be used to transfer data from each cluster to central repository
  2. Syslogs – rsyslog agents will transfer data to a central logs server which then will be pulled to central repository using NiFi rsyslog processor in order to ingest into solr.
  3. PAR – PAR release logs are currently dumped on daily basic to a shared file system. These logs will be transferred using sftp to the central repository

1. . Data Ingestion
   1. NiFi could be used as data ingestion and data flow definition tool to connect with various data sources and process the collected data through the system.
   2. Further we could add few more data sources in order to enhance the datasets, The system should be capable enough to add when needed
2. Data Enrichment
   1. Currently only seven identified logs will be used to data aggregation, if needed other sources could be added to the repository to be used for data aggregation.
3. Data Analysis
   1. The data will normalized to identify pattern or co-relation. Queries need to be built to connect various data sources on a timeline to visualise it such that an event could be tracked to various data sources.
   2. We need anomaly detection mechanism to put in place in order to automatically detect data discrepancies and events linked to data insecurity
4. Data Visualisation/Alerts
   1. Tools like banana will be used to present the data timeline for each cluster. These visualizations should be able to present the events, their severity which can further the drilled down to understand actions performed during the time frame captured by other logs.
   2. For every cluster we should be able to trigger alerts, visualize the data on timeline, drill down the event to see all the data sources associated with the event and any potential reason for breach.
   3. Separate Dashboard should be provided for every cluster that is being monitored.
   4. The possible threat alerts should be emailed to appropriate people.
   5. The data should be provided as possible in graphical manner in order to answer questions such as who, when, what, how and why.

Considerations for System Design:

1. The initial deployment of the monitoring system will be in batch mode considering some of the resources are difficult to gather real time. The system should be able to capture, store, analyse any type of security data in an efficient manner.
2. The longer term deployment should provide batch as well as real time data processing. The data should be enriched and processed faster providing threat intelligence.

Following diagram depicts the system under consideration.



# Roll Out Approach

There are currently 12 production/pre-prod cluster which may hold production data that need to be monitored.

The solution will be implemented in a phased manner starting with pre-prod clusters.

Phase I - Pre-Prod

1. HDP55 – FIPL UAT
2. HDP58 – Pre-Prod1
3. HDP 59 – Pre-Prod2

Phase II – Discovery

1. HDP06 - Discovery
2. HDP10 - RBWM / SAS Grid
3. HDP12 – RBWM Discovery

Phase III – Production

1. HDP01 – GBM/CMB/Payments Live
2. HDP02 – Staging
3. HDP03 – FIPL Live
4. HDP04 – Finance/Risk Live
5. HDP05 – RBWM Live
6. HDP07 – Compliance Live
7. HDP08 – RBWM/ SAS Grid
8. HDP13 – Finance/Risk Live

Phase IV - Contingency

1. HDP09 – Staging DR (HDP02)
2. HDPXX – Staging DR

In order to implement the centralized monitoring solution it would first developed in Test Lab. Once this solution is tested and approved it would then be implemented in production systems.

1. Currently all the nodes in the clusters use rsyslog daemon to send data to a centralized cluster not owned by GBDS group. For the centralized monitoring solution, rsyslog configuration needs to be changed on all the nodes to send data to centralized logging system owned by GBDS.
2. Ranger scripts would have to be put in cron in order to send the data to the centralized monitoring system.
3. For other external systems, a system user would be created which would need to be put in appropriate groups to get access to identified systems.

# Expected outcome

1. Continuous tracking of access to the systems
   1. User logins
   2. HDFS accessed
   3. Detect access anomalies for the users
   4. Alert access anomalies
2. User access and anomalies co-relation with external systems
3. Ability to co-relate the reasoning behind the user access and usage anomalies.
4. Ability to detect unauthorized data access (Data that is out of user’s access level) with all possible reasoning and knowing the unknowns.

# Key Performance Indexes

1. Number of users accessing each cluster with internal and external classification.
2. Number of unrelated user actions detected.
3. Number of deliberate actions detected.
4. Number of unknown access locations detected.
5. Number of unrelated file locations detected.
6. Names of unrelated clusters accessed.
7. Number of external users detected.
8. Frequent commands used by the user, number of users using them
9. Frequent user actions identified.
10. Frequent user location identified
11. Frequent file locations accessed
12. Number of anomalies in user, actions, location, file system accessed.
13. Time taken to detect unrelated action performed
14. Time taken to communicate unrelated activity to stakeholders.
15. Time taken to co-relate user action to intent.

# Planned Deliverables

Phase I

Reports -

Weekly reports

1. Number of users accessing each cluster with internal and external classification.
2. Number of unrelated user actions detected with categorization inadvertent, deliberate, inaction.
3. Number of deliberate actions detected.
4. Number of unknown access locations detected.
5. Number of unrelated file locations detected with categorization inadvertent, deliberate, inaction.
6. Frequent commands used by the user, number of users using them
7. Most frequent user actions
8. Most frequent user location identified
9. Most frequent file locations accessed

PHASE II

Reports -

1. Names of unrelated clusters accessed with categorization inadvertent, deliberate, inaction
2. Number of external users detected.

Live Dashboard

Highlight anomalies

PHASE III

1. Automatic anomaly detection
2. Near real time alerts sent to stockholders.
3. Real time dashboard for the phase I reports

Action Categorization

|  |  |  |
| --- | --- | --- |
| Inadvertent | Deliberate | Inaction |
| Mistakes | Fraud | Skills |
| Errors | Sabotage | Knowledge |
| Omissions | Theft | Guidance |
|  | Vandalism | Availability |

Actor Classification:

Internal External