ACCOUNT LOCKOUT MANAGEMENT WITH BMC TRUESIGHT IT DATA ANALYTICS

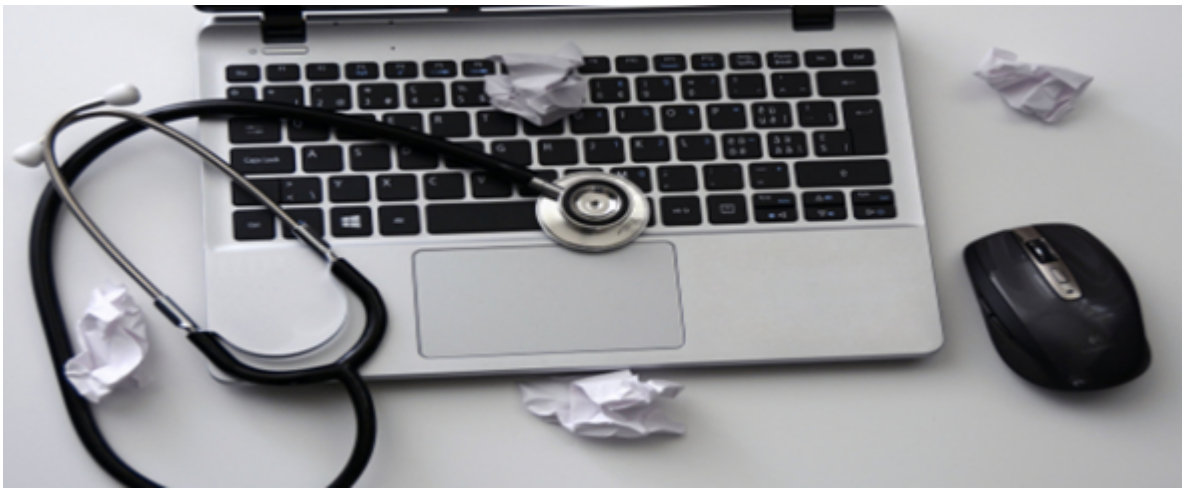
Enterprises globally are investing meticulously in data integrity and security tools from business and regulation perspective. The importance of these tools has gained more advantage after the recent movement of government vigilance regarding information and communication flow in most of the countries. Implementing strong password policies is therefore imperative and at the same time critical for business. However, strong password policies at times act like a double-edged sword bringing in a huge inflow of account lockout incidents for the IT Service Desk.

Addressing account lockout Issues for any IT service desk is a cumbersome task given the number of such tickets toping the incidents logs every day along with never ending calls to the desk for password resets. Scenarios like these resonate with the majority of IT Service Desks across the enterprises. The amount being spent on administrative staff to handle account lockout issues too is not a nominal cost that the organizations have been incurring for the longest time. Seemingly for service desks, there is no way out of this.

A countless number of account lockout issues not only impacts the efficiency of service desks, but spreads over various facets involving productivity loss, frustrated users, and huge administrative burden. However, automation can truly redefine the resolution process of account lockout scenarios

while offering an enhanced user experience to both the service desks and the users.

This white paper highlights, how automation of account lockout resolution can save hours of productivity for the users and the service desk teams at smaller and larger organizations. BMC IT has effectively saved productivity time of its service desk by using BMC TrueSight IT Data Analytics. The number of hours invested in resolving such cases was brought down drastically from an average of 3-4 hours each ticket to a mere 10 minutes.



Current Scenario

Account lockout is a process of automatically disabling a user account based on specified criteria like too many failed login attempts. Failed login situations could arise due to various reasons, for example, a user returning from a long holiday and after somehow pushing himself back to work he tries to remember his password, he makes several guesses but ends up exceeding a given number of attempts. In another situation, the user can mistype password five times simply because he has not had his coffee yet. This makes account locked out and typically follows with a phone call to the helpdesk. The entire process consumes crucial business resources in terms of the time spent by the service desk on resolving this issue as well as the loss of employee/user productivity. Similarly, password expiry poses another challenge as once a password is changed, it gets updated only in Active Directory and nowhere else. Thus, leaving a user locked out from his/her account.

Even the most efficient organizations spend a significant amount of time and cost on account lockout management. On average, IT departments spend almost one-third of their total productive time on the resolution of user lockouts and password issues. The time that IT staff spends on these problems is only the top of the iceberg, as soon as we consider the lost user productivity and service downtime, the impressions are likely to rise by manifold.

Typical Account Lockout Resolution Workflow Use Case

A general task flow, when a user gets locked out generally looks like as mentioned below:

- “Account Locked Out' error reflects on the user's screen, following which the user contacts the service desk.
- The service desk engineer verifies the user and unlocks the account.
- If the problem persists, the user calls service desk once again and asks for further investigation.
- Service desk engineer performs a routine lookup of possible sources of account references.
- After checking all account references, service desk engineer unlocks the account.

- If the problem persists anyway, the service desk engineer would reach to DC Admin to perform the further investigation. It is difficult for even a Level 3 engineer to search all DC servers, number of log files, and events to identify the source details of the lockout for a specific user.

BMC IT Introduced the Change

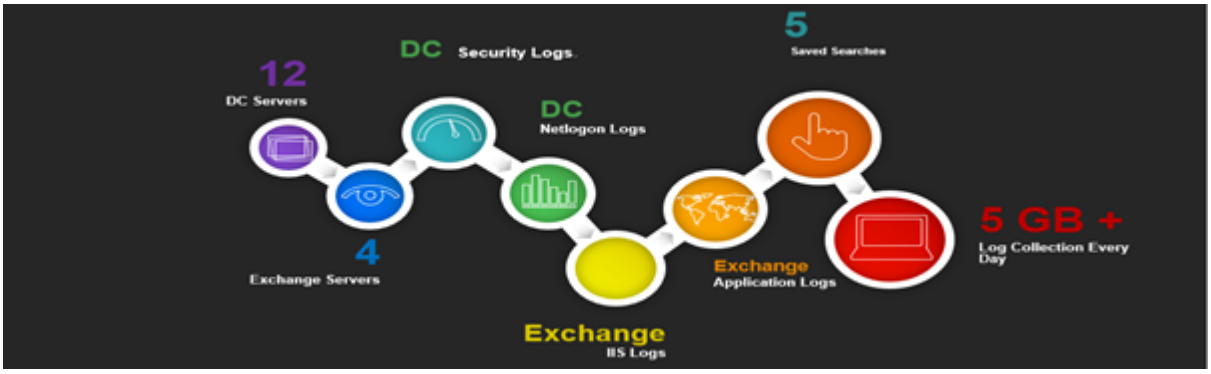
BMC IT Service Desk receives more than 1,000 incidents monthly for account lockout issues. Service Desk's best approach was to try and test multiple resolutions to identify possible cause, Resolution times ranged from 3-4 hours. The productivity impact was 3,000-4,000 hours per month. Part of the challenge was that there were so many different services and infrastructure involved that the support analysts could not get a clear root cause to address the failing logins.

IT initiated an effort to address this issue using BMC TrueSight IT Data Analytics (ITDA). By integrating all relevant services, defining appropriate logging levels, and collecting all the data from the required sources to provide a comprehensive view of source devices and services. The team then prioritized triage based on the highest volume sources to draft knowledge that would quickly resolve the lockout depending on application and device.

The new visibility allowed the team to confidently identify root cause and resolve issues in 10 minutes vs. 3-4 hours.

ITDA is configured to collect the logs from 12 DC servers and 4 exchange servers and in total Collecting the logs from 32 Log files .

Now Service Desk is enabled to use a single query to run across multiple servers and log files to provide the result within a few minutes.



Using BMC TrueSight IT Data Analytics Solution

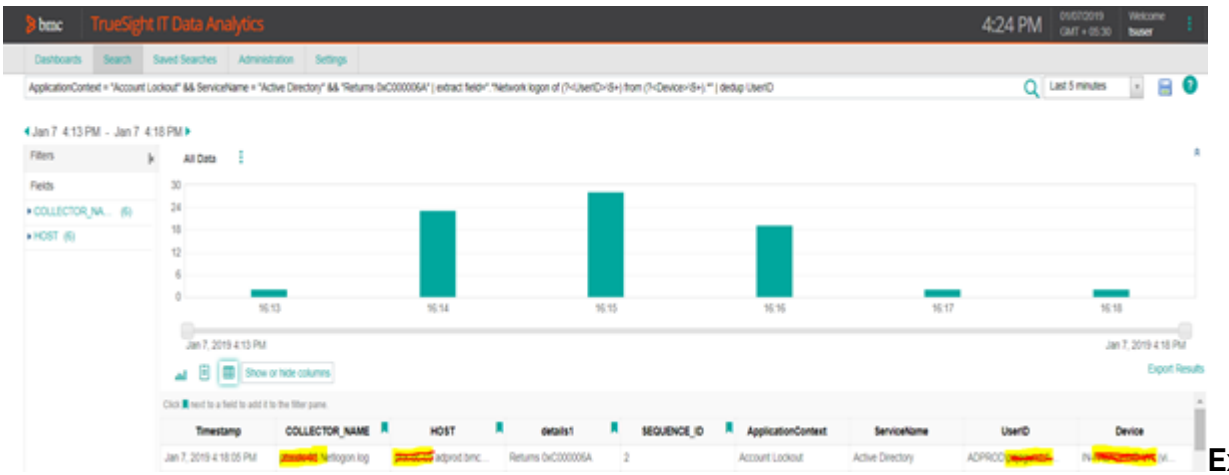
- A user receives 'Account Locked out' error and calls the service desk.
- SD Engineer Logs in to TrueSight ITDA to run the query.
- The engineer receives the result with source details causing the lockout.

This adoption has brought down the actual resolution time of the requests drastically to help in reducing the productivity loss for the end users. BMC IT in turn too has saved time and efforts of its L3 Team, which now can focus on other critical issues.

How TrueSight IT Data Analytics Configured

TrueSight IT Data Analytics is configured to collect the DC Netlog and Security Logs in real time.

- TrueSight ITDA is configured to collect the logs from 12 DC servers and 4 exchange servers
- The Log collection is enabled using BMC Patrol Agent running with ITDA KM
- All the collectors are Tagged with Service name “Active Directory “which makes ease of Search / Consolidation and with context “Account Lockout”
- All the Data collectors are configured with 30 Days retention period to help analyse historical logs
- The Search query on DC security Logs has been configured to check the event ID = 4740, which triggers the lockout event
- The Saved Search has been configured to extract the Field ‘Source Network Address’ causing lockout and user account name
- The Search Query for Netlog has been configured to check the error “Returns 0xC000006A” and field extraction for user account

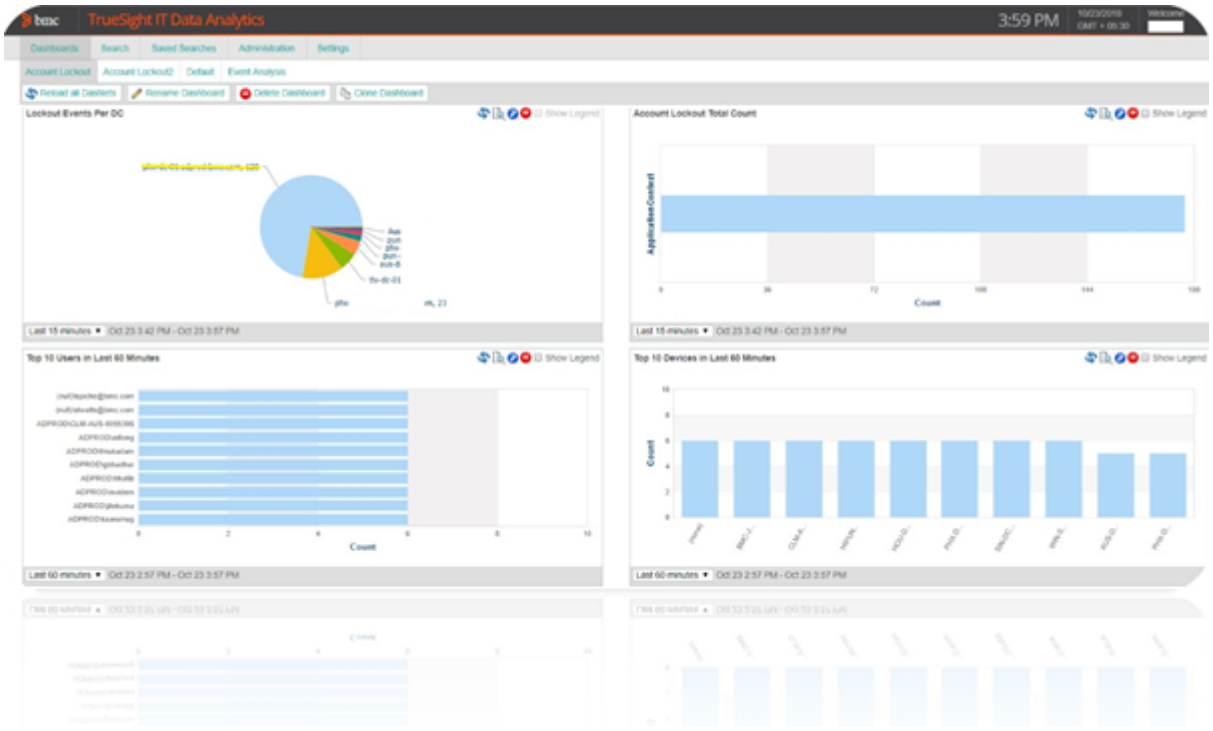


Examples-

Saved Search for DC Security Logs:

ApplicationContext = "Account Lockout" && ServiceName = "Active Directory" && "ID=4740" || "ID=4625 " | extract field=".?Source Network Address:+\s(?<SourceAddress>\S+).*"*

Saved Search for Netlog:
ApplicationContext = "Account Lockout" && ServiceName = "Active Directory" && "Returns 0xC000006A" | dedup UserID



Benefits

By using TrueSight IT Data Analytics BMC IT has augmented the performance of its Service Desk and the list of numerous benefits includes: -

- Reduces Turnaround Time for account lockout Incidents from several hours to just 10 Minutes
- Enhances User Experience
- Reduces number of L3 escalations
- Incident analysis based on historical data
- Enables quick analysis of Structured & Semi-Structured events/logs.
- This has saved average **3,000 hours/month** employee productivity

Conclusion

TrueSight IT Data Analytics is helping BMC IT to Consolidate and connect data from all tiers in a single pane of glass for enterprise-wide visibility while offering continuous and real-time collection of all relevant data. A lockout is effectively a global outage for an end user and the most impactful for them, BMC IT has made the transformation with TrueSight IT Data Analytics to support end users which Is resulting in to Significant improvement in business perception of IT.