

TECHNOLOGY BRIEF

CA User Activity Reporting Module | May 2011

CA User Activity Reporting Module: capabilities and architecture

agility
made possible™



table of contents

EXECUTIVE SUMMARY	3	Section 3: Benefits	10
Section 1: Challenge	4	Establish IT activity compliance	
Monitor insiders		Accelerate time-to-value	
Investigate security breaches		Lower total cost of ownership	
Lack of business relevance		Section 4: The CA Technologies advantage	12
Protecting local logs from privileged users		CA Services	
Section 2: Opportunity	7	Section 5: Conclusions	13
CA User Activity Reporting Module: overview		Section 6: References	14
Product architecture			
Key product features			

executive summary

Challenge

Compliance regulations and industry mandates like SOX, PCI, HIPAA and the EU Data Protection Directive require organizations to review IT user activity and archive it for several years for investigation. Logs prove what system and user activities are taking place on a system or a network device and can be used to identify policy violations and investigate security breaches. However, secure and reliable collection of logs at high volume across various sources—from physical, network and security devices to hosts, databases and applications—is a challenging task. In the absence of an effective user activity reporting solution, organizations are struggling to keep operational costs low while still trying to meet their compliance objectives efficiently.

Opportunity

Organizations need a cost effective user activity reporting solution that offers scalable and distributed architecture. CA User Activity Reporting Module provides enterprise-wide visibility of IT user activity allowing you to be IT activity-aware from a compliance and security perspective. CA User Activity Reporting Module not only can reduce operational costs by reducing inefficient, error prone procedures for log collection and compliance reporting, but can also simplify compliance auditing and forensic analysis. With out-of-box support for other Identity and Access Management (IAM) products from CA Technologies, agent-less log collection capability, and predefined compliance reports, CA User Activity Reporting Module is designed to complement any existing IAM product implementation and provide quick time to value.

Benefits

CA User Activity Reporting Module can solve user activity and compliance reporting challenges and enables organizations to establish compliance with requirements for monitoring IT activities by:

- Enriching queries and reports to show business relevance by grouping events by assets and user roles
- Discovering policy violations based on IT activities via actionable alerts
- Integrating with IAM solutions from CA Technologies along with many other commercial log generating products

- Reducing total cost of ownership by allowing quick deployment, delivering automatic subscription updates, compressing logs to minimize storage requirements and leveraging your existing hardware investments and maintenance contracts through the soft appliance model

Section 1: Challenge

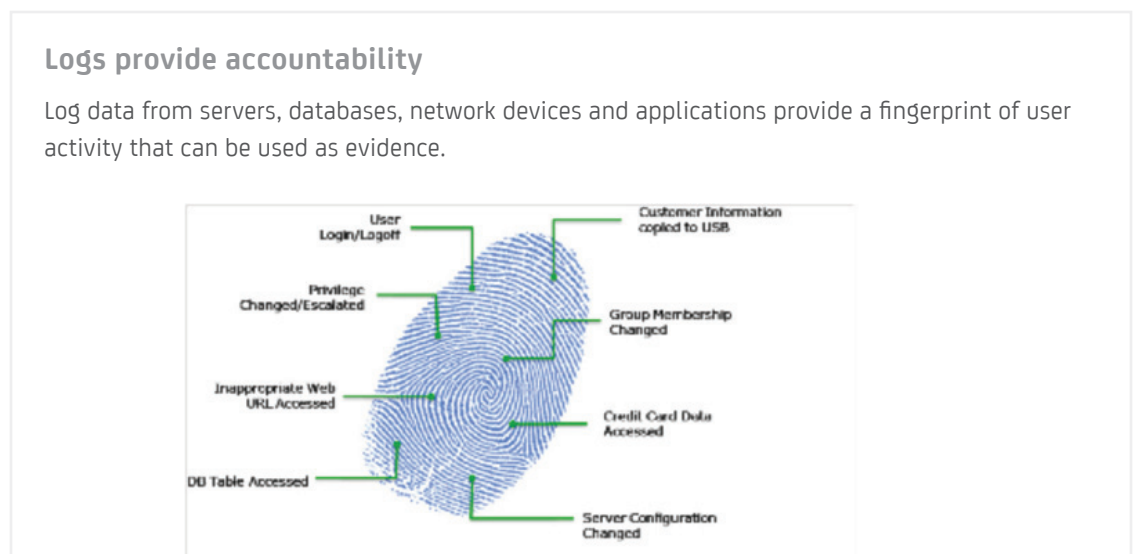
Why care about user activity reporting?

Over the last decade, IT has transformed the way business is done. More and more information is now residing on servers and databases increasing the risk of data loss and identity theft. At the same time, the focus on threat vectors has flipped completely from the outside to the inside. It is much easier for sophisticated thieves to recruit a greedy insider to leak sensitive data and to conduct fraud or IT sabotage. In such an environment, the conventional security measures of protecting the perimeter and putting in more access control in an increasingly complex IT environment are not enough. Both economics and IT complexity favor a surveillance model focused on monitoring of user and IT activity logs, instead of just defending the perimeter.

User activity logs prove what system and user activities are taking place on a system or a network device and can be used to identify policy violations and investigate security breaches. User activity data contains a wealth of information that provides insight into your IT environment. Hence, it's critical to collect, process, review and store user activity data.

With the increasing number of government regulations and industry mandates implementing user activity reporting is becoming more challenging. Some compliance mandates such as the Payment Card Industry's Data Security Standard (PCI-DSS) impose strict and clear user activity reporting

Figure A



According to a Verizon 2011 Data Breach Investigation Report, 88% of all insider breaches were conducted by regular employees and end users, proving that organizations must monitor all employees, not just privileged users, to detect potential data compromises.

requirements while others like Sarbanes-Oxley Act Section 404 provide a high level requirement allowing organizations and industries to come up with their own best practices framework to meet compliance requirements, like COBIT & COSO. Failure to comply with these regulations may lead to heavy fines, brand erosion and loss of customer confidence.

Monitor insiders

The threat of attack from insiders is real and substantial. Insider threats can emanate from any of the following:

- IT admin or privileged user
- Recently terminated employee
- Temporary employee or contractor
- Business partner
- Careless or negligent employee

Threat from insiders is different from external threats. Unlike external attacks, an insider attack involves someone who has authorized access to the network and information about the target system. While it is possible for an outsider to find a feasible external attack vector, it is much easier to collude with a disgruntled, greedy or poorly trained insider to cause financial fraud, data theft and IT sabotage. This makes it nearly impossible to prevent and stop all insider attacks.

User activity monitoring can help discover and prevent insider attacks. Implementing rigorous access controls to prevent illegitimate user access to data is a common approach, but relying solely on this method causes problems because it can hinder user productivity and also cannot scale. Monitoring user activity enable an organization to keep track of what users are doing in the environment and alert IT staff of policy violations or if an unapproved change has been made to a critical server.

Investigate security breaches

Regulations like HIPAA, CA SB 1386 and the numerous state breach notification laws require an organization to disclose the security breach to the person or organization affected. IT and user activity can be used to investigate the security breach to find not only who did what but also how it happened so that internal controls can be fixed and processes can be improved. The following table summarizes the wealth of information stored in logs:

Figure B

Log Sources	Purpose	Forensic Value
Server Logs	Monitor System Admin and user activities on Windows and UNIX servers	<ul style="list-style-type: none"> ▪ Login success/failure ▪ Account creation/deletion ▪ Audit policy changes ▪ File access (read/write/delete) ▪ Privilege escalation
Database Audit Logs	Monitor activities of DBA, users and applications connected to database	<ul style="list-style-type: none"> ▪ DB login ▪ Data access, modification, deletion ▪ DB schema and configuration changes ▪ DB user account/group changes
Identity Provisioning Logs	Monitor accounts and group changes	<ul style="list-style-type: none"> ▪ Account creation/deletion/modification ▪ Privilege escalation ▪ Group membership changes ▪ Password changes
Data Leak Prevention Logs	Monitor usage of data	<ul style="list-style-type: none"> ▪ Discover critical data ▪ Inappropriate usage of data
Web/Web-Proxy Logs	Monitor configuration changes, data theft/loss, and URL visited	<ul style="list-style-type: none"> ▪ Connection to specific website ▪ Data uploads ▪ HTTP tunneling for data theft
VPN Logs	Evidence of remote access to systems and resources	<ul style="list-style-type: none"> ▪ Network login success/failure ▪ Was there a large data transfer to a remote site?
Firewall/Network Logs	Proof of connectivity in and out of the company	<ul style="list-style-type: none"> ▪ Where did the data go? ▪ What did the system connect to? ▪ Who connected to the system? ▪ Who was denied connection?
Vulnerability Assessment Logs	Monitor vulnerabilities found on critical assets	<ul style="list-style-type: none"> ▪ Vulnerability found ▪ Security patch applied
Anti-Malware Logs	Monitor virus break outs, discover malware and spyware	<ul style="list-style-type: none"> ▪ Virus, malware or spyware found in critical assets(s) ▪ Virus, malware or spyware removed/quarantined

Lack of business relevance

Raw logs are cryptic and do not carry a lot of business relevance. Organizations are challenged to generate business relevant reports on user activity by asset groups (like a complete list of in-scope PCI servers) or user groups (such as a list of system administrators) in a given organization.

Protecting local logs from privileged users

Privileged users like system administrators or DB administrators know where the logs are stored locally on systems and are familiar with the auditing policies used within the organization. They can cover their own tracks by deleting records within local log files since they have complete access to the systems. Organizations must quickly move the logs to a remote location which cannot be accessed by those privileged users and also monitor if attempts are made to delete the local log files across systems.

Section 2: Opportunity

CA User Activity Reporting Module

CA User Activity Reporting Module provides user activity and compliance reporting and security investigation for identity, access and information usage across physical, virtual and cloud environments. It is designed to effectively verify security controls and streamline reporting and investigation of user and resource access activities to accelerate and simplify compliance and improve efficiencies.

CA User Activity Reporting Module can accelerate and simplify user activity and compliance reporting and investigation. It delivers predefined reports that are already mapped to various regulatory and control frameworks. These reports can be quickly customized, automatically delivered to your auditors and easily accessed by the Chief Security Officer (CSO) alongside other security metrics in your custom web portal. The product provides report trends that can help verify the effectiveness of security controls and expose control weaknesses that need to be proactively managed and controlled. Further investigation of policy violations can be completed quickly using log correlation and visual log analysis tools with granular drill-down capabilities. In addition, a team of CA Technologies researchers provides regular, automatic report updates, allowing organizations to keep up with various changing regulatory reporting requirements.

CA User Activity Reporting Module: overview

CA User Activity Reporting Module collects logs from a variety of applications and devices using both agent-less and agent-based methods. It then normalizes the log to CA Common Event Grammar (CEG) and reduces the volume of logs by filtering unwanted events based on pre-defined event filtering policies. Processed events are available for reporting, alerting and multi-dimensional investigation. Based on log archival policy, CA User Activity Reporting Module compresses logs and stores them on external storage systems for long term storage.

Product architecture

CA User Activity Reporting Module consists of the following components:

CA User Activity Reporting Module Server CA User Activity Reporting Module Server performs all necessary steps required for log data management, including: a) log aggregation, b) suppression and summarization, c) reporting and alerting, and d) log archival. In a large deployment, CA User Activity Reporting Module Server can be deployed to perform one or more of the following roles:

- **Collection Server** This instance of CA User Activity Reporting Module server performs log collection and aggregation. It stores logs locally in proprietary DB files and creates a compressed archive when each DB file reaches its capacity. It incrementally moves the archives to the Management Server based on a configurable schedule.
- **Management Server** This instance of CA User Activity Reporting Module server collects and manages log archives from multiple Collection Servers. The Central Log Server can be configured to store logs on a Storage Area Network (SAN) or Network Attached Storage (NAS) systems.
- **Report Server** Running queries on large data sets can be resource intensive. Hence, in some cases CA User Activity Reporting Module Server can be deployed as a dedicated Report Server. The Management Server can also serve as a Report Server.

- **Subscription Proxy Server** CA User Activity Reporting Module Server can be configured to be an online or offline subscription proxy to download and distribute subscription updates to other CA User Activity Reporting Module Servers known as Subscription Clients.

The CA User Activity Reporting Module Server uses the onboard agent to collect logs from various commercial off-the-shelf and custom applications.

CA User Activity Reporting Module Agent Optionally, CA User Activity Reporting Module Agent can be installed on remote collection points to filter unwanted events at the source and encrypt logs prior to transmission to the CA User Activity Reporting Module Server. CA User Activity Reporting Module Agent can be configured to run one or more connectors. Each connector collects raw events from a single event source, and sends normalized events to CA User Activity Reporting Module server for storage

CA User Activity Reporting Module product integration Product integration is the means by which raw events are processed and normalized for display in queries and reports. An integration includes:

- **Log sensor** A log sensor is an integration component designed to read from a specific log type such as syslog, text file, etc. CA User Activity Reporting Module provides log sensors for Syslog, text log file, Windows WMI, ODBC, Tibco and OPSEC LEA.
- **Message parsing file(s)** A XML Message Parsing (XMP) file consists of rules to parse events from a given log source.
- **Data mapping file(s)** A Data Mapping (DM) file maps parsed events into CA Common Event Grammar.
- **Content packs** A content pack consists of a set of reports targeted towards specific compliance mandates such as PCI-DSS, SOX, etc.

CA User Activity Reporting Server is the source for subscription updates from CA Technologies. The Subscription Proxy Server by default is configured to download new updates based on a preconfigured schedule.

Key product features

CA User Activity Reporting Module provides a broad range of capabilities to help your organization address its user activity and compliance reporting needs, including:

User activity and compliance reporting: Provide predefined and customizable reports mapped to common security auditing guidelines and compliance regulations (such as PCI DSS, SOX, HIPAA, FISMA, NERC, BASEL II, JSOX and more) that can be emailed and run on schedule or on demand.

User activity investigation: Deliver visual log analysis tools with drill down capabilities that can expedite the investigation of user and resource activities and the identification of policy violations.

User activity log correlation: Provide predefined and customizable log correlation capability, focusing on connecting user activity (what happened) with the individual who performed it (who did it) via analysis of complex patterns of audit logs.

Automatic compliance report updates: Provide regular, automatic content and program updates, including new compliance reports, new queries, new log correlation rules, product integrations, release upgrades and more.

Soft appliance: CA User Activity Reporting Module comes in a soft appliance consisting of a hardened Linux OS, an embedded data store and CA User Activity Reporting Module application. CA User Activity Reporting Module is quick and easy to install on certified hardware specifications from your preferred hardware vendor—Dell, IBM or HP. The soft-appliance is self-managed with automatic product updates to reduce management overhead. This allows an organization to leverage their existing hardware maintenance contracts.

Control violation alerting: Many security breaches can be prevented by detecting inappropriate access to critical resources. CA User Activity Reporting Module provides out-of-the-box action alerts that can be used to find violations to security policies in your organization. These action alerts can be modified or new action alerts can be created on the fly to appropriately police access to sensitive information. CA User Activity Reporting Module can notify you via email or RSS feed whenever a control is violated.

Multi-dimensional analysis with drill-down: CA User Activity Reporting Module simplifies investigation of security incidents, anomalous user activity or root cause analysis of system/service failure by providing multi-dimensional and interactive web UI with drill down capabilities. For example, you can open a Resource Access by Administrators report and drill-down to find which privileged user successfully modified a file on a server outside of office hours.

High data compression for log archival: CA User Activity Reporting Module provides high compression of log archives by a 10:1 ratio, thus reducing the cost involved in log archival.

IAM, CA Spectrum® and Mainframe integrations: CA User Activity Reporting Module helps extend the capabilities of leading CA Technologies solutions such as IAM (e.g. CA Access Control, CA Role & Compliance Manager, CA DLP and more), CA Spectrum and CA Mainframe solutions by delivering integrated user and resource access activity reporting for these solutions.

Role-based access control CA User Activity Reporting Module provides fine grained entitlements over access to log data, reports, queries, and product administration based on roles. CA User Activity Reporting Module comes with predefined roles of Administrator, Analyst, and Auditor. These roles can be modified and new roles can be created based on job function. CA User Activity Reporting Module also supports external user stores such as Microsoft Active Directory, CA SiteMinder®, Novell eDirectory, Sun One Directory and CA Directory.

Agent-less and agent-based log collection CA User Activity Reporting Module provides support for multiple agent-less log collection protocols such as syslog, Windows WMI, ODBC, OPSEC LEA, and more.

CA User Activity Reporting Module provides optional agent-based log collection to meet one or more of your following needs that are not met by agent-less collection methods.

- Filtering of unwanted logs at the source
- Secure log collection
- Tiered collection for enhanced scalability and failover capabilities

CA User Activity Reporting Module agents can be managed centrally using the server administration UI to configure new connectors or suppression rules, monitor agent status, and deploy new updates.

Custom integration wizards CA User Activity Reporting Module provides a Web UI-based custom integration wizard that allows the ability to parse and map logs from homegrown applications to the CA Common Event Grammar. This custom integration can be configured as a connector on a CA User Activity Reporting Module Server or as a remote agent to start collect logs and generating reports or alerts.

Any-log collection CA User Activity Reporting Module can collect raw events from unsupported log sources like homegrown applications in an organization. These logs can be archived and used for clear text search for forensic investigation. This enables an organization to efficiently become compliant with regulations while they create a custom integration for a given homegrown application using the custom integration wizard.

Section 3: Benefits

Simplify user activity reporting

Establish IT activity compliance

- **Accelerate and simplify compliance reporting:** Provides simple, automated tools that can reduce an otherwise overwhelming amount of data into reports with varying levels of detail that are useful to different stakeholders and satisfactory to auditors, and expedites user activity investigation, enabling you to figure out “what happened” quicker and shorten daily log analysis cycles.
- **Enable continuous compliance:** Delivers automatic compliance reporting updates, allowing you to more easily keep up with changing regulatory reporting requirements. Provides report trends that can efficiently verify controls on an ongoing basis in a cost-effective manner.
- **Out-of-the-box compliance reports:** CA User Activity Reporting Module comes with hundreds of reports focused on specific requirements of various government regulations like SOX, HIPAA, FISMA, etc. or industry mandates like PCI DSS.
- **Interactive investigation with drill-down:** CA User Activity Reporting Module provides interactive reports with multi-dimensional log analysis and drill down capabilities. This can simplify security forensics and root cause analysis for user activity related IT incidents.
- **Control violation alerting:** With automated violation alerting, organizations can respond to incidents without undue delay.

Accelerate time-to-value

- **Soft appliance:** CA User Activity Reporting Module is designed to be quick and easy to install on a recommended hardware platform from a preferred vendor. Please check the CA User Activity Reporting Module certification matrix available at CA Support at support.ca.com for up-to-date information on certified hardware specifications.

- **Agent-less log collection:** CA User Activity Reporting Module supports various agent-less log collection methods like syslog, OPSEC LEA, ODBC, Windows WMI, and more. This helps an organization to efficiently configure CA User Activity Reporting Module to collect logs from hundreds of log sources.
- **Any-log collection:** CA User Activity Reporting Module can collect raw logs if the log source does not have an out-of-the-box integration available and allows clear text search on these logs. This helps an organization to collect and archive logs from custom or homegrown applications without requiring the creation of mapping/parsing rules for normalization upfront.

Lower total cost of ownership

- **Embedded, self-managed data store:** CA User Activity Reporting Module uses an embedded database and does not require separate installation of expensive relational database systems, thus reducing the cost involved in procuring these databases and DB administrators required to maintain them.
- **Data compression:** CA User Activity Reporting Module provides up to 10:1 data compression to reduce data archival costs.
- **Automatic updates:** Organizations no longer need to spend cycles patching or upgrading log manager servers and agents in their environment. CA User Activity Reporting Module uses a subscription process to update the underlying OS, product binaries and ecosystem by downloading the update from CA Subscription Servers.
- **Centralized management:** Using CA User Activity Reporting Module's administration web UI, organizations can centrally manage its user activity reporting infrastructure including agents, log store, report service, subscription service, and integration library.
- **Integration with IAM products from CA Technologies:** CA User Activity Reporting Module enhances existing investments in CA Technologies security solutions by providing out-of-the-box integration with products like CA Access Control, CA Role & Compliance Manager, CA DLP, CA Identity Manager, CA SiteMinder, CA Top Secret® and CA ACF/2™.

High availability: CA User Activity Reporting Module supports failover and replication capabilities to enable high availability. You can make your user activity reporting infrastructure highly available at multiple levels:

- **Raid configuration:** The hardware used for deploying CA User Activity Reporting Module soft appliance must be configured so that first 2 drives are RAID 1 and all remaining drives (3 or more) are RAID 5. RAID 1 provides redundancy for the OS and the application, while RAID 5 protects data against loss of any one disk.
- **Agent failover:** CA User Activity Reporting Module agent can be configured with a primary Collection Server and a list of secondary Collection Servers for failover. In case the primary Collection Server is not available CA User Activity Reporting Module Agent sends the collected logs to the next available Collection Server from the list.
- **Configuration replication:** CA User Activity Reporting Module stores configurations centrally and can be configured to replicate the configuration store for high availability.
- **Log archive replication:** It is important that the log archives stored on an external storage system be highly available as well. Most of the commercial storage systems (NAS/SAN) support high availability. CA Technologies can work with you to determine the right storage device for your log archival needs.

Disaster recovery It is important for your organization to prepare for disaster recovery to enable business continuity in case of a calamity:

- **Configuration backup:** All your configurations in an existing deployment of CA User Activity Reporting Module in your organization can be backed up easily in an exported XML file. This includes your configuration settings for the servers and agents, federation maps, reports, queries, alerts, access policies and more. This exported XML can be imported back to recover your environment.
- **Log data archive backup:** CA User Activity Reporting Module server can write data to an external storage system. Most commercial storage systems support mirroring and backup software for timely backup and recovery of the stored data. CA Technologies also provides high performance Disk-to-Disk and Disk-to-Tape backup and recovery solutions like CA ARCserve® Backup and CA ARCserve® Replication to help you protect your log data.

Secure platform Maintaining the integrity of log data is critical for compliance and investigation of a security breach.

- **Log data integrity:** CA User Activity Reporting Module Servers store logs in a binary format with read only access on the system. Also, the log data stored on external storage systems can be protected by using WORM (hardware or software) based storage solution. Check with your local CA Technologies sales contact if you'd like our recommendation for choosing the right storage device for WORM based storage.
- **Encryption:** CA User Activity Reporting Module uses SSLv3 for all transmission of log data between the agent and the server. This prevents others from eavesdropping and tampering with logs in transit. This also enables digital chain of custody.
- **Agent registration:** It is important to make sure that no one can plug a rogue agent into your user activity reporting infrastructure to cause Denial of Service or send spurious logs to conceal an incident. CA User Activity Reporting Module Server uses a trust based registration mechanism to allow only trusted agents to connect to them.
- **Hardened appliance:** CA User Activity Reporting Module server soft appliance has been hardened so that only those services and ports strictly required for CA User Activity Reporting Module are running on the appliance. Our security experts regularly perform penetration tests on the soft appliance and monitor for new relevant vulnerabilities. A patch will be made available to CA User Activity Reporting Module Server for download via the Subscription Service when a vulnerability is discovered.

Section 4: The CA Technologies advantage

Leverage end-to-end solution from CA Technologies

Effective user activity and compliance reporting and investigation for identity, access and information usage is imperative to meeting compliance requirements. CA Technologies helps verify controls, as well as deliver the security controls that you need. CA User Activity Reporting Module can simplify compliance by providing predefined and customizable reports and accelerate investigations using visual, drill-down log analysis and pattern-matching log correlation. It allows organizations to keep up with various changing regulatory reporting requirements with automatic compliance report updates. CA User Activity Reporting Module not only integrates with IAM products from CA Technologies, but various other IT and Security

Management solutions, helping customers optimize IT for better business results. CA Technologies solutions for mainframe and distributed computing empower organizations to more effectively govern, manage and secure their IT operations.

**Figure C
Integration
with Security
Management
products from
CA Technologies**

Key user activity reporting use cases for Security Management integrations.

Product	Key user activity reporting use case(s)
CA Access Control	<ul style="list-style-type: none"> Privileged user monitoring Shared account monitoring Resource and system access by users Privilege escalations with effective user IDs User session tracking
CA DLP	<ul style="list-style-type: none"> Critical data found on inappropriate system Inappropriate usage of data or theft
CA Identity Manager	<ul style="list-style-type: none"> Account creation, deletion Group membership changes Rogue account creation User provisioning/de-provisioning of identities when hired, fired or promoted User password reset Measure usage of privileges assigned vs. privileges used
CA SiteMinder	<ul style="list-style-type: none"> User login to web applications Web resources accessed by users Policy changes
CA Role & Compliance Manager	<ul style="list-style-type: none"> Role violation Compare actual usage for better certification Segregation of Duty (SoD) violations
CA Top Secret for CA ACF/2	<ul style="list-style-type: none"> User login/logoff to z/OS or z/Linux Mainframe resources and system access by users Account creation, deletion on mainframes Group membership changes

CA Services

CA Services can provide implementation assistance for CA User Activity Reporting Module delivered by CA Services staff and a network of established partners chosen to help achieve a successful deployment and realize the desired business results as quickly as possible. Through our proven methodology, best practices, and expertise CA Technologies can help you achieve faster time-to-value for your product implementation.

Section 5

Conclusions

With growing pressure to be compliant with regulation mandates and the increasing importance of monitoring insiders while reducing operational costs, CA User Activity Reporting Module can help meet your organization’s user activity reporting needs. It provides a high performance and scalable user

activity reporting architecture for collecting large volumes of IT and user activity logs for reporting, violation alerting, investigation and archival. It helps you meet your objectives by providing:

- **Improved compliance:** Establish compliance with out-of-the-box integrations and compliance reports.
- **Rapid time-to-value:** Quickly deploy your user activity reporting solution by taking advantage of soft appliance model with agent- less collection.
- **Reduced total cost of ownership:** CA User Activity Reporting Module can reduce TCO by using an embedded log store, providing high data compression for archival and automatic update. CA User Activity Reporting Module integration with other IAM products helps reduce administrative overhead and overall project costs.

Section 6

References

[DB1]—“Verizon 2011 Data Breach Investigations Report”

http://www.verizonbusiness.com/resources/reports/rp_data-breach-investigations-report-2011_en_xg.pdf

CA Technologies is an IT management software and solutions company with expertise across all IT environments—from mainframe and distributed, to virtual and cloud. CA Technologies manages and secures IT environments and enables customers to deliver more flexible IT services. CA Technologies innovative products and services provide the insight and control essential for IT organizations to power business agility. The majority of the Global Fortune 500 rely on CA Technologies to manage their evolving IT ecosystems. For additional information, visit CA Technologies at ca.com.

Copyright ©2011 CA. All rights reserved. All trademarks, trade names, service marks and logos referenced herein belong to their respective companies. This document is for your informational purposes only. CA assumes no responsibility for the accuracy or completeness of the information. To the extent permitted by applicable law, CA provides this document “as is” without warranty of any kind, including, without limitation, any implied warranties of merchantability, fitness for a particular purpose, or noninfringement. In no event will CA be liable for any loss or damage, direct or indirect, from the use of this document, including, without limitation, lost profits, business interruption, goodwill, or lost data, even if CA is expressly advised in advance of the possibility of such damages.

CA does not provide legal advice. Neither this document nor any CA software product referenced herein shall serve as a substitute for your compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, policy, standard, guideline, measure, requirement, administrative order, executive order, etc. (collectively, “Laws”)) referenced in this document. You should consult with competent legal counsel regarding any Laws referenced herein..