CA Identity Manager Reporting

Presenter:

Chris Thomas
Principal Support Engineer
SME IdM Reporting

January 20, 2015

ca technologies

Webcast Agenda

- Topic 1: Post Install Configurations *(Windows / Linux)*
  - Tedious manual / error prone process quickly simplified
  - Upgrade *(security enhancements)* Legacy BO integration.
- Topic 2: Audit Reports
  - Setup and enable.
  - Configure and report
  - Maintenance and scoping.
- Topic 3: Snapshot Reports
  - Setup and capture
  - Comprehend process and design.
- Live Q&A with Chris Thomas

Post Install Configurations

Common problems, *nix installations,

- During implementation many times "*all*" (both audit and snapshot) reports fail with "*connection errors*". This issue has been solved repeatedly since IdM 12.0. All solutions have been meticulously documented below.
  - More Info: **Can't view reports.**

- Importing CA IdM Crystal reports within the Business Intelligence Archive Resource (biar) can be a confusing manual process. For windows, you should be using the Import Wizard, for linux the import biar file shell script will suffice.
  - Importing default IDM reports (Use this for Windows, don't follow bookshelf)

- Install guidance for Linux / Unix, lessons learned.
  - **Identity Minder Reporting on Linux. (the missing manual)**
  - **Install Reporting on Solaris**

Post Install Configurations

Security updates, Firewall setup

- Apache security vulnerabilities (tomcat, MySQL)
  - Upgrade cabi 3.3 SP1, which will upgrade to Tomcat 7 and use sql anywhere for cms db.
    - **Upgrade Report server and Tomcat**
  - Security vulnerabilities with Tomcat 7, upgrade to Tomcat 8.
    - **Upgrading CABI 3.3 SP1 Tomcat version-windows.pdf**
- When required, setup IdM reporting in a firewalled environment; Where the report server, application server and client workstation all communicate over the network via the enterprise firewall.
  - **Identity Manager Reports through a Firewall.**

Audit Reports

Architecture, Setup, Blank Reports

- IdM Auditing is mutually exclusive from BusinessObjects (BO) auditing db, and IdM's Task Persistence and archive db, but easily confused.
  - **Architecture Best Practice**
- Setup auditing sounds simple, but this manual setup generates quite a few issues.
  - **Enable / Configure Auditing.**
- If auditing isn't properly enabled, reports will show up blank.
  - **Approval Report blank**
  - **Account Detail Report Blank**
  - **Enable / Disable Users' caveats**

Audit Reports

Localization, customization, scalability

- Audit reports aren't certified for localized environments.
  - **Audit Reports NOT translated in Localized IdM environment**
- CA Business Intelligence (CABI) audit reports will only work when configured to run against IdM's audit db, unless you customize the OOTB reports.
  - **Custom Identity Manager Reports.**
- Auditing can easily grow extremely large over time. If you're in a large scale environment, care should be taken so that you, and your deployment, don't unnecessarily suffer from information overload.
  - More info: **large scale audit database**

Snapshot Reports

Make a snapshot report, Understand architecture and Design

- Configure snapshot definition, Capture snapshot, associate it with an OOTB Report, request it, then view it.
  - **Create a Snapshot Definition**
  - **Associate a Snapshot Definition with a Report Task**
  - **Capture Snapshot Data**
  - **Request a Report**
- IdM Reporting architecture and Design explained.
  - Database structure
    - **Reporting Architecture Best Practice**
  - Reporting design Challenges
    - **Deprecation of Snapshot Architecture**
  - Work effectively within the snapshot design.
    - **Critical reporting fix for large scale audit database**
- **Quick Demo** *(time permitting)*

Q&A

- Please enter your question into the Q&A WebEx window.
- Follow the **CA Security Community**!

ca.com/talksecurity

- Follow @CASecurity and @CA_Community on Twitter!

Join CA Communities – Become a CA Champion!
Visit communities.ca.com.

- **LEARN** about best practices and use cases. Lower your TCO and maximize impact.
- **CONNECT** with product management and support. Ask a question or submit an idea for a future release.
- **SHARE** your experience and expertise with other CA customers and partners.

- Join the CA Security Community.
  - Products covered:
    - CA Single Sign-On
    - CA Identity Suite
    - CA Privileged Identity Manager
    - CA Secure Cloud
    - CA Data Protection
    - CA Risk Authentication
    - CA Strong Authentication
    - CA Directory
  - Go to ca.com/talksecurity