20180627 InCommon Federation Manager Incident Summary

July 26, 2018

Summary

During a routine upgrade to the InCommon Federation Manager application on the evening of June 27, 2018, a configuration error led to the accidental deletion of all data from the production database. The database was partially restored later that evening using a backup from the previous day, and fully restored by the following afternoon. There was no interruption to metadata signing and publishing.

Impact

- The Federation Manager service was unavailable or in a degraded state for 19 hours and 15 minutes (from 4:30 PM CDT on June 27, 2018, until 11:45 AM CDT on June 28, 2018).
- InCommon staff identified 13 entities having changes that had been published in metadata before the upgrade on June 27, but had not been captured in the database backup from June 26.
  - For the 7 entities with changes involving critical functional elements (including new entities, changes to signing certificates, and new ACS endpoints), InCommon staff manually applied the changes and notified the relevant site administrators.
  - For the 6 entities with changes involving only informational elements (contacts, logo and privacy URLs), InCommon staff contacted the relevant site administrators to coordinate next steps.
- Other database changes that could not be reconstructed from published metadata (including changes to user roles, passwords, and in-process metadata) were re-applied on a best-effort basis by InCommon Registration Authority staff.
- There was no interruption to metadata signing, publishing, or distribution.

Analysis

The root cause of the incident was a configuration error in the production instance of the application. The configuration error caused a test command during the deployment process to truncate the production database. In addition, the most recent database backup was from the previous day, June 26. The database was partially restored later during the evening of June 27, but the following morning, June 28, it was discovered that not all tables had been restored correctly. The database was then restored again, and all entities were verified against published metadata.

Other Issues

This incident highlighted opportunities to improve our deployment planning and change control processes, and it reinforced the need to expand on our continuous integration process by building a continuous deployment pipeline.

Prevention and Next Steps

To protect against similar incidents in the future, we've corrected the configuration error in the production application instance. We've also expanded our change management processes to include more rigorous deployment and rollback planning, and we're working to build a continuous deployment pipeline that will support automated deployment testing.

Operational Value

The recovery effort spanned multiple business units and provided a thorough test of our disaster recovery procedures. Service monitoring and alerts worked as expected. Our practices of preserving generated metadata and ensuring consistent ordering of elements in metadata helped to minimize the recovery time.