Incident Report - May 20, 2015

Incident #2015-81

Summary

On the morning of May 20th, 2015 for a period of about half an hour (between approximately 7:15 – 7:45am) the production Shibboleth Single Sign-On (SSO) service was unavailable, and a service notification page was displayed to any users attempting to access a Queen's University Shibboleth SSO protected production website or service. Affected services included: Moodle, Liferay Portal (my.queensu.ca), SOLUS, PeopleSoft, and Ensemble Streaming. Any user who already had an active Shibboleth SSO session during this period should have been able to continue using the sites whose service providers they had authenticated with, however new logins would not have been possible during this period.

This issue was the result of attempting to update the metadata configuration on our production Shibboleth Identity Provider (IDP) https://login.queensu.ca, for the Canadian Access Federation. We were previously utilizing SHA1 signed metadata which became deprecated (by the CAF), and was replaced with new SHA256 signed metadata. This configuration is different than all our other defined relying parties, as the metadata for the CAF is combined and encrypted. This special configuration was not taken into account when trying to update the metadata, resulting in the Shibboleth IDP being unable to restart correctly.

As this was occurring during a morning service window, the secondary IDP node was shut down in order to fully examine the operational status of the primary IDP node through the load-balancer. During this time as the secondary node was offline, and the primary node was having issues restarting, the load-balancer displayed a service outage notification. After about 20 minutes of attempting to troubleshoot the issue, the configuration was reverted to its previous state, and both production Shibboleth IDP nodes were back online by 7:45am.

As metadata updates are frequent and normally routine, Middleware was not always creating change control tickets to track them. Because there was no change control issue for ITS staff to refer to, a notification was issued at about 8:10am summarizing the time period of the outage and some of the affected services. The IT Support Centre did not receive any tickets about this issue, as it occurred and was resolved before 8:00am. Middleware has since created a new Shibboleth IDP update and restart procedure that includes always pre-creating change control tickets and allows for testing configuration changes without causing a service outage.

Issue

Attempting to update the metadata configuration on our production Shibboleth Identity Provider (IDP) https://login.queensu.ca, for the Canadian Access Federation, which is combined and encrypted, and our only relying party configured in this manner. The normal configuration changes to utilize new metadata were insufficient, resulting in the Shibboleth IDP being unable to restart. The configuration was reverted to its previous state, and the IDP was brought back online.

Impact

During the outage, any users attempting to login to a Queen's University Shibboleth SSO protected production website would have been presented with a service outage notification page. Some of the production sites affected included: Moodle, Queen's Portal (my.queensu.ca), SOLUS, PeopleSoft, and Ensemble Streaming.

Users who already had an active session with a Shibboleth Service Provider would have been able to continue using the particular sites they had logged into, but would have been unable to log into other SSO protected sites.

Root Cause

This issue was the result of attempting to update the metadata configuration on our production Shibboleth Identity Provider (IDP) https://login.queensu.ca, for the Canadian Access Federation. This configuration is different than all our other defined relying parties, as the metadata for the CAF is combined and encrypted. We were previously utilizing SHA1 signed metadata which became deprecated (by the CAF), and was replaced with new SHA256 signed metadata. This special configuration was not taken into account when trying to update the metadata, resulting in the Shibboleth IDP being unable to restart correctly. Taking the second node offline to test the performance of the first node through the load-balancer caused a service outage.

Resolution

After about 20 minutes of attempting to troubleshoot the issue, the configuration was reverted to its previous revision utilizing SVN, and both production Shibboleth IDP nodes were back online by 7:45am. The issue was investigated, it was discovered how to correctly update the CAF's metadata configuration, and this update was made during a service window the following morning.

Communications (Internal)

A change control ticket was not created prior to this configuration update, and while the issue was occurring it seemed more prudent to resolve the issue than spend the time crafting a notification. Once the issue was resolved, an ITS notification was sent out to describe the issue, and inform the user base.

ITSPP Communications (External)

Notifications (May 20th 2015)

- 8:10am – Shared Authentication Services unavailable between 7:15-7:40am + List of Affected Services

Lessons Learned

- A Change Control ticket was not created prior to configuration update, these will now always be created such that other ITS staff (including on-call and the support centre) can be aware of work happening outside normal business hours, and know what to do when a monitoring system shows one of our services as offline.
- A new Shibboleth IDP update and restart procedure was created, which includes updating and testing the node with lower load-balancer priority, without the need to take the secondary node offline, preventing future service outages during routine configuration changes.
- Increased awareness of special cases in our production Shibboleth IDP's relying party configuration, including the Canadian Access Federation, Concur, and Lynda.com, which all have unique additional requirements.

Action Items

- Create new Shibboleth IDP update and restart procedure for future changes, preventing unnecessary service outages.
- Ensure that when updating the Shibboleth configuration of the handful of special configurations in production, that the required changes have been fully investigated.
- Always create iTrack Change Control tickets prior to configuration updates on production systems, especially important if working from home outside normal business hours.