Root Cause Analysis


Summary: On Monday February 4, 2013, at approximately 3:00 PM, the SSL certificate on the eDir and LDAP servers expired. As a result, multiple services were unavailable, such as: Blackboard, Roxen, VPN, HPSM, VoIP Call Centers, Wireless (UAlaska) as well as others. Within 30 minutes OIT Security generated a new certificate. Within 60 minutes Technical Services (TS) applied the certificate to eDir, which allowed access to the page; however, search functionality was still down. Immediately following, it was discovered that for LDAP authentication, the certificate would also need to be applied to the LDAP servers before all services were restored. Documentation critical to the repair effort was stored on one of the unavailable systems, which exacerbated the situation. Documentation was obtained and the first LDAP server was brought back online at approximately 12:30 AM, February 5th. All services were restored at this time. The new certificate was applied to the remaining LDAP servers and each was brought back online, restoring full redundancy at 2:45 AM. At 7:15 AM, February 5th, The Support Center reported that the Call Center was not allowing logins, preventing calls from being received by the Support Center and the Registrar Office. It was determined that this was due to the same expired certificate. Certificate was applied and service was restored at approximately 11:00AM.

Quick Takeaways:

- Outage was the result of inaction by the service owner
- Review and clarify certificate renewal process
- Consider central system-wide management of certificates
- Ensure hardcopy or other suitable backup of critical procedures

Detail Timeline:

January 4, 2013 – InCommon sent a notification that the certificate for eDir would expire in 30 days. The email was sent to and received by the IAM-L listserv as well as the original approver in OIT Security. The listserv recipients include all members of the Identity and Access Management (IAM) office, the Chief Information Security Officer, one member of Telecommunication Services and one member of TS. IAM is the eDir service owner. No action was taken to request a new certificate for the eDir service.

January 7, 2013 – OIT Security sent a follow-up email to all members of the IAM office providing instruction to renew the certificate.
February 4, 2013, at 2:59 PM - The SSL certificate for the eDir service expired. As a result, multiple services were unavailable, such as: Blackboard, Roxen, VPN, HPSM, VoIP Call Centers, Wireless (UAlaska) as well as others.

February 4, 2013, at approximately 3:20 PM – Outage was reported via the Support Center and TS was notified. OIT Security immediately generated a new certificate. TS applied the certificate to the two servers which provide the eDir service. The eDir front end became available at approximately 4:00 PM; however, eDir search functionality and those services which rely on LDAP for authentication were still down. TS found that the documentation required to bring the services online resided on one of the unavailable servers.

February 5, 2013, at approximately 12:30 AM – TS accessed the documentation and applied the certificate to one of the LDAP servers. This restored all services at approximately 12:30 AM. The certificate was applied to the remaining servers, which restored full redundancy at 2:45 AM.

February 5, 2013, at approximately 7:15 AM – The Support Center reported that the Call Centers were not allowing logins. This affected the Support Center, Video Conferencing Services and the Registrar’s Office. This was due to the same expired certificate. Telecommunication Services applied the certificate and service was restored at approximately 11:00AM.

**Identified Problem Areas and Future Prevention:**

The root cause points to a failure to act on the 30-day notification or the follow-up email provided by OIT Security. The service owner for eDir is IAM. The issue was avoidable and the impact was severe.

There is a perceived lack of ownership for the service. The service is hosted on servers administered by TS. IAM does not have full administrative access to the servers. A logical process is to have the service owner open a ticket to have TS renew the certificate and track to closure. This did not happen. Although multiple offices received the 30-day notification, only OIT Security took action.

The current management strategy for SSL certificates is distributed among the certificate owners and OIT Security. OIT Security is the single point of approval for all certificates, yet it appears each service owner is left to manage the certificate once it is approved. The OIT Security office has the capability to generate reports based on pending expiration dates of existing certificates. This does not enable them to track the renewal process, though a report could be used to increase awareness of pending expiration dates.

The documentation needed to restore service was located on a server which was unavailable due to the outage. This significantly extended the time needed to restore service. Departments should consider hardcopy or other suitable backups of important procedures.

One alternative identified is to make certificate renewals an annual process. Certificates can be renewed on an annual or semiannual basis regardless of when they expire.