Table of Contents

Kerberos issue

Description

An upgrade to the Kerberos KDC that supports the Linux services caused several authentication related problems on the Batch service, Castor and interactive Linux services (lxadm and VOBOX).

Impact

- Several users had problems logging into lxvoadm and lxadm, and the VO boxes (misc tickets).
- CMS and ATLAS had problems accessing xrootd files on Castor from the batch nodes (GGUS alarm ticket)
- ATLAS T0 batch jobs were unable to obtain a Kerberos token (jobs failed) for around 30 minutes (GGUS alarm ticket).

Background

The Kerberos services for CERN are based on Microsoft's Active Directory following the migration from the Heimdahl kerberos service earlier in the year. Following the completion of the Exchange 2003 mail service to Exchange 2010, it was possible to raise the security level to Windows 2008 levels in order to increase functionality (such as authenticated-only access to group members for privacy improvements). One of the new features was the advanced encryption services (AES 128 and 256) support for Kerberos authentication will be available.

This change has been scheduled with the online community to be performed during a technical stop since an issue with the Active Directory service would have a significant impact on the environment in the technical network.

The change was announced in the IT C5 meeting on the previous Friday (6th May). Since the change was felt to be a low impact one, there was no announcement posted to the service status board or included in the IT News letter.

Time line of the incident

All times are in Swiss time.

08:10 Active directory settings modified

Functional levels for the Domain and forest were moved from 2003 to 2008 levels.

11:55 Ticket reported to Kerberos regarding misc login issues

SNOW ticket INC:037486 from IT/PES on call, summarizing misc reported ssh login issues.

14:07 xrootd access from cmsRun not working since this morning

CMS raise a GGUS alarm ticket (https://gus.fzk.de/ws/ticket_info.php?ticket=70434)

14:21 xrootd access from cmsRun not working since this morning

CMS decreased importance of their GGUS alarm ticket (https://gus.fzk.de/ws/ticket_info.php?ticket=70434) Changed priority from top priority to less urgent since they were suspecting some issue on their code.

17:41 Massive failures due to lost AFS token on ATLAS Tier-0 LSF batch nodes

Atlas raise a GGUS alarm ticket (https://gus.fzk.de/ws/ticket_info.php?ticket=70450)

18:06 xrootd access from cmsRun not working since this morning

First workaround verified and proposed to experiment (https://gus.fzk.de/ws/ticket_info.php?ticket=70434). It required to add one line in the users job.

19:37 xrootd access from cmsRun not working since this morning

Final workaround verified and proposed to experiment (https://gus.fzk.de/ws/ticket_info.php?ticket=70434). This does not need the extra line (although it can live with it in most cases).

22:53 xrootd access from cmsRun not working since this morning

Ticket closed (https://gus.fzk.de/ws/ticket_info.php?ticket=70434). After observing successful reading (xrdcp) from LSF jobs running as cmsprd ticket is closed

Analysis

The Kerberos tokens issues for the Batch system are retrieved using a master certificate authentication, through the kinit command. To differenciate the Active Directory tokens from the Heimdal tokens during the migration phase where both KDC coexist, the various scripts are checking token encryption to make the difference (as the realm cern.ch is the same on both KDCs).

The Active Directory upgrade did an unexpected change on the kinit token issuance based on certificate, providing AES256 encrypted tokens when ArcFour tokens were expected. As a result, Active Directory tokens are not identified properly and cannot be renewed, preventing batch jobs to run properly. Kinit command allows to force an encryption type, but this give an error 'invalid password' which is definitely not expected here, and the we are not able to understand yet.

The impact of the change on the batch system was not anticipated and, while there had been testing with lxplus and AFS, there was not a regression test performed with the token extension procedure.

Follow up

- Prepare test case for issue and raise a support call with Microsoft to understand why it was not possible to force the encryption type with kinit.
    - Created 'Urgent' Incident 111051122694692 (https://premier.microsoft.com/viewincidents.aspx?&incno=111051122694692)
- Agree simple regression test for kerberos token extension which can be used when testing new configurations of AD.
- Understand the delay between the initial change at 08:30 and the alarm tickets being created (around 5 hours later)

- Review the plan for the Heimdahl Kerberos de-commissioning to see if we can remove the dual Kerberos configuration in batch/lxplus in the short term.
- Review change publication procedures with the new IT service status board to determine how changes which are expected to have a low impact can still be visible for supporters who need to understand potential causes of problems.

Links

This topic: PESgroup > IncidentKerberos10052011
Topic revision: r13 - 2014-11-20 - TWikiAdminUser