IOWA STATE UNIVERSITY
IT Services Technical Notes
IT

Windows Administrators Meeting

December 9, 2011
Notes (taken by Steve Kunz [ITSYS])

Meeting Started (9:00)

Announcements

- **Account expirations:** Steve Kunz [ITSYS] announced that account expirations took place this week. Provisioned account that were suspended in the past (because the user is no longer affiliated with the university) were deleted.

AD "Job Title" Attribute – Possible Change? [Steve Kunz - ITSYS]

Steve Kunz [ITSYS] talked about a suggestion to place a person's official university title (which can be seen in the information on info.iastate.edu) into the AD "title" attribute (which appears in the "Job Title" fields on the "Organization" tab for a user in ADU&C). Currently the AD "title" contains the proper name (first name followed by last name) followed by the affiliation (faculty/staff/affiliate/student) followed by the long name of their department. This information is loaded from directory.iastate.edu (from the "title" LDAP attribute).

Kunz said the change seems a reasonable one but one side effect is that two pieces of information currently on the AD "Job Title" would not be available – the affiliation and long department name. [Info since the meeting: the long department name already appears on the AD "department" and "physicalDeliveryOfficeName" attributes and is seen in the "Office" field on the "General" tab in ADU&C, where it would continue to be available - SLK]

Kunz asked if anyone were relying on the information in the current format. In the discussion that followed it appeared nobody in the meeting was relying on the current format of the "Job Title". A couple suggestions were made regarding the loss of the affiliation information. One suggestion was that it could still be included with the correct official title, perhaps with square-brackets around it to separate it from the actual title. Another suggestion was that the affiliation be placed on the existing "employeeType" attribute (which is not displayed on ADU&C though could still be seen by ADSIedit, for example). Another thought would be that it could be appended (in square brackets) after the "Description" (which already contains the proper name in first-name followed by last-name order).

This topic will be discussed further in an upcoming CCSG meeting and have an email thread in the CCSG and WinAdmin mailing lists so people have time to provide input. Studies need to be made as to whether or not anyone seems to be using the mentioned fields already for their own purposes (since they were not mastered in the past). Watch for more in the future.

Comments/questions/suggestions to Steve Kunz at skunz@iastate.edu

Protecting Outward-facing Servers from Password Hacking Attacks [Beata Pruski - ITSYS]

Beata Pruski [ITSYS] gave a talk and demo on some new tools the Enterprise Admins will make available for detecting account-hacking on Windows systems. These tools will be valuable in protecting the member systems from being “auto-blocked” by the Enterprise domain controllers when too many failed password attempts are made by users attempting to hack into ISU accounts using member systems. The tools to be provided will allow system administrators to regularly scan their own security logs (logon failures must be enabled in the audit policy for the system) and when a threshold is reached for a given IP a local IPSec rule would be created that would block all IP traffic from the offending IP address. If the member system protects itself soon enough from outside attack then the domain controllers would never see enough failed attempts to auto-block the system.

The components created by Pruski/Kunz would allow email notification in addition to auto-blocking (or email notification only – no auto-blocking). They would be simple to install and be run via a scheduled task. Work on bundling the software and writing documentation is in progress. Send comments/questions to Beata Pruski [ITSYS] at bapruski@iastate.edu.

There was some discussion about the fact that other issues can cause systems to be auto-blocked by the domain controllers that do not involve account hacking by malicious systems. One example is when the system time on the member system becomes incorrect enough to cause all Kerberos authentications to fail. A recent problem in this area happened with SCCM boot images that were setting the time zone incorrectly. The following boot images have been corrected to fix the problem:

1. WinPE 3.1 Boot Image (x86)
2. WinPE 3.1 Boot Image (x64)

If you use these components you should rebuild all boot media built prior to 11/09/11. A TechNote on this issue is available at:
http://www.tech.its.iastate.edu/windows/admin/SCCMtzprob.pdf
Thanks to Tim Danzer [H SCI] and Darrin Fischer [ITSYS] for solving this problem.

Open Discussion

No time was available for open discussion.

Meeting Adjourned (10:00)

Next meeting is scheduled for January 13 (provided a sufficient agenda exists).