

Survey Results for Imanami

An Osterman Research Survey Report

Published May 2010



Survey Results

BACKGROUND AND METHODOLOGY

Osterman Research conducted a survey during April 2010 on behalf of Imanami to understand issues related to Active Directory (AD) administration in organizations of various sizes. A total of 155 surveys were completed using the Osterman Research survey panel.

The mean number of employees and email users at the organizations surveyed was 10,229 and 9,526, respectively; the medians were 1,000 and 750. 51% of the respondent organizations had 1,000 or more employees; 48% had 1,000 or more email users. In order to qualify for completion of the survey, respondents had to be involved with and/or knowledgeable about AD administration in their organization.

USER PROVISIONING

The survey found that 42% of organizations have updated user-provisioning capabilities during the previous 12 months. In terms of the most important aspects of user provisioning, authentication credentials for system access were deemed important or extremely important by 89% of respondents. 86% deemed that accounts associated with each user are this important, followed by managing group membership or role assignments from which entitlements may flow (72%).

Among the least important aspects of user provisioning are assignment of roles (57%) and access policy/rule sets (60%). Further, 48% of respondents believe that identity/access management/life cycle solutions are very important, while another 37% believe that these solutions are somewhat important. Only 1% determined that these solutions are not important at all.

IT TIME INVESTMENTS

Managing groups is a significant time investment for many organizations, although the results from the research varied widely. Our research found that the median IT time investment in managing groups during a typical week is 8.3 person-hours per 1,000 users. If we assume that the average, fully burdened salary for an IT administrator is \$80,000 annually, that translates to a total cost of \$16,600 per 1,000 users annually, \$16.60 per user per year, or \$1.38 per user per month.

Interestingly, the survey also found that less time is being spent on managing groups when compared to time investments from a year ago. When asked how many person-hours per week were spent on managing groups 12 months ago, respondents indicated a median of 8.9 person-hours per week, representing a decrease of 7% during the past 12 months. That said, while 20% are spending more time in managing groups now compared to one year ago and 21% are spending less time, the vast majority – 58% – are spending the same amount of time managing groups as they were last year.

We also segmented the data into only those that have updated user-provisioning capabilities during the past year. We found that among those that had updated these capabilities, none were spending more time managing groups now compared to a year ago, 26% were spending less time and 74% were spending the same amount of time.

This clearly indicates that updates in user provisioning capabilities had at least some impact on the amount of time that organizations spend managing AD groups.

THE PAIN OF UPDATING GROUPS IN AD

On balance, the survey revealed that updating groups in AD is not tremendously painful: 16% responded that these updates are not at all painful and another 47% told us that they are not “too” painful. However, 10% responded that updating groups in AD is painful or very painful, and another 27% believe it to be “somewhat” painful. Clearly, this represents enough pain that a way to alleviate the difficulties with AD updates, coupled with the problems caused when groups are not updated in a timely manner, would be welcomed by a fairly significant proportion of decision makers.

We also found that 59% of organizations manage groups in AD only manually, 8% use an automated system, and 33% use a combination of manual and automatic methods.

We examined ratings for the pain of updating groups in AD for those that use only manual methods, expecting that those performing only manual updates would have a more “painful” experience with AD updates. However, that turned out not to be the case: although there were slight differences between the manual-only group and the overall population, there was little difference between the two groups. This tells us that current, automated methods of updating groups in AD do relatively little to alleviate the pain of group updates.

WHY ARE AD GROUPS USED?

The most common reason that AD groups is used is to grant access to files and folders, cited by 93% of respondents. The next most common reasons are granting permission to systems (78%), applying Group Policy Objects (GPOs) at the group level (73%), and sending email to distribution groups (66%). The least common reason for using AD groups is to send email to mail-enabled security groups (43%). Further, 33% of organizations have non-traditional uses for AD groups, such as not to email a group or to grant/deny access within a security group. However, 56% of organizations have used AD groups for SharePoint access, a role for groups that we anticipate will become significantly greater with the increasing use of SharePoint over the next 12-18 months.

APPLICATIONS FOR AD GROUPS

The survey also found other reasons and applications for AD groups and GPOs:

- 58% of organizations have applied GPOs to a group of computers by creating a security group with computers as members of the group(s).
- 48% of organizations allow mail-enabled security groups and another 16% reported that they possibly do so.
- 38% of respondents have considered creating a workflow to wider audiences to improve response times on projects and other tasks, such as using a distribution group or security group for workflow approvals.

- 36% of respondents would consider using a GPO that would force a country-specific email signature line for each user in that group. Among large, multinational companies (something for which we did not screen in the survey), we anticipate that this proportion would be much higher.
- 32% of respondents have, at some point, created a group for text-message emergency notifications.
- 22% of organizations use workflow to control users joining or leaving groups through a self-service portal.
- 17% of organizations have used AD groups to disable email communication between two sides of their organization. This is extremely important for establishing and enforcing ethical walls in heavily regulated organizations, such as energy companies in which the transmission and distribution sides of the business must not communicate with one another.

WHAT HAS BEEN THE IMPACT OF SECURITY BREACHES?

In one out of five organizations surveyed, someone has accessed information from AD that they were not authorized to access. Further, there have been many well-publicized, high-level security breaches – for example, the Privacy Rights Clearinghouse offers a database of data breaches of all types that have occurred since 2005. However, 37% of respondents to the survey told us that these security breaches have had no impact on the way that they use AD groups, while another 38% of respondents are concerned but have done little in response. That said, 16% of organizations are considering changes to the way they manage groups as a result of major data breaches and another 9% are concerned and have actually changed the way that they use groups.

This clearly indicates that the consequences of major security breaches have not been lost on many decision makers in the context of how they manage AD groups. We would anticipate that continued data breaches, coupled with additional regulations aimed at victim notification, will drive more organizations to adopt stricter controls for data access, one of which will be in the way that AD groups are managed.

THE RISK OF OUT-OF-DATE AD GROUPS

The survey found that 31% of organizations consider out-of-date AD groups to be risky or very risky, while another 39% consider them to be somewhat risky. Only 31% consider out-of-date AD groups to pose little or no risk to their organizations.

CONCLUSIONS

There are a number of conclusions that we can draw from the research:

- User provisioning is an important pain point for many organizations, so much so that more than two in five organizations updated these capabilities during a fairly serious recession.
- Managing AD groups is a time-consuming and expensive task for the typical organization. For example, an organization of 2,500 users will consume more than

Survey Results for Imanami

one-half of a full-time equivalent (FTE) IT staff member's time. This is a significant use of IT staff time for a task that is important, but offers relatively little competitive advantage to an organization. If it can be demonstrated that a technology was available to reduce the amount of time devoted to managing AD groups, this would likely resonate with a large proportion of mid-sized and large organizations.

- Updating groups in AD is a sufficiently painful experience that many organizations are willing to make investments to alleviate this pain. This will be more important over time as organizations use AD groups to manage their growing SharePoint deployments.
- Also in the context of increasing use of SharePoint is the importance that will be placed on keeping AD groups up-to-date. As a growing proportion of corporate content migrates to SharePoint, and as the consequences for data breaches become more severe, managing AD groups more effectively and in at least a near real-time manner will become more important. This will be particularly true in heavily regulated industries like energy, financial services and healthcare.

© 2010 Osterman Research, Inc. All rights reserved.

No part of this document may be reproduced in any form by any means, nor may it be distributed without the permission of Osterman Research, Inc., nor may it be resold or distributed by any entity other than Osterman Research, Inc., without prior written authorization of Osterman Research, Inc.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.