How Cisco IT Migrated to Microsoft Active Directory

Automated migration and provisioning tools reduce cost of migrating to Active Directory and simplify training and troubleshooting.

Cisco IT Case Study / Business Applications / Active Directory Migration: Cisco IT previously maintained separate directories for each network operating system and Web application, with 50 directories in the lab environment alone. To simplify training and troubleshooting, reduce costs, and facilitate compliance with the Sarbanes-Oxley Act, Cisco IT is consolidating these directories into a single enterprise directory. This case study describes why and how Cisco IT is making this transition. Cisco customers can draw on Cisco IT's real-world experience in this area to help support similar enterprise needs.

"Our automated migration script enabled us to migrate to Active Directory for $630 per Windows desktop, compared to an industry average of $2000 to $3100."

– Ray Beauchesne, IT Program Manager, Cisco Systems

BACKGROUND

A directory service stores information about entities associated with the network, such as routers, desktops, applications, and people. Applications access the directory service before granting access to users, and network administrators use it to view up-to-date topology information. Directory services come in two types. Network operating system (NOS) directories are used for a specific operating system or application. Enterprise directories, in contrast, provide a central repository of information about people and their access rights.

CHALLENGE

The Cisco Systems® IT group traditionally maintained separate NOS and Lightweight Directory Access Protocol (LDAP) directories for each application server, including mail servers, MeetingMaker calendar servers, TACACS+ authentication servers, , Oracle applications, and Macintosh and Windows desktops. Managing disparate NOS and LDAP directory services—50 in the lab environment alone—created problems for Cisco users, administrators, and application developers. Users had to keep track of multiple user accounts and passwords to log into different systems. Administrators had to be trained on different systems, and update multiple directories when employees joined or left the company. Cisco developers, in turn, had to write different code for every directory that their applications would need to access. "Maintaining separate directories increased costs because we had to train different people to support each one and pay licensing fees," adds Ray Beauchesne, IT program manager. "It also complicated compliance with the Sarbanes-Oxley Act, which stipulates that a given individual should have access to certain data and applications and not to others. The more directory environments you maintain, the harder it is to ensure compliance." Finally, multiple directory environments made it difficult to identify the responsible group if a problem arose.

Cisco IT decided to deploy a single LDAP enterprise directory and to consolidate its NOS directory services where possible. "Even after adopting an enterprise directory, Cisco still needs standalone directories—for example, to ensure security when partners access resources, and to shield the production network when new applications are tested," Beauchesne explains.

The impetus to take action came in the late 1990s, when Windows NT 4.0 was approaching end of life. Cisco IT needed to transition its Windows workstations, servers, and users to a new directory service, and seized the opportunity to migrate all NOS directories throughout the company to a single platform.

Cisco IT faced two main challenges in revamping its directory strategy. One was to select a directory services product with the lowest cost of ownership. “We wanted to use the same product for the enterprise directory and NOS directories,” says Dave Jones, directory services architect. The other challenge was planning the directory services architecture to simplify administration, protect the integrity of the master database, and ensure fast response as employees around the world tried to authenticate against various applications. “To simplify administration, our goal was to automate updates whenever possible,” says Jones. “Fewer manual changes to network information would reduce the chance of human error. It would also help ensure consistent host and application configuration.”

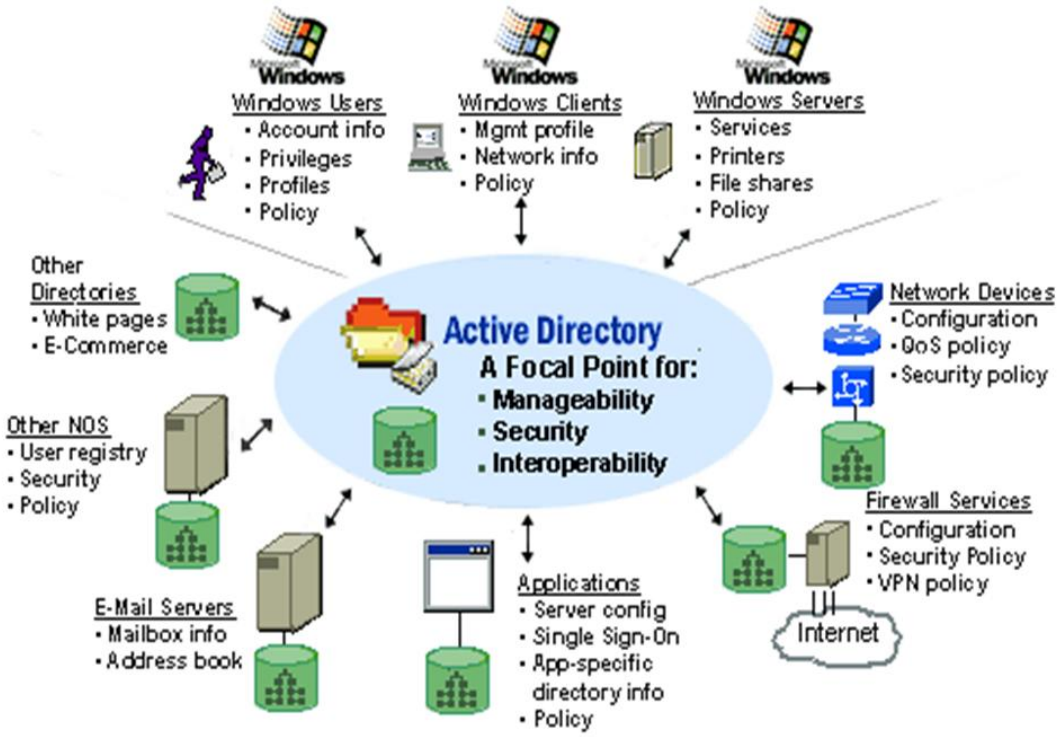
SOLUTION

Choosing a Solution: Microsoft Active Directory

Cisco IT selected Microsoft Active Directory as both the enterprise LDAP directory and NOS directory solution. “Active Directory provides all of the directory functions that Cisco needs in one product,” says Beauchesne. Those functions include enterprise directory and NOS directory functions, public key infrastructure (PKI) and Kerberos security services, LDAP v3, and network device management capabilities (Figure 1). “In addition, Active Directory is built into the Windows operating system, sparing Cisco from paying a separate licensing fee,” says Beauchesne.

The strong relationship between Cisco and Microsoft also factored into the decision: In 1997, Cisco entered a strategic partnership with Microsoft to develop advanced network solutions based on Active Directory. Today, many Cisco products use Active Directory.

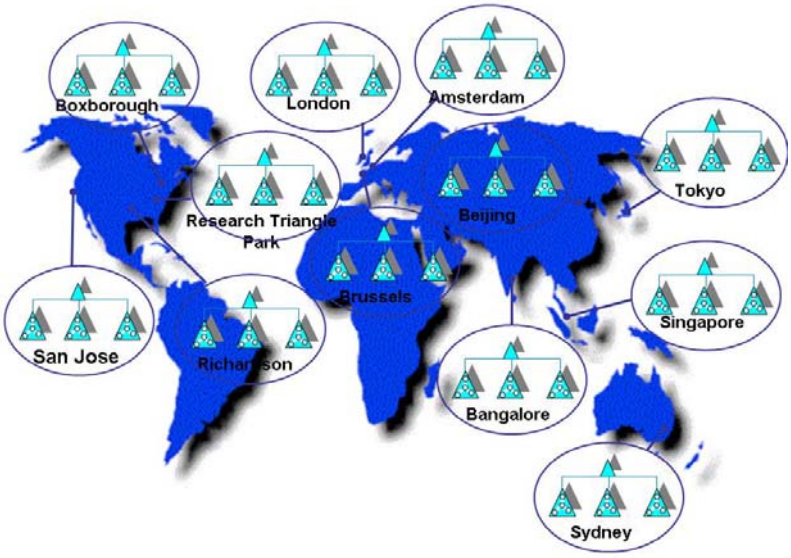
Figure 1. Microsoft Active Directory



Architecture

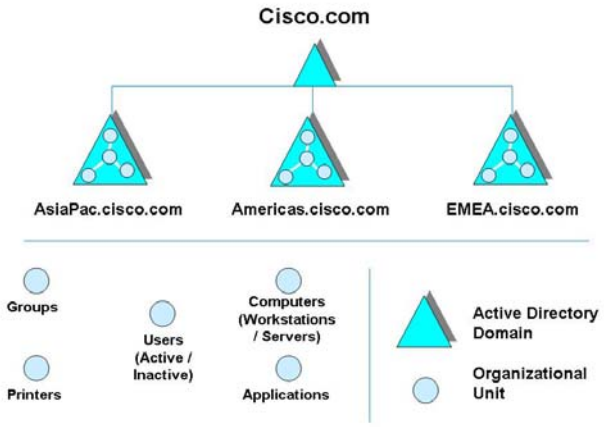
Cisco IT deployed Active Directory in 12 locations on Cisco's all-packet network (CAPnet), a global backbone on four continents (Figure 2). The sites have very high bandwidth, providing fast response as users in nearby offices attempt to access applications that invoke the directory service. "Latency is slightly greater than it would be if we deployed Active Directory domain controllers at every Cisco site, but not enough to justify the added security risk and the logistics of replacing failed servers," says Jones.

Figure 2. Active Directory Core Sites on Cisco Global WAN



Each Active Directory deployment site has five domain controllers—a root domain, three child domains based on geography (Americas; Europe, Middle East, and Africa (EMEA); and Asia Pacific), and a redundant domain for the local geography (Figure 3). For example, the Amsterdam deployment has an additional EMEA domain controller. "Placing geography-based domain controllers in each location makes it possible to locally authenticate Cisco employees who travel to other parts of the world, reducing latency," says Beauchesne. "We've reduced authentication time from minutes to seconds in some cases, which improves productivity and can prevent application timeouts."

Figure 3. Active Directory Architecture



All domain controllers also serve as Active Directory global catalogs, which provide a subset of object information and can be used to find information about users or devices if their domain is not known. To simplify administration, every domain controller is identical—an HP DL 360 server running Windows 2003.

Cisco IT needed to preserve at least a few separate instances of Active Directory—or “forests”, in Active Directory terminology. New applications that use Active Directory are tested first in the development forest, then in the staging forest, and are finally moved to the production forest. “We wanted to isolate our production, lab, and development forests,” Beauchesne explains. “There’s no need to provide our developer partners in other countries with access to our production environment, for example.”

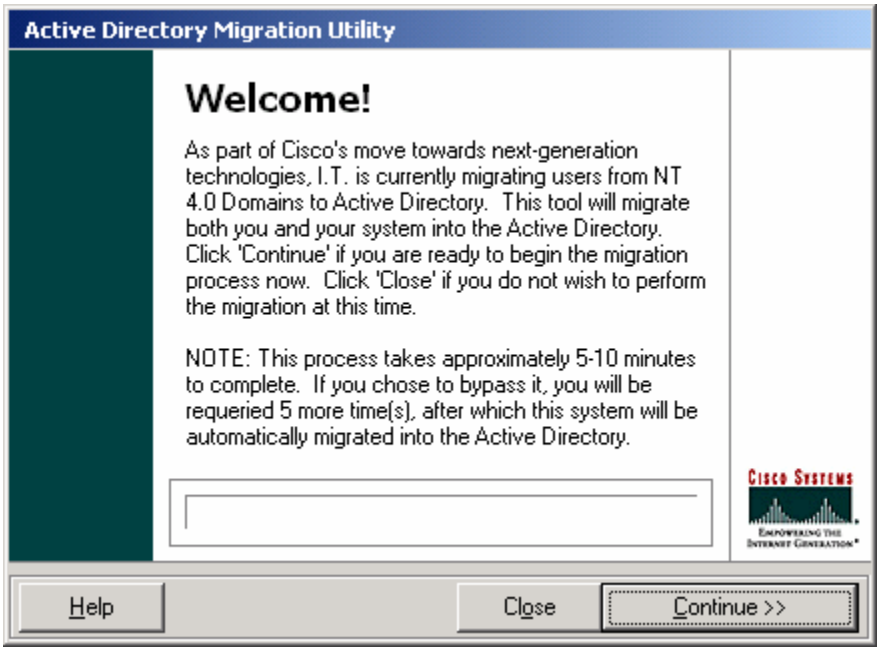
Automated Migration

Migrating from constantly used NOS directories to an enterprise directory without interrupting business continuity would be challenging—Jones compared it to jumping from moving car to another. “We wanted to automate the migration as much as possible, to minimize business risk,” he says. Automating the migration process would also cut costs. Gartner Group estimates that typical migration costs to a new directory service average $2000 to $3100 per desktop. With approximately 50,000 desktops, Cisco stood to save considerably by reducing the per-desktop migration cost.

A member of the Cisco IT team met the challenge by writing a utility to automate migration from the company’s previous Microsoft Windows NT 4.0 NOS directories to the new enterprise directory. Cisco IT ran the utility daily for seven months to populate user accounts in Active Directory, migrate group accounts from Windows NT 4.0 to Active Directory, and migrate security identifiers (SIDs). When a user logged into Windows NT 4.0, the script automatically performed the following actions (Figure 4):

- Enable the Active Directory user account
- Place the Active Directory account into the local administrator’s group
- Copy the Windows NT 4.0 account profile settings to the new Active Directory account
- Create a computer account in Active Directory
- Join the computer to Active Directory
- Set the user’s password in Active Directory
- Reboot the computer

Figure 4. Automating Migration from Windows NT 4.0 Directory to Active Directory



The utility wrote each action to a log file on the local machine. A rollback feature allowed for full recovery if a critical error occurred. “In fact, the utility migrated 99 percent of Cisco users to Microsoft Active Directory with no human intervention,” says Beauchesne.

Automated Provisioning

To ensure that Active Directory data remains current, approximately 100 batch provisioning scripts capture changes from the master database and execute daily at intervals ranging from 15 minutes to 24 hours. When needed, Cisco IT can provision Active Directory on demand. Jones characterizes the approach as “provision as much data as possible, master as little data as possible in Active Directory.” For user provisioning and lifecycle management, for example, Cisco used its existing Perl development environment to integrate Active Directory with PeopleSoft. When new employees are entered into the PeopleSoft system, they are automatically entered into a master database, and then provisioned to Active Directory. Similarly, when the human resources team updates PeopleSoft to indicate that employees have left the company, their Active Directory access accounts are automatically deactivated.

Figure 5 shows data that is automatically provisioned into Active Directory:

Table 1. Data Sources for Automatic Provisioning of Active Directory

Data Within Active Directory	Source
Employees	Feed from PeopleSoft
Groups	Windows NT 4.0
SID history	Windows NT 4.0
Mailboxes	Feed from database
Mail aliases	Feed from e-mail group
Printers	Feed from printer group
Site topology	Router config file repository
Schema extensions	Active Directory Schema Manager
Organizational units	Active Directory Forest Manager
Domain controller configuration	DNS settings, event logs setting, hot fixes

Automated Updates to Network Topology

An up-to-date network topology is an important feature of directory services—it helps IT staff find the fastest connection to a given network resource. “An incorrectly configured site topology can result in replication issues between domain controllers that affect the availability of directory-enabled applications,” says Jones. While Active Directory includes a facility to manage the network topology from within the product, it requires a manual update—not a viable solution for Cisco Systems, whose network changes daily. Cisco IT made the network topology feature of Active Directory more scalable by automating the update process. A Cisco IT team member wrote a script that pulls config files from Cisco routers daily to find the devices to which they connect and the speed of those connections, and then automatically adds this information to Active Directory.

Replication

Active Directory provides a capability called multimaster replication, which automatically replicates a change made anywhere on the network. For example, if an administrator at headquarters in San Jose adds a Cisco router in a domain controller, the change is replicated on all Americas domain controllers around the world. “The fact that we placed domain controllers on high-bandwidth CAPnet sites avoids bandwidth problems relating to replication,” says Jones.

To ensure rapid recovery during a disaster scenario, Cisco IT does not store master data in Active Directory itself, but in a separate database. “The main advantage of keeping the master separate is that we avoid the tragedy that would ensue if we lost a directory,” says Beauchesne. “In addition, maintaining a separate master database improves auditing and gives us greater control over which system administrators can make changes, and how often.”

Web-Based Proxy Management

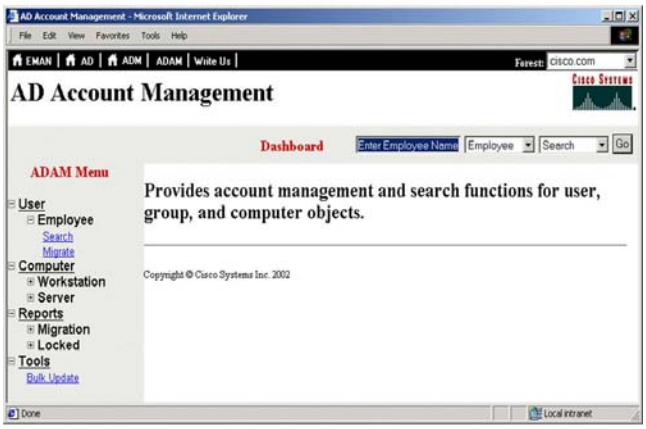
Local administrators sometimes make changes to the domain controller—for troubleshooting, for example—and then neglect to reverse the change. The unfortunate result is inconsistent server configurations, which complicate maintenance and troubleshooting. “To prevent changes to a local domain controller from disrupting the directory service, we decided that system administrators would access the domain controllers or the Active Directory application itself only by way of a Web-based proxy service,” says Jones. “The local configuration of applications or services would change on the server itself, and yet the actual Active Directory data would remain unchanged.”

To enable Web-based proxy management, Jones' team converted the Active Directory native controls into Web tools that Cisco developed internally. Using the Web-based proxy management of Active Directory, Cisco network administrators can:

- Manage accounts and search for users, groups, and objects (Figure 6)
- View and model the replication topology
- View and create schema extensions
- Manage Active Directory forest extensions across domains and servers

"Web-based proxy management is our way of delivering a globally distributed service through a centrally managed server," says Jones. "No matter where you are in the world, the Active Directory behaves the same."

Figure 5. Sample Screen for Web-Based Proxy Management of Active Directory



RESULTS

Rapid, Low-Cost Migration

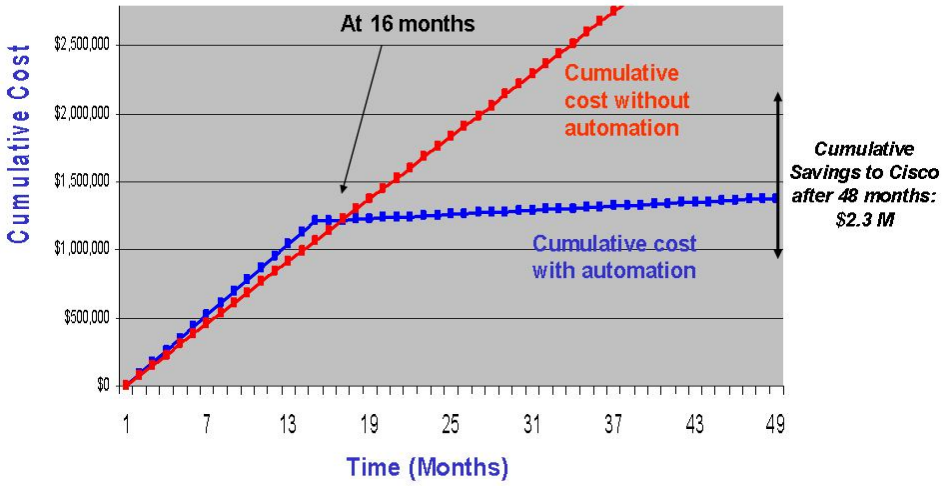
Cisco IT migrated approximately 41,000 users, representing 93 percent of employees, in just seven months, with limited staff resources. "Our automated migration script enabled us to migrate to Active Directory for $630 per Windows desktop, compared to an industry average of $2000 to $3100," says Beauchesne.

Return on Investment

As a result of automating directory updates with Active Directory and its own provisioning scripts, Cisco IT achieved ROI in just 16 months (Figure 7). Anticipated 48-month savings include:

One-time migration cost savings from automated migration tool:	$1.5 million
Ongoing operational cost savings for Windows services:	$2.3 million
Ongoing operational cost savings for UNIX services:	$2 million compared to SunOne or $4.3 million compared to Sun Network Information Service (NIS+)
Total 48-month savings:	$5.8–8.1 million

Figure 6. AD Automation ROI in 16 Months



Deployment of Cisco Unity Voicemail

Cisco Unity® voicemail and unified messaging services work in conjunction with Active Directory. Therefore, after deploying Active Directory, Cisco IT was able to extend Cisco Unity unified messaging throughout the company. Now Cisco employees can check both e-mail and voicemail from either of those inboxes, improving responsiveness and productivity.

NEXT STEPS

Cisco has completed the decommissioning of the Windows NT 4.0 directory, and is in the process of decommissioning MeetingMaker and the POP mail server directories.

LESSONS LEARNED

According to Beauchesne, the chief lesson learned is, “the fewer domains, the better.” When Cisco IT first deployed Active Directory, it configured four user domains—North America, Latin America, EMEA, and Asia Pacific. The rationale for multiple domains was to stave off bandwidth problems resulting from replicating objects like employee photos across the Cisco global WAN. The problem never materialized. “Because we deployed servers in central sites, we have more than adequate bandwidth,” says Jones. “In fact, maintaining separate domains caused problems because certain applications are not domain-aware—that is, they don’t understand having users in multiple places. That’s not an issue if you’re using Active Directory as a NOS directory, but if you’re using it as an enterprise directory, a single domain is preferred.”

FOR MORE INFORMATION

To read the entire case study or for additional Cisco IT case studies on a variety of business solutions, visit Cisco on Cisco: Inside Cisco IT www.cisco.com/go/ciscoit

NOTE

This publication describes how Cisco has benefited from the deployment of its own products. Many factors may have contributed to the results and benefits described; Cisco does not guarantee comparable results elsewhere.

CISCO PROVIDES THIS PUBLICATION AS IS WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Some jurisdictions do not allow disclaimer of express or implied warranties, therefore this disclaimer may not apply to you.

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Europe Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: +31 0 800 020 0791
Fax: +31 0 20 357 1100

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at **www.cisco.com/go/offices.**