

APPLICATION NOTE

April 2006

Identity-Enabled Information Lifecycle Management (ILM)

ABSTRACT

Information Lifecycle Management (ILM) has long focused on the one-way migration of data from high-cost media to less-expensive storage options. Identity-Enabled ILM takes data management to a new level by introducing data access based on organizational identities and support for bi-directional information flow. This paper describes Identity-Enabled ILM and Sun's rollout strategy.

- 1 Executive Summary 2
- 2 Introduction 2
- 3 New approach to ILM 2
- 4 Access Rights 3
- 5 Bidirectional Data Flow 3
- 6 Portfolio for Identity-Enabled ILM 4
 - 6.1 Step 1: Leverage Core Technologies to Control Data Access 4
 - 6.1.1 On-boarding 4
 - 6.1.2 Change 5
 - 6.1.3 Departure 5
 - 6.1.4 Reporting 5
 - 6.2 Step 2: Improve Data Trust 5
 - 6.2.1 Granular security at the file level 5
 - 6.2.2 Identity-based storage monitoring (integration with Identity Auditor) 5
 - 6.2.3 Reporting 5
 - 6.3 Step 3: Improve Data Value 6
- 7 Summary 6

1 Executive Summary

Information Lifecycle Management (ILM) has become well known in the last several years. But organizations are finding that simply adopting ILM is not enough. To provide more secure, cost-effective access to data, the next phase in ILM maturity is the development of “Identity-Enabled” ILM.

Identity-Enabled ILM links data access to specific roles within an organization. It adds the idea of a *user* lifecycle to that of the *information* lifecycle. Users will require access to different information as they move to different positions within an organization. Sun solutions, such as the Identify Management and Automated Data Manager software, can link these roles to appropriate data automatically.

Identity-Enabled ILM also addresses the need to bring data back from archival media to “active duty.” Increasingly, data is not sent to the archives to die; it may need to be accessed for business or audit purposes at any time. This bi-directionality is an important new data management concept.

This paper introduces Identity-Enabled ILM, provides information about Sun’s supporting portfolio, and outlines Sun’s strategy to roll out this methodology.

2 Introduction

Today’s organizations face a myriad of IT challenges, including managing data growth, protecting data, and simplifying data management; all while attempting to reduce IT costs. Recent breakthroughs in Information Lifecycle Management (ILM) have provided part of the answer. However, today’s ILM strategies solve just part of the problem.

Most ILM approaches focus on static tiers of storage, and do not take into account the dynamic, bidirectional nature of data access. Perhaps more importantly, today’s ILM methodologies do not have enough emphasis on data security. Any discussion of security focuses on encrypting data, but there is no emphasis on effectively controlling access to data throughout its entire lifecycle.

Sun addresses these problems with Identity-Enabled Information Lifecycle Management. Identity-Enabled ILM is designed to make data management more cost-effective and compliant while making sure that data is secure and available. It makes sense for today’s data-intensive enterprises, introducing an identity-driven approach to controlling and accessing data throughout its lifecycle.

3 New approach to ILM

Identity-Enabled ILM goes far beyond data security, taking into account the way data is really used, shared, and accessed by today’s enterprises. Sun’s blueprint for Identity-Enabled ILM provides streamlined, automated data control over long periods of time. It can reduce storage and operating costs today and will enable greater use of stored data in the future.

Identity-Enabled ILM brings *value* to the storage environment, helping to optimize data flow and address compliance issues. It ties access rights to user identities and IT policies, so the right people have access to the right data — at the right times in their career lifecycles. It maintains *simplicity* in the data environment through automation and data consolidation. And it provides a simple mechanism for ensuring the *trustworthiness* and security of corporate information, integrating Identity Management, Data Management, and Compliance technologies from Sun to protect information by controlling access throughout its lifecycle.

Identity-Enabled ILM is designed to make data management more cost-effective and compliant while making sure that data is secure and available.

Identity-Enabled ILM focuses on lifecycles — not just data, but users. Organizations can automate employee data access as they rise from the stockroom to the boardroom.

The key to Identity-Enabled ILM is its focus on lifecycles — not just *data* lifecycles but also user lifecycles. How should data be handled at various stages of its life, and how should access to that data be modified as data users move through various stages of their careers? Identity-Enabled ILM makes sure that data is handled appropriately and securely while making sure the data is stored in the most cost-effective way at every stage.

Identity-Enabled ILM speaks volumes about our core philosophy at Sun — a holistic, big-picture philosophy that rethinks the relationship between information and the people who use it. Below are some key considerations for understanding its potential.

4 Access Rights

ILM was originally created in response to a valid need; namely that data should be managed differently at different phases of its lifecycle. While it has vastly improved data management, traditional ILM has limitations:

- It focuses on tiered storage to reduce costs.
- Data movement across tiers tends to move in one direction, from primary disk to secondary disk or tape.
- Multiple separate products are required to classify, manage and move data. This is especially apparent in archiving and backups.
- It's focused on data migration and retention, but not data access.

One of the holes in today's ILM strategy involves access rights. This goes beyond “secure access,” which for many storage vendors means encryption. Encryption is an important aspect of data security and something that Sun does better than most, but controlling access to data with encryption keys is just a start.

Data must also be managed with regard to the access rights of individuals and applications. Who needs to have access, and why? Access rights take into account the roles and responsibilities of the people who generate and use the data, and make sure that access is being granted appropriately.

Over time, as these people move from job to job, from department to department or from company to company, access rights must also change to reflect their changing roles and responsibilities. Identity-enabled ILM provides the ability to tie enterprise roles to information lifecycle management. For instance:

- Automatic provisioning of user access rights and storage allocation can happen at the application level, file system level and device level to streamline access management, simplify compliance and improve data security.
- Audits can be conducted on applications, file systems and devices to validate business policies.
- Files can be automatically backed up and archived when a user separates from the organization.
- Information assets can be classified, secured and protected to prevent so-called “CNN Moments” when confidential information falls into the wrong hands.

5 Bidirectional Data Flow

ILM allows policies to be set so that data is moved to appropriate tiers of storage as it ages. Newly created data is kept on primary disk for fastest access, while older data is migrated to secondary storage or archived in long-term storage. This strategy is effective in reducing storage costs, allowing older data to remain accessible without using expensive primary disk to store it.

Security should mean more than encryption and passwords. Role-based data access provides an additional level of protection essential to modern compliance.

While ILM traditionally focused on one-way data migration, evolving needs often call for bi-directional flow. Sun StorEdge™ SAM-FS software addresses this need by caching data accessed from secondary storage and resetting the lifecycle clock.

The problem is that most ILM strategies move data in one direction only, from primary to secondary or tertiary storage. In a traditional ILM strategy, when data moves to tape, it stays on tape, even if the data goes active again. When users recall a file, they are either accessing it on tape and getting less-than-optimal performance, or they make a new “active” copy of the file, contributing to data sprawl.

Identity-Enabled ILM addresses bidirectional data flow with Sun StorageTek™ SAM FS storage archive and management software. With this technology, data is migrated to secondary storage as it ages, and is brought back into disk cache whenever it’s recalled. Just the act of accessing data allows authorized users to changes the data’s classification from “dormant” to “active.” When data files move into disk cache, the lifecycle clock is reset, and the file is subject to the same migration policies as other active data. Thus SAM-FS allows customers to manage information based on its ever-changing value to the business.

The bidirectional flow of data also drives the need to control access rights to the data as it is migrated to different resources or placed on compliant devices. For example, once regulatory data is stored on a compliant device, even the original owner may not change it, so the owner’s access rights must be modified the moment the file is saved. Similarly, if a content creator leaves the company or moves into a new position, access rights to original files may need to be limited.

6 Portfolio for Identity-Enabled ILM

With a portfolio of identity products, operating system products, storage products, and server products, Sun is uniquely positioned to deliver Identity-Enabled ILM solutions in a phased rollout:

Figure 1. Phased rollout stages for identity-enabled ILM.



Sun products simplify the association of privileges and identities at all levels. Also, you can link access and reporting to all stages of employment, from on-boarding to departure.

6.1 Step 1: Leverage Core Technologies to Control Data Access

The first step in delivering Identity-Enabled ILM is to improve data access. This is accomplished by simplifying the way access privileges are provisioned at all levels. Out of the box, Sun identity management products provide workflow templates to automate how storage is provisioned and how users will access their data. Here are some examples:

6.1.1 On-boarding

- Automatically allocates storage when a user comes on board
- Provides access to file systems
- Provides role-based storage allocation and data control

6.1.2 Change

- Ties enterprise role-based access to user's data
- Provides time-based access to information and corporate data
- Changes a user's data access as job role and organizational relationships change

6.1.3 Departure

- Automatically initiates backup/archive of user's data (workflow and retention will vary based on user security level)
- Automatically terminates access

6.1.4 Reporting

- Provides visibility into who has access to data based on sensitivity (highlights excessive access violations and erroneous aggregation of privileges)
- Links users directly to the information they create and access

Proof point: Identity Manager has workflow templates to automatically trigger backup jobs to archive a user's file system data when the user departs the organization. This feature reduces storage cost by expediting the movement of data to lower cost storage tiers. It also improves security by eliminating access to dormant data. Customers have worked with our professional services organization to automate these actions via scripts utilizing the Identity Management and Automated Data Manager software (formerly SAM-FS). Sun will work to incorporate this functionality into the products in the future.

User authentication is simplified with a common storage management portal providing role-based, single sign-on across many of our data management products. In addition, Sun StorageTek™ software products will leverage Sun-developed technology including Access Manager, Java Authentication and Authorization Service (JAAS), and Pluggable Authentication Module (PAM) to provide highly secured access management.

Proof point: Sun has integrated the role-based, single sign-on functionality from the IDM solutions into the StorageTek Enterprise Storage Management Portal. The ESM Portal allows users to manage the entire storage environment from a single integrated console. The integrated single sign-on functionality ensures that only those users with the appropriate access rights (beyond password authentication) will have access to critical business information and can perform critical tasks such as zoning and provisioning.

6.2 Step 2: Improve Data Trust

To ensure the trustworthiness of data, there must be indisputable evidence that the data is secured through access control and/or encryption, and that it is protected with adequate backup and/or archive procedures.

6.2.1 Granular security at the file level

- ESM Integration
- SAM-FS Extensions
- Improves security and access tracking

6.2.2 Identity-based storage monitoring (integration with Identity Auditor)

- Monitors storage access and activities to maintain integrity
- Provides forensics into what users are doing

Sun provides a role-based, single sign-on portal across many of our data management products.

Sun products include numerous checks to ensure data security, ranging from encryption to tracking and reporting on individual events in the life of a file.

6.2.3 Reporting

- Indicates who has done what to information, and manages risk
 - Indicates if users have tampered with sensitive data
 - Tracks changes in emergency access cases

Proof point: Identity Auditor ingests 5310 Compliance Archive log files and validates that data usage patterns match policy regulations. This functionality is critical to ensuring true compliance — organizations not only can control who has access to the data but can monitor the activities and behavior of the users that have access. An administrator that is accessing the compliant data in an excessive manner may in fact be attempting to alter or copy that data. This solution ensures a level of granular security that goes far beyond traditional compliance and security methods.

6.3 Step 3: Improve Data Value

To get the benefits of ILM, data must be classified into logical groupings. Mapping metadata to business objects and business processes can be a daunting challenge. What's more, customers often have a difficult time quantifying the cost associated with the different storage tiers and an even more difficult time determining charge-back costs to users.

By integrating application-level roles, responsibilities, workflow, data access privileges, and data retention policies with storage-level data access features and policy management, customers can potentially use Sun technologies to optimize data flow and ensure total data compliance. By further leveraging the integration of Identity Management with Enterprise Storage Manager, we can provide reports to determine cost of storage tiers and the charges to individual users or groups. These reports are key to helping managers understand how to better manage storage and link people, technology and processes in a bid for continuous improvement.

7 Summary

Sun provides the first solution for Identity-Enabled ILM, allowing organizations to better manage rapidly growing amounts of data. The solution combines Sun's industry-leading products for Identity Management and Data Management.

By adding the dimension of *who* (identity) to *what* and *when* (the information lifecycle), Sun's identity-enabled ILM solution gives organizations more control over how people manage and access their data — the only way that organizations can get ahead of data sprawl. Organizations can now manage data by identity to reduce storage costs, strengthen compliance, and make data more valuable because it can be securely shared with more people for more uses.

Sun's solution puts data in its place, allowing people to make the most use of it for productivity and collaboration, regardless of the application platform that originated the data.

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA **Phone** 1-650-960-1300 or 1-800-555-9SUN **Web** sun.com



© 2006 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Enterprise Storage Management Portal, Activity Auditor 5320, SAM FS, GSM, Identity Auditor, Access Manager, Java Authentication and Authorization Service (JAAS), Pluggable Authentication Module (PAM), 5310 Compliance Archive System are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries.

JT 0036 A 04/06