IBM Security Directory Integrator

Simplifying identity silos and cloud integrations

Highlights

- Build a single authoritative directory by transforming, migrating and synchronizing identity and generic data from heterogeneous sources
- Solve virtual directory use cases by helping prevent slow data sources from becoming bottlenecks
- Simplify cloud management with support for the System for Cross-domain Identity Management (SCIM) standard
- Use as a directory repository to create an end-to-end directory service solution that can support hundreds of millions of entries
- Support identity store browsing with included IBM Directory White Pages application

Even on today's smarter planet, many organizations have no single authoritative directory. Instead, they deploy department-specific applications at all levels of the organization, resulting in dozens of application-specific directories that may contain related—though not identical—data. With accounts spread across heterogeneous applications and services, it can be difficult to identify and resolve conflicts among all the sources of identity or generic data—such as when a user's job title (and related permissions) is changed in one application but not in others, or when a data file is modified on a distributed server in a complex environment. Inconsistencies like these—when an employee leaves, for example—increase the potential for security breaches and audit failures.

Maintaining data consistency across multiple data repositories requires the ability to synchronize information quickly and efficiently. If an employee's name changes, for example, changing the status in one information store should initiate the same change in other stores across the organization.

IBM® Security Directory Integrator offers both small and large organizations a cost-effective way to synchronize heterogeneous identity and generic data sources and build an automated, authoritative data infrastructure. By enabling organizations to maintain consistent and trusted data across multiple identity or generic resources, Security Directory Integrator can help users leverage emerging, on-demand business models.

Synchronize data across applications and directories

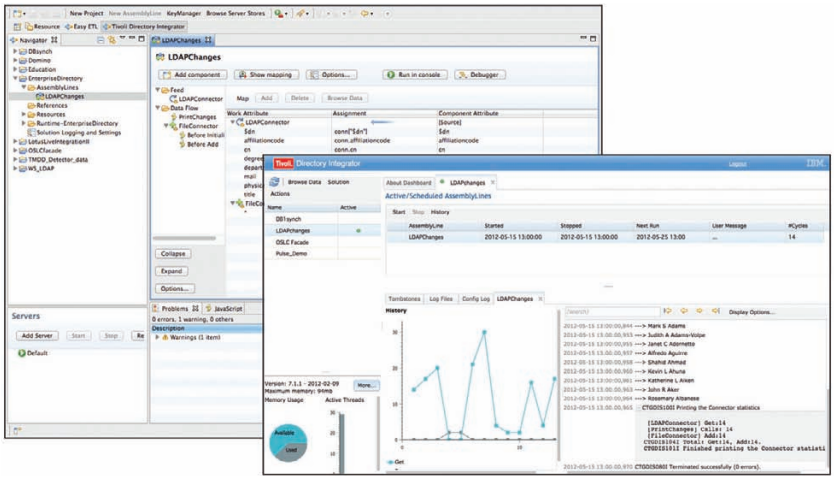
Security Directory Integrator helps create a single authoritative source of data residing in silos in various sources such as databases, directories, files and applications. Using configurable business rules, identities can be correlated to reconcile data from various data sources and create a unique set of data. This solution also helps solve various virtual directory use cases with a hybrid approach: It creates a centralized data store, but still provides the capabilities to manage and authenticate users at the original sources where they were created and continue to be maintained.

Security Directory Integrator helps rapidly deploy various applications, such as IBM Security Access Manager and enterprise White Pages, through a single point of access. By using the highly scalable IBM Security Directory Server infrastructure as the backbone, applications can meet almost any service-level agreement, even if the original data source is slow.

When an authorized user makes a change to a data source, such as a human-resource application or a telephone directory, Security Directory Integrator automatically detects the change and propagates it to the appropriate system. The flexible and agentless architecture enables users to create an up-to-date, single, authoritative data source or use it for point-to-point integration. Security Directory Integrator also includes a scalable, industrial-grade, v3-compliant Lightweight Directory Access Protocol (LDAP) store to provide back-end support.

Automate and integrate identity data to help reduce costs

Security Directory Integrator helps organizations build an authoritative identity data infrastructure to help optimize security and provide the trustworthy data required for cost-saving IT automation. With Security Directory Integrator in place, the user identity data that applications require is updated automatically when the authoritative data sources are updated—even if that source is managed by another application in a different repository.



IBM Security Directory Integrator uses a hybrid architecture to create a single, authoritative view of identities. It provides virtually unmatched scalability and performance as well as distributed authentication to support fragmented ownership.

The flexible architecture enables both meta-directory as well as point-to-point integrations. As a meta-directory, Security Directory Integrator synchronizes data that resides across IBM and non-IBM directories, databases, password stores, collaborative systems and applications. Consequently, it helps organizations maximize the accuracy of the data they maintain and reduce the costs associated with manual updates. When an authorized user makes a change to a definitive data store, such as a human-resources application or a telephone directory or private branch exchange, Security Directory Integrator automatically detects the change and pushes the modification out to all the other databases and applications that store and use the same data.

Unify identities across systems

Security Directory Integrator is a complete solution that provides everything organizations need to integrate identities, with capabilities that range from creating a single, authoritative data source to implementing point-to-point integration. Security Directory Integrator is offered in two versions. While sharing identical functionality, IBM Security Directory Integrator Identity Edition is available as user-based licensing, while IBM Security Directory Integrator General Purpose Edition is offered as processor-based licensing.

Security Directory Integrator includes Security Directory Server, which provides a robust LDAP server that enables organizations to create virtually any type of high-performance scalable integration. Security Directory Integrator includes features such as:

- **Federated Directory Server**—This feature helps create a single authoritative data source by integrating and correlating identities located in directories, databases, files, applications and more. Federated Directory Server:
  - Creates a centralized data store of data silos while federating authentication to the original data sources, enabling organizations to preserve their existing processes for managing users and passwords.
  - Helps rapidly deploy enterprise-wide applications, such as Security Access Manager and White Pages, through a single point of access.
  - Provides identity correlation and attribute transformation to help ensure that authoritative data is consistent across various existing data systems.
  - Enables data augmentation from other sources.
  - Eliminates the need to modify existing systems, since integration is applied on top of existing resources.
  - Provides a modern browser-based user interface as well as a rich set of integration capabilities.
  - Enables the creation and management of groups across multiple sources.
- **White Pages**—This application helps create an organization's hierarchical structure on top of the authoritative data source. It is based on the Profiles component of IBM Connections, an application that includes social-networking capabilities.
- **User Management in Cloud**—This SCIM implementation helps to on-board and off-board user identities in cloud environments.
  - SCIM supports user management in the cloud through a Representational State Transfer (REST) interface rather than through traditional LDAP protocol.
  - SCIM client connector enables Security Directory Integrator to read and write to a system that provides a SCIM interface.
- **Auditing and reporting**—These features provide insight into user activities. Built-in integration with IBM Security QRadar® SIEM allows deep correlation of user activities. Sample reports are also included to help simplify management.

Flexibly connect resources and respond to changes

Security Directory Integrator provides a flexible, open architecture that allows users to synchronize data sources already in place. A dynamic synchronization layer between the data

structure and the applications creates flexibility by eliminating the need for an intermediate proprietary data store. If an organization requires a centralized meta-view, Security Directory Integrator can synchronize to any IBM or non-IBM data store—unlike competitor solutions that require their own proprietary architectures. For organizations that choose to deploy an enterprise directory solution, Security Directory Integrator helps ease the process by connecting to identity or generic data from various repositories throughout the organization.

To enable rapid deployment and easy extension, Security Directory Integrator uses multidirectional data flows called AssemblyLines, based on an incremental, component-based methodology. AssemblyLines can be shared, pooled and reused across all Security Directory Integrator solutions deployed within an organization. Security Directory Integrator solutions can dynamically alter their configurations and behaviors at run time based on external properties, and provide asynchronous communications that can drive work between multiple AssemblyLines—and across multiple servers. Built-in connectors and parsers allow users to integrate a wide range of systems. Security Directory Integrator supports most standard protocols, application programming interfaces (APIs) and formats, including:

- Extensible Markup Language (XML) and JavaScript Object Notation (JSON)
- Java Database Connectivity (JDBC)
- LDAP
- Java Message Service (JMS)
- Java Naming and Directory Interface (JNDI)
- HTTP/REST
- Web services

To flexibly respond to system changes, its event-driven engine enables real-time change detection, transformation and modified data propagation to other systems. Events can include arriving emails, records updated in databases or directories, incoming HTML pages from a web server or browser, arriving web services-based Simple Object Access Protocol (SOAP) messages, and other types of events defined by users.

Changes can be detected and extracted from:

- Files in XML, LDAP Data Interchange Format (LDIF), comma-separated values (CSV) or custom formats
- IBM Domino® or IBM Notes®
- IBM Security Directory Server
- Microsoft Active Directory
- Oracle Directory Server Enterprise Edition (formerly known as Sun Java System Directory Server)
- IBM Security Directory Server for IBM z/OS® on IBM System z®
- Relational database management systems that include IBM DB2®, Oracle, Microsoft SQL and custom systems
- SAP enterprise resource planning (ERP) systems
- IBM Maximo® software
- Custom data sources, using built-in delta-detection services

Take advantage of fast, simplified installation and management

Security Directory Integrator provides an easy-to-use graphical development tool and web-based management console. The administrative management console simplifies monitoring of AssemblyLines into a single view. A library of prebuilt components, such as connectors, parsers, password interceptors and event-handling mechanisms, allows Security Directory Integrator to integrate into a wide variety of environments with minimal disruption. Plug-and-play functionality helps to drive quick time to value as the components facilitate rapid prototyping and implementation.

Additionally, the open framework based on Java technology enables the extension of virtually all of the integration components and provides easy access to a range of management tools that enable administrators to perform system configurations and send real-time notifications to external applications. The Action Manager application, integrated with the administrative management console, enables high-availability deployments by monitoring Security Directory Integrator solutions and triggering customized actions, allowing administrators to quickly add failure detection, response features and customized health monitoring.

Benefit from flexibility in Security Directory Integrator

The flexibility of Security Directory Integrator enables it to be used in a wide range of scenarios. The following examples demonstrate how Security Directory Integrator can add value to an organization's infrastructure.

One common problem shared by many organizations is the presence of numerous sources of identity data. Sometimes, a business need can require an organization to establish a new directory that is continuously maintained with information from the sources as data is modified there. Other times, the need may require all systems to have a minimum amount of information from all the other systems. Business needs will dictate the technical approach. In both scenarios, however, Security Directory Integrator can be used to detect changes in all systems, properly transform data to match the requirements of each individual system, and ensure that valid data is propagated in near real time.

In another common scenario, data may need to be augmented with related data in another system. When an organization plans to create a web-based application for both employees and customers, several concerns must be considered. The externally facing application will most likely have its own authentication service in the demilitarized zone (DMZ) that is securely separated from the existing internal security systems. However, it needs to contain information about all employees, as well as customers. Furthermore, it is quite possible that additional information from internal ERP systems needs to be added to the user accounts. This might include customer details or internal organizational structures that enable the application to handle workflows correctly. In this scenario, Security Directory Integrator can securely place employee information into the externally facing directory while creating new passwords for them, and can automatically send email to the employees with login credentials to the new enterprise application. Information from ERP systems can be extracted, augmented and added to the customer data in the same directory.

Why IBM?

IBM has designed Security Directory Integrator to be easy to use, easy to deploy and able to generate a rapid return on your investment. Security Directory Integrator provides the flexibility to scale from small to very large deployments.

Security Directory Integrator is designed to complement security solutions like IBM Security Identity Manager and IBM Security Federated Identity Manager for user provisioning, delegated administration and federation. It also helps with rapid deployment of IBM Access Manager. Through tight integration with other IBM infrastructure software—including IBM WebSphere®, Domino and Connections middleware—and infrastructure management products such as IBM SmartCloud® Control Desk and IBM Tivoli® Application Dependency Discovery Manager, Security Directory Integrator can help your organization build the real-time, authoritative data foundation it requires for on-demand services.

IBM Security Directory Integrator at a glance

Supported platforms:*

- IBM AIX® v7.1 and IBM Power Systems™ v6.1
- Microsoft Windows Server 2012 Standard
- Windows Server 2008 R2 Enterprise Edition
- Red Hat Enterprise Linux 5 Advanced Platform 64-bit, v5
- Red Hat Enterprise Linux Server 64-bit, v6
- SUSE Linux Enterprise Server 64-bit, v11/v10
- Red Hat Enterprise Linux Advanced Platform for z/Series 64-bit, v5
- Red Hat Enterprise Linux Server for z/Series 64-bit, v6
- SUSE Linux Enterprise Server for z/Series 64-bit, v11/v10
- Oracle Solaris for SPARC v10 and v11

For more information

To learn more about IBM Security Directory Integrator and other software solutions from IBM, contact your IBM representative or IBM Business Partner, or visit: **ibm.com**/security

About IBM Security solutions

IBM Security offers one of the most advanced and integrated portfolios of enterprise security products and services. The portfolio, supported by world-renowned IBM X-Force® research and development, provides security intelligence to help organizations holistically protect their people, infrastructures, data and applications, offering solutions for identity and access management, database security, application development, risk management, endpoint management, network security and more. These solutions enable organizations to effectively manage risk and implement integrated security for mobile, cloud, social media and other enterprise business architectures. IBM operates one of the world's broadest security research, development and delivery organizations, monitors 13 billion security events per day in more than 130 countries, and holds more than 3,000 security patents.

* For detailed system requirements and additional information on each operating system, visit: **ibm.com**/infocenter/prodguid/v1r0/clarity/index.html

IBM Corporation
Software Group
Route 100
Somers, NY 10589

Produced in the United States of America
December 2013

TID14028-USEN-02