Modernizing Legacy Directory Servers

TECHNICAL BRIEF

Legacy directory servers make it nearly impossible to keep up with today's identity and access management (IAM) requirements. Having seen no major innovation for more than a decade, they're missing many modern IAM features and leave bloated and costly hardware footprints. Plus, many systems like Oracle/Sun Directory Server Enterprise Edition (DSEE) are now facing end-of-life support realities. Critical business and IT initiatives are being held back. The urgency to replace legacy systems has never been higher.

READY FOR A MODERN IDENTITY MANAGEMENT SOLUTION?

A modern directory server and identity management platform from Ping Identity can offer a quantum leap forward in performance, reliability and security while reducing costs and enabling faster time to market for new applications. These are necessities in today's IT environment that are impossible to achieve with prominent legacy directory servers such as Oracle/Sun DSEE.

	Ping Identity	ORACLE Sun
Proven 99.999998% availability in demanding enterprise deployments	✔	✖
Extreme performance and scale with hundreds of millions of identities	✔	✖
Significantly lower operational and support costs (25-90% less than legacy)	✔	✖
Versatility to deploy on-premises, virtualized or in the cloud	✔	On-premises Only
REST APIs and LDAP support	✔	LDAP Only
End-to-end data encryption and security	✔	✖
Support for structured and unstructured data	✔	✖
Bi-directional data sync across diverse data sources	✔	✖
Integrated load balancing	✔	✖
Extremely efficient IT resource usage	✔	✖
Ongoing product innovation and enterprise-grade product support	✔	?
Detailed operational performance monitoring and analytics	✔	✖
Reliable single or multi-master replication	✔	✖

TOP 5 REQUIREMENTS FOR A MODERN DIRECTORY SERVER

If you're evaluating a directory server and identity management platform, here are the key capabilities you should consider to address current and future needs

1. Extreme performance, scale and reliability

Support for a rapidly growing number of applications and engagement channels requires that an identity management solution does four things extremely well: 1) accommodate dataset growth, or the ongoing increases in the number of data objects that accompany user growth and digital engagement; 2) reduce latency, or the amount of time it takes to process operations against growing datasets, 3) increase throughput, or the rate of operations per second, even as the number of data objects is also increasing, and 4) provide carrier-grade high availability even through unexpected demand spikes.

2. Integrated end-to-end security

Keeping identity data secure requires a multi-tiered approach that protects data at rest, in motion between end points (from data store to application, for example), and data while it's in use in applications. To protect data at all three points, you need an integrated system of end-to-end encryption and authentication/authorization, as well as tools that govern data access and monitor data use.

3. Synchronization and unification of identity data

Synchronizing and unifying data across on-premises and cloud-based systems is the key to meeting today's identity data management challenges. To synchronize and unify data requires a directory server solution that makes it possible to easily do two things: 1) create a secure, centralized view of identity data across heterogeneous on-premises data sources, and 2) achieve secure bi-directional data synchronization (cloud-to-premise and premise-to-cloud).

4. Expose identity data to modern and legacy applications

Once you have a centralized, secure identity data store in place, the data needs to be exposed to the applications that need it. Existing applications may require LDAP support with up-to-date LDAP protocols. New applications and development teams often prefer developer-friendly REST APIs or SCIM. Supporting all of these protocols is crucial and will dramatically speed time to market for new applications and services.

5. Migration tools built specifically for legacy data stores

To migrate away from legacy data stores such as Oracle/Sun DSEE with minimal effort requires an identity management solution with tools designed specifically for these products. For example, the new solution should be designed to enable phasing out of existing LDAP directories with zero downtime and no client changes by automatically routing client requests to the appropriate directory server environment. It should also automate migration of existing configuration and schema to reduce manual effort.

QUESTIONS TO ASK WHEN EVALUATING SOLUTIONS

Does the solution have proven success in high-demand scale and performance use cases with enterprise customers?

Will the solution be able to support a zero-downtime transition to a new directory?

Will sensitive data be centrally secured while at rest, in motion and in use by applications?

How easy is it to install and configure? Does it offer command line and web-based configuration interfaces?

How versatile and extensible is the solution? Is there a Java SDK and support for LDAP, SCIM and REST API protocols?

What about platform support? Is your operating system supported?

Does it comply with industry standards? Is it compliant with LDAPv3 IETF RFCs, SCIM, 3GPP UDC and SPR specifications?

Prepare for Future Customer IAM Requirements

Customer identity and access management (CIAM) has now been clearly defined by analysts and is just around the corner for many organizations. CIAM can require you to store hundreds of millions of customer identities and adhere to more stringent data security and privacy regulations while providing features that go beyond traditional IAM requirements. Your transition may be closer than you think. Modernizing legacy directories now can better prepare you for the transition when the time comes.

Ping Identity

Ping Identity is the leader in Identity Defined Security for the borderless enterprise, allowing employees, customers and partners access to the applications they need. Protecting over one billion identities worldwide, the company ensures the right people access the right things, securely and seamlessly. More than half of the Fortune 100, including Boeing, Cisco, Disney, GE, Kraft Foods, TIAA-CREF and Walgreens, trust Ping Identity to solve modern enterprise security challenges created by their use of cloud, mobile, APIs and IoT. Visit pingidentity.com.

#3154 | 10/06 | v00b