

White Paper

Building a flexible, cost-effective, and durable identity infrastructure through virtualization

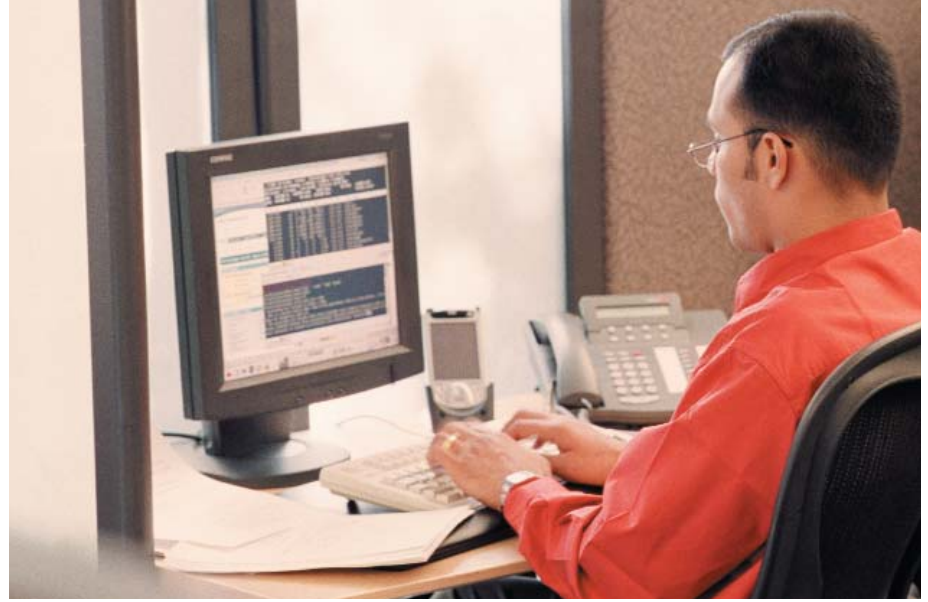
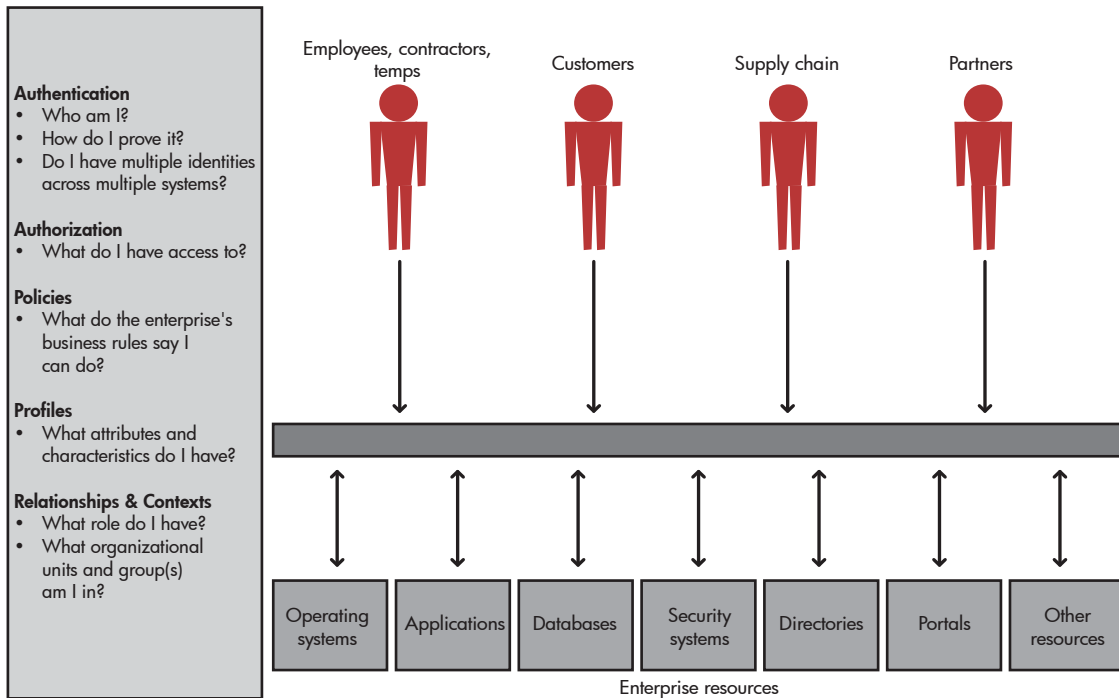


Table of contents

The challenges of Identity Management	2
What is Identity Management?	2
Limited choices for deployment	2
Directory services revisited	3
An inflexible approach	3
What is a Virtual Directory?	4
The Radiant Logic and HP solution	4
Benefits of Virtualization	4
The RadiantOne process for building an identity infrastructure	5
The Radiant Logic and HP Advantage	7





The challenges of Identity Management

What is Identity Management?

With the growing complexity of the enterprise infrastructure, organizations are wrestling with the challenges of managing secure access and administration of employee, customer, partner, and vendor identity across a wide range of systems.

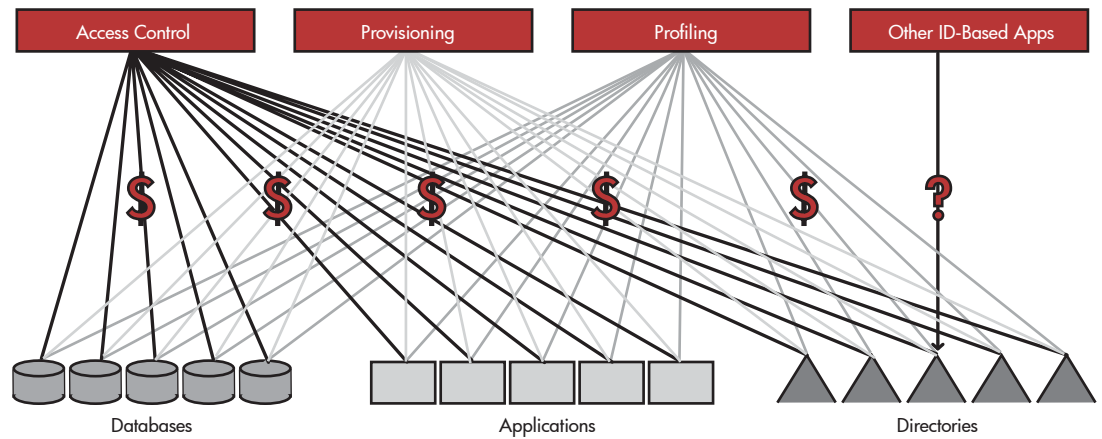
Managing multiple sources of user identities and security contexts across all of these applications is a daunting task. Identity Management is the convergence of functionalities, such as authentication, authorization, entitlement, delegated administration, user registration, and services provisioning. The purpose is to determine—electronically—who individual users are, what they can and cannot do, and how to automate the delivery or removal of a set of services to them based on well-defined business policies.

Limited choices for deployment

Unfortunately, achieving the benefits of identity management has proven to be quite elusive for many enterprises due to the lack of viable deployment options.

Many companies tried implementing a single identity management application, such as Web access control, and used ad hoc integration with existing sources of identity data. However, bypassing any sort of reusable infrastructure compounds complexity issues, creates a very tight coupling between data and application, and leads to more integration costs in the long term.

Trying to solve the infrastructure problem by leveraging an enterprise directory and using metadirectories or ad hoc synchronization for integration leads to many of the same problems. Until now, this approach has proven to be complex, expensive, slow to change, and time-consuming. Due to the inflexibility and complexity of the integration



process, it is a “solution” characterized by high costs, custom code, and long deployments.

The key to a successful implementation of Identity Management starts with a proper identity infrastructure—one that is more flexible than traditional approaches and transcends the problems associated with complexity. To meet the challenges and fully realize the benefits of Identity Management, an identity infrastructure must leverage existing identity information from various sources, tie it together, reconcile it, and provide it in the manner, format, schema, and structure that the various Identity Management business applications require.

Directory services revisited

It is clear that the directory services model is the right approach because it makes identities easy to access, but this alone is not sufficient. Any directory and application integration effort needs to reconcile two conflicting business requirements:

1. A durable and efficient Identity Management infrastructure must be able to cater to changing needs. Adaptability and flexibility are key in a world where business models and processes evolve continuously to match market demands. Security requirements are no different and are subject to the even more stringent constraints. Thus, a directory services solution model needs an integration layer in order to deliver the different identity views and contexts required by access management, provisioning, profile management, and other identity-driven applications.
2. At the same time, organizations rely upon an existing fixed set of applications and IT infrastructure that serves existing needs well and could not or should not be modified.

These two requirements have proven to be the choking point for most identity management projects. The layer designed with a central directory to reconcile the existing identity

information that is scattered across many applications has proven to be quite inflexible. Despite sizable investments in enterprise directory and metadirectory deployments, many enterprises have realized very limited results.

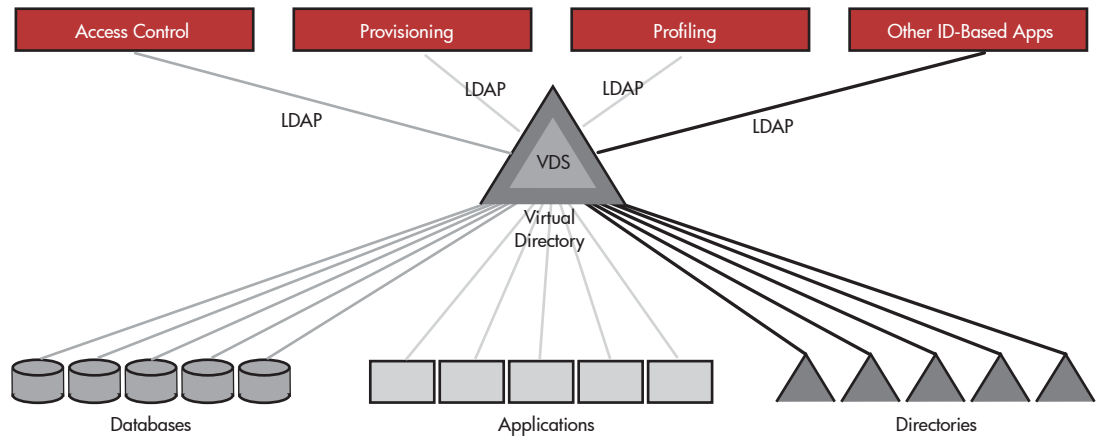
An inflexible approach that does not take into account the context of an operation

The problem is that most traditional directory integration technology, including metadirectories, are based on an approach that is static in nature. These first-generation solutions are too narrowly focused on the “object-to-object”, “attribute-to-attribute” synchronization aspect of the integration effort. That is, they copy some piece of identity information that resides in a specific application into a central directory. These functionalities are necessary steps of the integration process, but they are not sufficient by themselves.

You need a set of tools—such as those found in the Virtual Directory—that will reveal the complete picture of identity that is buried in existing applications. Even more importantly, the relationship between objects is ignored in current integration technologies because of a lack of “metadata” management. By ignoring relationships between objects, these integration technologies lose information about the context in which an operation occurred.

The capability to capture a global picture of the different application contexts—especially their security contexts—has completely eluded traditional approaches to directory integration. Focusing on synchronizing data from one location to another is like translating an article word by word. Similarly, ignoring context and relationships and not providing a full inventory and mapping of the metadata for an application is like skipping sentences in that article and hoping it will still make sense in the end.

In short, Identity Management requires an infrastructure that can combine on-demand, fragmented information sources with a set of common, shared identities stored in a logically centralized directory service.



Fortunately, a new approach to directory and application integration tools solves this dilemma. Based upon the concept of virtualization—a design philosophy that has been quite successful in operating systems, device drivers, networking, and backup—Virtual Directory technology is characterized by its exceptional flexibility.

What is a Virtual Directory?

A Virtual Directory is an adaptive middleware service that dynamically brings in information from existing data stores and makes it appear as a logical unified directory. It provides the shared context of a classical directory while extending the classical directory on the fly with attributes from existing application structures. A Virtual Directory allows you to

- Quickly simulate and emulate the directory environment and create what-if scenarios that quickly match the requirements of identity management applications with existing information from the current environment.
- Create a layer that integrates existing information and data with identity management requirements in a flexible, cost-effective, and durable way.

These principles provide the foundation for the RadiantOne platform.

The Radiant Logic and HP solution

You can take advantage of a standards-based approach to integrating applications and directory, and then accessing them through the new generation of virtualization—RadiantOne, the mission-critical Virtual Directory for HP platforms from Radiant Logic.

Based on J2EE-certified Java™ application servers from industry leaders, like BEA, that ease development, integration, and management tasks, and available on the fault-tolerant and highly scalable HP NonStop platform,

the RadiantOne Virtual Directory Server (VDS) maps heterogeneous data sources. VDS automatically converts schema and data into XML and LDAP objects through the process of virtualization; these objects can be easily organized into a flexible, adaptive directory hierarchy. The RadiantOne VDS aggregates data, and then organizes and presents that information through an LDAP-enabled directory structure to provide a critical integration layer for directories and applications. On a HP NonStop platform, RadiantOne offers additional mission-critical features not found in any current directory implementation: high throughput in terms of transactional writes and updates and advanced distributed cache management. A key advantage is that these operations can be done “on the fly” without changes to the existing application and data sources infrastructure (schema and data).

Benefits of Virtualization

Deploy new Identity Management business initiatives quickly and cost-effectively

With RadiantOne Virtual Directory Server (VDS), you can build a flexible layer for integration that makes it easy to add new Identity Management applications. RadiantOne’s virtualization technology allows you to deploy as many or as few directory views as needed. This enables rapid deployment of new business initiatives and means a significant time savings for your IT department, reduces the need for custom code, simplifies complex integration tasks, and boosts overall productivity.

The RadiantOne VDS solution provides built-in flexibility so you can avoid a “boil-the-ocean” implementation, instead deploying in a stepwise fashion and relying on one vendor for all platforms: HP supports Linux for smaller, departmental deployments; HP-UX for mid-size, divisional deployments; and the HP NonStop platform for mission-critical, enterprise-wide deployments.

Realize enhanced return on existing assets

Because adaptive enterprises seek to leverage the information already residing in existing applications—as well as provide access control for new initiatives—you need a solution that lets you take advantage of all the knowledge and business logic that's already part of the enterprise system, including proprietary applications. One of the main advantages of RadiantOne is its capability to provide a quick inventory of all existing identity data with its relevant contexts as they exist in their current application environments—often revealing potential security risks, such as accounts for former employees, orphaned accounts, or unreconciled identities.

Furthermore, virtualization provides an aggregation of otherwise fragmented information into meaningful business/process contexts and publishes this information in a directory structure. RadiantOne functions at the data server level of the overall business infrastructure, bringing together all pertinent data in a manner that every business application or initiative—old or new—can effectively use. With the RadiantOne VDS in place, companies have the infrastructure to leverage their existing investments in data. Without it, mining identity data from existing applications in a cost-effective manner is nearly impossible.

HP's years of experience providing solutions at the enterprise level enhance the system's ability to unlock information in existing applications and make it available to an identity-management system.

Reduce development and deployment time

RadiantOne virtualization technology replaces custom code-based integration by advanced meta-driven tools with all the benefits of off-the-shelf software in terms of cost and fast deployment time. Today's Fortune 500 organizations face the challenge and risks of bringing together information about customers or employees that's fragmented across numerous systems both inside and outside the company. Because the different pieces of information reside in applications with different schemas, data formats, and APIs (application programming interfaces), it's a formidable task to centralize this data. By virtualizing the data to make it dynamically available to every identity management application/initiative, RadiantOne VDS enables you to respond more completely and more quickly to customers, suppliers, partners, and employees—delivering a strong competitive advantage based on a durable infrastructure.

The HP platform supporting the RadiantOne solution is based on common industry standards, such as J2EE, providing maximum agility in development and deployment. Companies can leverage last-mile integration and customization from HP Services to further speed solution implementation.

Reduce deployment and management costs

Traditional LDAP directories require data to be extracted from the authoritative data source and transformed into a format matching the LDAP schema of the directory. The data is then loaded into the directory using Lightweight Directory Interchange Format (LDIF).

To maintain current information in the directory, you must repeat this process on a periodic basis. But the RadiantOne VDS does not hold any information in the directory itself, so there is no requirement to replicate or synchronize data. Instead, requests from LDAP clients return live data from the authoritative source; VDS manages schema transformation automatically.

Through server consolidation and the ease of managing a single system, the Radiant Logic and HP solution provides lower overall cost of ownership. You will realize guaranteed durability of your investment because the system supporting the Virtual Directory is based on industry standards.

Create a more flexible and durable infrastructure

Each identity management initiative has unique requirements for the underlying directory schema and tree. Existing directory solutions are rigid. Jonathan Penn of the Giga Information Group states, "When a directory's schema does not match what an application expects, one of them must change." Existing solutions require agreement from all users of the infrastructure, which leads to meeting upon meeting to determine the directory schema. RadiantOne provides the ability to create as many views of the data as necessary for the needs of all of the directory initiatives.

The RadiantOne process for building an identity infrastructure

Radiant Logic's proven process allows the components associated with Identity Management to be broken down into manageable tasks.

Building an identity infrastructure is a living process, constantly undergoing changes and updates. This is why it is important to have an infrastructure that is flexible to adapt to changing needs and reduces the amount of work it takes to perform changes.

The process for building an identity repository:

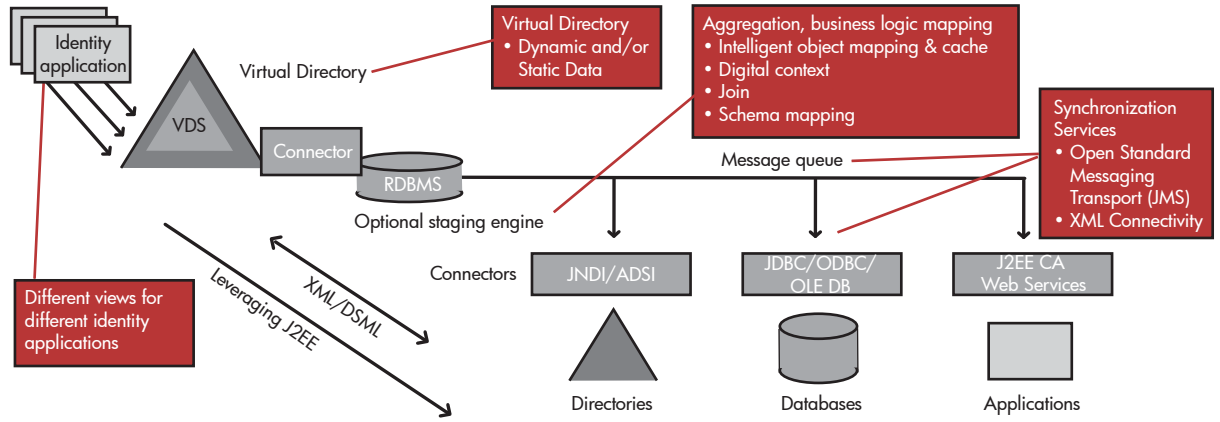
- Inventory—Take stock of your identity information and preserve existing relationships
- Organize and simulate—Assemble identities in a directory tree and test the design
- Integrate—Join identity information together and preserve the rich context from existing sources
- Deliver—Deliver identity to applications and users in the format they require

Step 1—Inventory

Tracking sources of identity information

An identity is the sum of all the information that defines a person, object, or service throughout the enterprise. Most identity information is already available, but not centrally located.

The first step for building an identity infrastructure is to inventory what is already available. An identity infrastructure should leverage and reuse available identity information instead of recreating existing information.



RadiantOne Schema Manager provides tools to capture the metadata that defines the structure of existing relational databases, directories, and applications. The structure of the database, the information inside, and the relationship of one set of objects to another set of objects can quickly be organized and accessed. Using RadiantOne Schema Manager, an administrator can take stock of what identity information is available, what information should be included (or excluded) from the directory tree, and build a common identity profile.

RadiantOne Schema Manager

- Provides a map of all identity schemas to a common format
- Is a GUI-based tool for easy editing and configuration
- Includes wizards and automated transformation for rapid deployment

**Step 2—Organize and simulate
Rapid design for fast turnaround**

Traditional directories force organizations to make hard choices. A directory tree structure built during the design phase ultimately becomes the one that is used, because that is the only one that is available.

With RadiantOne, your IT organization no longer has to feel tied to a bad directory design simply because of the time and cost involved in moving to a new one. RadiantOne Directory View Designer makes changing the tree easy, because tree design is separated from storing the data. After a tree structure has been constructed, it can be tested by simulation, giving administrators rapid turnaround to determine how the directory tree and entries look with live data.

RadiantOne DirectoryView Designer

- Provides an easy-to-use GUI-based tool for designing trees and entries
- Supports building multiple trees that can be used concurrently in Virtual Directory Server
- Constructs flexible, dynamic queries that map back to the existing identity sources

**Step 3—Integrate
Bringing identity together**

Different types of identity information require different levels of integration. For fields that change frequently, RadiantOne Virtual Directory Server supports direct access to databases, LDAP-enabled directories, and applications. Such information can be dynamically accessed, mapped, and integrated when it's requested, so the entry always stays up-to-date with the best available information.

RadiantOne Synchronization Services

- Create bi-directional links between the Virtual Directory Server and the sources of information
- Provides synchronization and change notification handled through Java Messaging Services

In an identity management repository, certain attribute types must be closely scrutinized, processed with business logic, and prepared before they can be used. In such cases, synchronization is required.

For example, to create a unique identity during integration (so that one identity isn't confused with another), some business logic is necessary to relate the fields to one another. However, you do not always know what information can be used to create uniqueness. In such cases, it would be prudent to synchronize those fields so that all of the unique identifiers can be analyzed first.

RadiantOne enables organizations to integrate identities dynamically or through RadiantOne Synchronization Services. Unlike other integration approaches that make synchronization the only option, RadiantOne allows you to make your own decisions, synchronize key attributes as necessary, and dynamically retrieve the rest.

Identity management solutions operate on a single instance of an identity, so the next step is to build a unique identity out of the various sources of identity information.

RadiantOne Unified Identity Manager enables designers to build a composite entry using the existing sources of data, so that the entry knows how to assemble itself. This means that an identity may have a Microsoft® Windows® system account name stored in Active Directory, an employee identifier from an HR database, and various other descriptors throughout the enterprise. The composite directory entry will know how to query the various sources to assemble itself dynamically.

RadiantOne Unified Identity Manager

- Provides tools to build a unique identity entry in RadiantOne Virtual Directory Server
- Applies business logic to determine how to assemble an identity that is located in multiple sources

Step 4—Deliver

Making identities available to applications

RadiantOne is a highly scalable, high-performance directory services platform designed to meet your enterprise requirements for identity management.

With the new RadiantOne LDAP Proxy load balancer, you can set up multiple instances of RadiantOne Virtual Directory Server to distribute load. In addition, RadiantOne Virtual Directory Server provides proxy features to make referrals to other directory servers, as well as being able to proxy authentication, using credentials from existing directories or databases.

RadiantOne Virtual Directory Server brings all of the identity information together and makes it broadly available into a directory tree. RadiantOne Virtual Directory Server allows you to rapidly construct a dynamic directory structure based on the information stored in your existing repositories.

RadiantOne Virtual Directory Server

- “On-demand” Virtual Directory structures and directory entries
- Intelligent caching
- Load balancing through proxy
- Support for open standards, such as LDAP v3, HTTP, XML

The Radiant Logic and HP Advantage

Mission-critical flexibility and availability

The RadiantOne VDS solution relieves your initial investment burden with built-in flexibility that enables stepwise deployment, so you use and pay for only what you need, supported by a complete platform from HP. You can start at the departmental level by implementing with HP on the Linux platform, upgrade to HP-UX as it deploys at the divisional level, and end up at the mission-critical enterprise level with the high-availability, 24 x 7 NonStop platform. HP NonStop servers incorporate unique technology that

allows them to withstand hardware and software failures while maintaining absolute data integrity. The servers stay up and running during routine maintenance and upgrades, support real-time remote backup for protection against environmental disasters, and provide instant and transparent recovery from outages.

The most scalable infrastructure platform available

An infrastructure solution demands an infrastructure platform that can support it, and HP and Radiant Logic have teamed up to deliver the most scalable Virtual Directory Server solution on the market today. The NonStop platform offers unstoppable availability and scalability, along with an open application development environment, Java technology-based tools, and support for just about any standard on the market. Combine this platform with Radiant Logic’s highly scalable and reliable directory services platform, and the result is extreme scalability, flexibility, and availability for even the most demanding enterprise applications and environments.

Leading directory application integration solutions

Radiant Logic is the leading provider of directory application integration solutions through virtualization. RadiantOne VDS delivers the identity infrastructure that accelerates the deployment of critical applications, such as security, profiling, and provisioning. By leveraging the business assets in your existing enterprise environment, RadiantOne can be deployed quickly in a stepwise manner to yield a substantial return on investment (ROI).

Industry-leading technology and performance

The RadiantOne Virtual Directory Server runs on HP platforms, including the NonStop fault-tolerant server that delivers typical network IN response times of 100 milliseconds, with the longest time frame taking approximately 300 milliseconds—which explains the solution’s extreme scalability and reliability and why it can grow so efficiently while taking up such a small footprint. To your network, the system appears to be a single service control point, instead of 8 or 16. This means a massive reduction in the cost of infrastructure and a significant advantage over traditional directory architectures.

HP Services

When HP stands behind your RadiantOne Virtual Directory Server, you can count on a single source for professional services, customer service, and other services. Built on more than 40 years of experience with a workforce of more than 65,000 service professionals and a global reach that extends into more than 160 countries, HP delivers complete solutions and support wherever they are needed. You purchase a turnkey solution complete with software, hardware, and comprehensive services because HP is committed to delivering end-to-end solutions backed by the reliability and innovation for which the company is known. That’s why the most successful enterprises rely on HP to make their businesses run.

For additional information, contact:

Radiant Logic

Phone: 415.209.6800 x150

Email: info@radiantlogic.com

www.radiantlogic.com

To learn more about HP's offering, visit www.hp.com

© 2003 Hewlett-Packard Development Company, L.P. The information contained herein is subject to change without notice. The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein. Microsoft and Windows are US registered trademarks of Microsoft Corporation. Java is a US trademark of Sun Microsystems, Inc.

5982-1295EN, 07/2003

