Infrastructure Applications

Catalysts for Directory Service Infrastructure

With the advent of the Lightweight Directory Access Protocol (LDAP) standard, many enterprises have come to recognize the value of basing their applications all on a consolidated, consistent Directory Service Infrastructure. However some enterprises are finding it hard to initiate the move into this valuable new technology, because infrastructure projects can be difficult to justify.

In the first place, infrastructure projects involve significant technical decisions that have to be explained to management. Even when the project manager is successful in explaining the technology, it is hard to generate any excitement among business managers for it.

Even more importantly, it is frequently hard to pinpoint the Return on Investment (ROI) for infrastructure projects. Application systems projects tend to be well aligned with business initiatives that have here-and-now returns; it is easy to identify ways in which those systems can share the returns for the business initiatives. However, infrastructure projects tend to support multiple applications, and tend to achieve their return over a long series of other projects. In these cases, the source of the return is much harder to identify.

Typically, infrastructure projects are justified in one of three ways: enumerating direct cost savings in infrastructure operations, such as reduced support staff; identifying future cost avoidance in application systems that will use the infrastructure; or simply getting funding from one or more application systems projects. However, there can be problems with these ways of getting support for projects. Direct savings in infrastructure may be inadequate; it is hard to generate much excitement in management and business leader ranks for technology investments. Future cost avoidance, while generally the largest factor in infrastructure value, seem to most to be further away, less tangible and less certain. And asking one application to pay for an entire piece of infrastructure may seem like “asking the first car down the road to pay for the turnpike.” Even if the application can afford it, it doesn’t seem fair.

Infrastructure Applications

One of the first users of a new piece of infrastructure may be an application-like system that is actually run by the infrastructure organization. This is the organization that is

responsible for technology, and may include data center operation, network operations, systems technical support, help desk, and like operations. Such applications tend to provide support capabilities to end-users. A typical such application in many companies is electronic mail. It is operated and supported by the infrastructure organization, but its end-users are found throughout the enterprise. Such applications are called *Infrastructure Applications*.

Packaging infrastructure applications with technology deployment to create an integrated project can have a wide range of benefits, and can help get an infrastructure project going. First and most simply, the application(s) may add return to the ROI equation. They may do this, at least in part, by streamlining some aspect of the infrastructure operation. In this case that organization also derives a benefit from the whole project. Most importantly, the end-user community gets some personal benefit from the new technology. They can see how it benefits them, and they can develop an understanding of its value. Lastly, other potential users of the technology have a model of its use and its value, which can accelerate the technology adoption.

Several infrastructure applications are surfacing as leading candidates to support a Directory Service Infrastructure project. Examples include:

- **White Pages**. The ability to look up phone number, e-mail address and other ways of locating a person.
- **Single Sign-On**. Providing end-users with a single point of access, where they are authenticated once and granted access to all of the data, applications and services for which they are authorized.
- **e-Provisioning**. Automated acquisition, delivery and set-up of equipment, facilities and security measures as a new employee is hired, or an existing one transferred.

White Pages

Most enterprises already have some sort of White Pages application. It is typically deployed on an intranet, but some companies have had such a system on their mainframes for years. However, there are several key differences between the first generation of such applications and modern, LDAP directory-based versions.

First of all, directories can consolidate information from many sources and serve all of it up. Thus directory-based White Pages applications tend to have far more information,

and consequently can provide far more ways of contacting an individual. In addition to name, e-mail address and phone number, a directory-based White Pages application can supply mobile phone number, pager number, internal mail address (mail stop), physical location, external mail address, and organizational unit.

Directory-based White Pages applications can also provide more functionality than early-generation versions. They can be structured to provide information about who is responsible for what function, or at least give a contact point for various functions in the organization (such access is called *Yellow Pages*). A directory-based approach also facilitates a reverse-lookup ("I know the telephone number, what is the name?"). Furthermore, if the organizational structure is included in the directory for supporting work-flow applications, the directory can provide access to organizational units in the enterprise (much like the government *Blue Pages* listing in a telephone directory).

With the extra information and the extra functionality, directory-based White Pages applications can provide more value. A directory can provide a consolidated, centrally managed repository of reliable information. It can be synchronized with Human Resources data, so that new hires, transfers and terminations are more likely to be incorporated promptly. Consistency of information is improved; for example, a user sees the same spelling of a person's name whether they are looking up a telephone number, an e-mail address or a pager number. Furthermore, end-users can use a single, consistent method of accessing any of the available information– a significant improvement over using different methods to access the information from each of the different systems that tended to hold it before it was consolidated in a directory. As applications begin using the directory, they too will get the same consistent information that the end-users get, reducing confusion and reconciliation time.

Single Sign-On

For years, the capability of having a single user name and password to log in to all of the applications, files and printers on a network was almost a holy grail: highly desirable, but never really attained. More recently, LDAP directories have demonstrated the technology necessary to support this capability. It is now possible to design an interface whereby an end-user logs in once to a central point on the network, and from there is given access to all of the appropriate applications, data and services.

The value of Single Sign-On is so great that it has been the single justification for an enterprise directory service in some enterprises (although if improperly architected, it can

become just one more application with its own unique, non-consolidated directory structure). It yields one of the best values in the whole field of Identity Management. Certainly, it improves the life of the end-user, who no longer needs to remember a long list of account codes and passwords. This alone generates enthusiasm and commitment across the enterprise. However, there are other benefits, including reduced cost for user administration; experience shows that 33% to 50% of all help desk work load involves helping people remember and reset passwords. Security is tighter during operation, with the exception that there is a single point of entry where all access could be compromised; it is at this point that the extra security technology built into directories becomes the vital cog in the wheel. And finally, security is much tighter as an employee terminates; all access can be cut off at the same time, so that there are no lingering security holes left open.

The field has matured in the last 2-3 years, and several vendors have established themselves with field-tested products to implement Single Sign-On solutions. Such vendors include Secure Computing, Access360 and Oblix.

e-Provisioning

The coordination of ordering equipment (such as computers, building passes, mobile phones and pagers), services (such as phone number, network access, and e-mail account) and access (applications and data) is called *e–Provisioning*. This is an example of a much broader application of the concept of identity management.

The ability to have all of these things ready by the time a new employee arrives, or an existing employee arrives at a new position, can make the employee productive much earlier than is the case in most enterprises. It can also reduce the cost of provisioning the employee, as the coordination is automated. At the same time, it can help enforce technology standards, as all equipment can be ordered and configured in a standard format. The ability to retrieve all of the equipment and turn off all of the services and access at termination can be a significant cost savings and security improvement.

The e-Provisioning market is still evolving. A few vendors are appearing with production-ready product. One of these is Business Layers, with their Day One product. Day One aims to coordinate the ordering of equipment, services and access– all primarily within an enterprise. Other companies with similar capabilities include iPlanet and Access360, although they emphasize network access provisioning. Another company,

Flatrock with its Instant Extranet software, focuses on coordinating access to applications and data, with all of the power and security to do it across enterprise boundaries.

There is some overlap between e-Provisioning and Single Sign-On. At the very least, e-Provisioning can automate some aspects of administration for Single Sign-On. Therefore, when considering packaging an infrastructure application with a directory project, it can be useful to architect both solutions at the same time.

The Bottom Line

Packaging any of these or other Infrastructure Applications with the deployment of a Directory Service Infrastructure as part of a well-structured project, will give impetus to Directory deployment. It helps by adding to the ROI for the business case, by generating enthusiasm among users and management, by streamlining infrastructure operation and by showing early return on the Directory Infrastructure investment. The key to success is integration of the Infrastructure Applications with Directory Service Infrastructure Architecture and Implementation.

Determining which Infrastructure Application to deploy and the correct architecture for the Directory Service Infrastructure can often be a daunting task. Reliance on solid experience from trained consultants is one way to assure that the benefits to the whole corporation are achieved when an Infrastructure Application is deployed along with a Directory Service Infrastructure