Directory Services
Frequently Asked Questions

1. **Which directory servers does OneNetPlus.com use?** We are agnostic when it comes to directory servers. At the moment, we use the OpenLDAP server on Linux, iPlanet's Netscape Directory Server on Solaris 8 and Microsoft Windows 2000 Active Directory. All of our proprietary tools are LDAPv2 compliant and above.

2. **Can MS Exchange be used as a directory server?** Exchange version 5.5 and above is LDAPv3 compliant, meaning it will respond to LDAPv3 queries. However, Exchange 5.5 is not nearly as extensible as a true LDAP Directory server.

3. **How does one choose which data elements go into a directory?** Only those data elements that will be used by two or more applications and/or will facilitate location independence should be included in the directory. Data that is highly sensitive or specialized should be excluded.

4. **Is an LDAP name space hard to change once deployed?** Yes, it is quite difficult to change. As a result, a well-designed schema is typically flat in nature. Poorly architected schemas are generally too hierarchical. If the design is kept flat, new attributes can be added without having to change the schema. Changes to schemas are also costly. We know clients who spent over a year completing a migration due to a poorly architected directory schema.

5. **How should one choose a directory server?** Any commonly used directory service will be LDAPv2 or LDAPv3 compliant, so the standard is not a differentiator. Administration tools, on the other hand, play a major role in deciding which directory server to choose. Scalability and price are also common differentiators. Most directory servers are priced on cost per entry; if the price goes down, the more entries one buys.

   In reality, the right choice may often include more than one type of directory server. There may be a need for Microsoft Active Directory and Netscape Directory Server to co-exist, each one playing a unique role. Microsoft Active Directory comes standard with Windows 2000, and is required for a Windows 2000 network. If a company is migrating to Windows 2000, Active Directory must be used. Novell Directory Server comes standard with a Novell Network, so if a company uses Novell, it is likely to consider deploying Novell Directory Server.

   In either case, if scalability is an issue (more than one million entries), Netscape Directory Server should also be considered. Keep in mind that these are rules of thumb and not absolutes.

6. **When multiple directories are deployed, are they typically integrated?** This depends on the reasoning behind choosing multiple directories. If one of the directories is to support a network operating system environment, then there will

typically be sharing between the two directories. This type of integration usually occurs at the point of origin, being the authoritative data sources.

7. **Which directory server does OneNetPlus.com recommend?** We are agnostic when it comes to directory servers. We would assess a client's specific situation and recommend the directory server that fits them the best, in terms of scalability, reliability, performance and price.

8. **What type of company can benefit from directory services?**

- A Company that is deploying software requiring directory services.
- A Company that spends too much time and money identifying the source of common data elements every time a new application is deployed.
- A Company that already has a directory server installed but has to spend time and money manually updating it.
- A Company that is rolling out an eBusiness initiative.
- A Company that would like to unify application logins.

9. **What are some major uses of directories?**

- eCommerce and eBusiness - Many aspects of eBusiness can be best facilitated via a directory implementation. User authentication (both strong and weak), application integration and entitlement are but a few. Simple integration between multiple backend systems can make or break an eBusiness initiative. It can speed the time to market as well as reduce system overhead, from a logical and procedural perspective, for long-term viability.
- Entitlement - Through authentication, a user can be entitled, and that entitlement can be passed to multiple applications. This kind of single login can greatly simplify the user experience. Positive user experience can be a strategic imperative in eBusiness.
- Email routing - MTA message transfer authentication.
- Network object management - Directory Enabled Network (DEN) objects include: servers, routers, hubs, all logins/passwords and program components. A program component, like a DLL, can be part of a library stored in a directory name space. If an application begins to fail, due to missing a DLL, a routine could query the LDAP name space and pick-up the required DLL.

10. **What is strong vs. weak authentication/security?** Authentication is the process of determining if someone really is who they say they are. One method of authentication is through logon and password. This is considered a weak authentication mechanism because passwords can be stolen or compromised very easily. A more secure mechanism for authentication is through digital certificates that are verified by a certificate authority, as part of a Public Key Infrastructure (PKI). This is considered strong authentication because it is much more difficult to compromise. Both weak and strong authentication have a place in an enterprise computing architecture.

11. **Does an LDAP query take longer, logically, than a basic database query?** No. LDAP stands for Lightweight Directory Access Protocol. The word "lightweight" is used because the protocol requires much less overhead than a database query. A database query generally follows a path that is something like ADO, to ODBC, to DBLib, to TDS, and then to the network layer of the database where it begins to encounter rules for locking, and referential integrity, etc. With LDAP, the query runs from the IP layer to the LDAP name space. Performance is typically much better with LDAP, which is one of the many reasons it is beginning to take such a strong hold in technology architectures today.

12. **What is Data Synchronization?** Data synchronization allows the data from one or many authoritative sources to update the directory service at regular intervals, keeping the directory data up-to-date and reliable.

13. **Do Directories work without Data Synchronization?** Data synchronization is not a prerequisite for directory services but without it, the data in the directory service will quickly become unreliable. If the data in the name space is not tied to an authoritative source, it will begin to degrade, weakening the effective use of the directory overall. When OneNetPlus.com's Data Synchronization Tools are included with a directory implementation, the return on investment relative to deploying LDAP, is more likely to be fully realized.

14. **When does LDAP become the authoritative source for data?** Since LDAP's intent is for read access and not update access, LDAP would typically not be an authoritative source for data that is volatile. LDAP was not intended for managing data changes from multiple applications. However, LDAP can be an authoritative source if the data is relatively static and there are no other more appropriate sources of data that can be classified as the authority.

15. **Can a company that already has an LDAP server installed benefit from data synchronization?** Absolutely. If they are manually updating data, then they are probably throwing people at the problem and potentially spending too much money on an error prone process. If they do not update it at all, then directory server data is probably degrading and being perceived as unreliable and untrustworthy. Data synchronization can be deployed to automate the update process, reduce the costs involved, and ultimately preserve the investment in the directory.

16. **What if a company has applications that are not LDAP capable?** LDAP will most likely be initially deployed to facilitate one of the IT objectives or requirements stated in FAQ #9. Enabling LDAP capable applications is one of these objectives. Applications that are not LDAP capable cannot benefit from a directory implementation per se.

    However, an investment in LDAP will not likely degrade even if it only to supports a single purpose. This is true for two important reasons. First, because LDAP is such an effective architectural tool, many common “off the shelf “applications have LDAP capabilities scheduled for their next release. Many of these are not just LDAP capable but actually require LDAP. Also, the majority of new applications, not yet

on the market , will have LDAP capabilities. The more applications that are LDAP capable, the better the return on the initial LDAP investment.

Secondly, OneNetPlus.com's Integrated Directory Services is a multi-pronged solution that includes directory tools as well as the data synchronization tool set. As previously described, our DataSync tools compile enterprise data and reconciles it to the LDAP name space on a regular basis. If our clients require it, we can configure DataSync to reconcile to a database target, as well as the LDAP name space. Remedy ARS is an example of an application, which we use operationally, that does not support LDAP queries as yet. The common information we reconcile to our LDAP name space is simultaneously reconciled to Remedy, for use within that application. Once Remedy becomes LDAP capable, this secondary reconciliation will be discontinued.

17. **How are VPN and Directory Services related?** VPN needs some way to authenticate everyone that logs into the network. Most VPN packages are LDAP enabled and look to LDAP for authentication. Because this concerns network access, the accuracy of the LDAP name space is critical (see FAQ #13 for the power of DataSync relative to directory services). As a bonus, once LDAP is set up for user authentication, the stage is set for single login for all services/applications that are LDAP capable.

18. **What does OneNetPlus.com's Integrated Directory Service include?** It is a multi-pronged solution that includes a directory tool and data synchronization, combined with level 1 help desk, all in a managed service delivery format.

19. **Do OneNetPlus.com's Integrated Directory Services have to be delivered as a managed service?** Because so much of Directory Services is infrastructure related, i.e. servers, topology, general application architecture and systems management, it is - a perfect candidate for a managed service. Relieving an IT organization of the infrastructure burden when deploying directories, allows them to focus more strategically on the use of this technology enterprise-wide. However, for those organizations that need to or want to manage their directories in-house, OneNetPlus.com can make our complete Integrated Directory methodology (tools and procedures) available to our clients through provisioning.

OneNetPlus.com
1325 Tri-State Parkway, Suite 325 Gurnee, Illinois 60031
Ph-847-855-4900 Fx-847-855-0846