Lotus. Domino. 6

Technical Overview

Level: All
Works with: Domino 6
Updated: 01-Oct-2002

by Jane Hosie-Bounar,
Christie Williams,
and Tara Hall

With the release of Domino 6, Lotus continues to play a major role in the e-business revolution. To meet the challenges of business globalization, frequent mergers and acquisitions, and the increasing demand for Web-based business tools, Lotus has combined both evolution and innovation in its latest upgrade of Domino server technology. The features in Domino 6 build on the features in Release 5 to address rapidly changing industry trends and to meet their challenges head on.

Domino 6 innovations expand the capabilities of the Domino messaging and collaboration server to maximize the value of Domino within your existing infrastructure and to provide robust support for your Notes messaging and Web applications. Whether your users are working with the Notes client or a Web browser, you can ensure that a single application meets their needs.

Server installation and setup improvements
Domino 6 provides additional installation options for UNIX systems, support for multiple versions on a single UNIX system, and an improved Domino Server Setup Program.

New UNIX installation options
Domino 6 provides four new UNIX installation options:
- Install template files
  Install the Domino 6 system templates overwriting any existing template files.
- Create /opt/lotus soft link during installation
  Creates a soft link to the /opt/lotus location if you choose not to install in the /opt/lotus location; this option is available for single Domino server installations only.
- Install Service Provider
  Sets up a service provider server after installation of a Domino Enterprise server.
- Add data directories only
  Adds data directories to an existing Domino installation creating a partitioned server or adds additional directories to an existing partitioned server.

Multi-version UNIX support
Domino 6 supports installation of multiple instances of the Domino server, each with its own program directory, on a single UNIX machine. The instances can include the same release of Domino (for example, only instances of Domino 6) or instances of Domino 6 and one instance of an earlier Domino release. If you want all instances to be the same release, install a Domino partitioned server. Then all Domino partitions share one program directory and, by doing so, conserve system resources.

Domino Server Setup Program

In the past, Domino server setup relied primarily on the databases setup.nsf and setupweb.nsf, which required either a Notes client or Web browser for setup. A new Domino Server Setup Program written in Java lets you set up a server either remotely or locally. The setup program is available on all server platforms. To set up the server locally, start the server after installation to launch the setup program. To set up the server remotely, use another Domino server command line prompt, a Windows client system with or without the Domino Administrator client, or a UNIX workstation to run the program. The new Domino Server Setup Program allows you to customize server setup.

Domino Server Setup Profile

The Domino Server Setup Profile is a file that automates the server setup program. You can record a server setup from a server or Windows client and then run the setup profile on another server or client to setup a local or remote server with standard settings. Use the profile to quickly configure a standard server such as a mail server.

Server scalability and performance

Domino 6 includes a number of enhancements that improve server scalability and performance.

Server startup and server performance

Domino 6 optimizes server startup to speed recovery and improve up-time. Improvements include:
- View logging is transaction logging of key views, which assures that you won't need to rebuild those views after a server crash.
- The ability to log information about the availability index, which reports back the health of the server. This index more consistently indicates the state of the clustered server and makes cluster load balancing easier to administer.
- Optimized process starts also improve server performance.
- Optimization of the agent manager startup procedure avoids opening all databases, which would slow server performance.
- Optimization of the schedule manager reduces overhead on server startup.
- Inclusion of a persistent directory manager cache enhances efficiencies.
- Enhanced cluster support, including automatic detection of software failures and automatic fault recovery, is now available across all Domino platforms.

For additional information, see the *LDD Today* interview "**Jim Rouleau on Domino 6 server availability**."

Replication

Streaming replication is a new feature that improves replication across all servers, and it especially improves mail server performance. Streaming replication involves a single server request, which then pulls in all the data (Notes documents and their attachments) into the database. This feature dramatically reduces replication time and works in all Domino 6 client/server scenarios.

Streaming replication also means that when using the Notes client you no longer have to wait until the replication is over before seeing replicated documents in folders. They appear individually, as soon as they are pulled into the system, and you can begin to work on them before the database has finished replicating. In addition, documents are replicated in ascending size order.

Streaming replication consists of two components:
- Object streaming
  When opening a note, object streaming retrieves all items and objects, including file attachments, images, and so on.
- The stream mechanism
  When retrieving notes from the source database, the stream mechanism issues one high-level transaction to get all the notes and all their objects. It uses object streaming to retrieve all the objects.

Client/server interactions

Client/server interactions are also more efficient in Domino 6. For example, an advantage of the new streaming feature is that, because attachments are also streamed, Open and Save operations are more efficient. Client/server interactions are also dramatically improved by less frequent unread table exchanges, as there is a significant reduction in the number of bytes exchanged between a client and the server.

Another performance enhancement is the use of incremental view reading, used to update design information and, in selected cases, user views. For example, when you move a document from one folder to another, the server is requested to provide just the incremental change it will take to fill the screen with the new view.

Network compression
Domino 6 has introduced more new features to reduce network utilization. Network compression reduces the number of bytes sent during transactions by up to 50 percent. Connections across heavily loaded links such as WANs and XPCs will see the most benefit. To use network compression, you must enable it on both the client and the server. Additionally, Domino 6 incorporation of "network" streaming also reduces the overhead of large transfers. See the *LDD Today* article "**Network compression in Domino 6**" for more details.

Autodialer for dialup ISP connections
The autodialer coordinates dialup ISP connections between servers. It links two Connection documents, so a server with a dialup Internet connection can connect automatically in case scheduled replication or mail transfer is initiated by another server.

Full-text search
The Domino 6 full-text search feature has also undergone major changes. Most data is now updated in place. In addition, Domino uses the NSF buffer manager for memory services, which improves caching and balances memory between NSF and FT. Furthermore, a new search processor results in closer integration of text and field retrieval and significantly faster Boolean processing.

Formula engine
The Domino 6 formula (compute) engine has had a major overhaul, resulting in computation performance up to two times faster than in previous Domino releases. This overhaul brings performance benefits in many areas including view refreshes, agents, and form rendering.

IMAP server
In earlier releases of Domino, the IMAP server was based on a layered approach that relied on using additional Notes items and views to maintain the IMAP-specific data for messages. In Domino 6, the core database layer (NSF) has been enhanced to include native support for IMAP semantics, and the IMAP server has been redesigned to use these new capabilities. In addition, the IMAP server now has a new multi-threaded and data-streaming architecture for additional parallelism, providing much higher performance and scalability.

Automatic fault recovery
Available for the Windows NT and UNIX platforms, automatic fault recovery shuts down and restarts a server without administrator intervention after an exception occurs. Fault recovery uses operating system resources, like message queues. When fault recovery restarts a server, it sends an automatic notification to whomever you specify when you set up fault recovery.

Event Generators and Event Handlers
Event generators replace probes and monitors. Event handlers were formerly referred to as event notification. You can use Event Generators to monitor server resources and network activity. Event generators gather information either by monitoring a task or statistic or by checking a server for access or connectivity. You can determine the criteria by which an event is created. When the criteria is met, an event is created, then passed to the Event Monitor task.

Event handlers determine which action to take when an event occurs. Event handlers can log an event or prevent an event from being logged, notify you when an event occurs, or forward an event for additional processing.

Improvements in administration
Domino 6 includes a number of administration features that give you powerful, centralized control over Domino and reduce your administrative tasks.

Policy-based management
Domino 6 introduces policy-based management, which goes well beyond Domino 5 Setup Profiles and greatly simplifies administration, helps you maintain standard settings and configurations, and speeds up deployment of changes throughout an organization, business unit, or workgroup.

A policy is a collection of settings related to a class of end users that can be applied either when registering new users or retroactively to existing users. You can set and manage registration, setup, archiving, desktop, and security policies. You create new policies from the Configurations tab and apply them from the People & Groups tab of the Domino Administrator.

Policies are easy to set up and apply, and because they use a parent/child, hierarchical model, they are easy to extend. The Policy by Hierarchy view shows the relationship among policies, subpolicies, and individual policy

settings. A Policy Synopsis, which is available from both the People & Groups and Configuration tabs, shows you the effective policy settings for the specified people and groups.
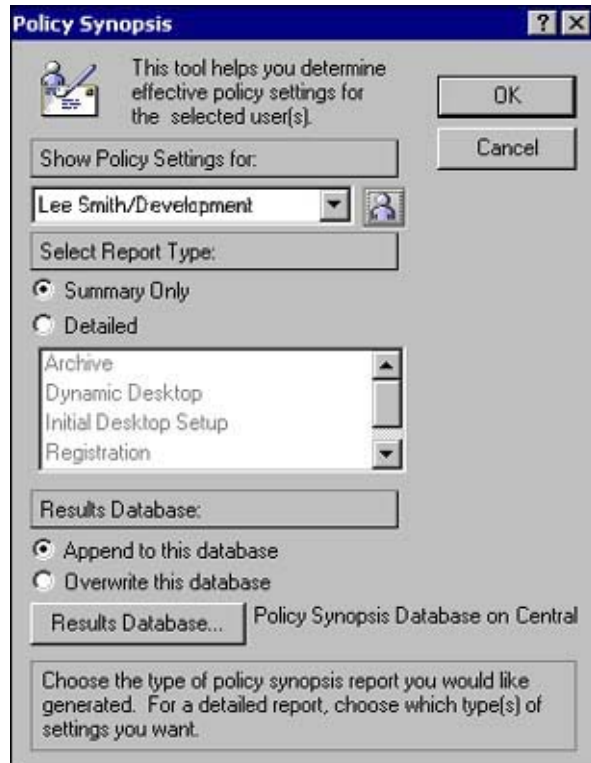
Registration policies
Policy-based registration options include such things as registration server, password options, mail server and template, Internet address information, ID and certifier information, and group assignments. When registering users, you simply choose the appropriate registration policy to apply all the policy's options to the users.

Setup and Desktop policies
Setup and Desktop policies include the same settings, which include options for specification of a corporate Welcome page, dial-up connection information, server names, applet security, proxies, preferences, and more. The difference between them is in how they are applied.

Setup policies are applied once to clients, on their initial configuration, and therefore, you use them for information that you do not want to keep updated on clients. Desktop policies are applied to all clients whenever a change in the policy occurs, so these policies include information that needs to be kept up-to-date.

Archiving policies
Using policies, you can set and manage archiving settings for users, including allowing or disallowing users to create their own archive settings for their own databases. You can use more than one set of archive criteria and designate more than one archive destination.

Security policies
Security policies contain password management and ECL fields. See the **New security features** section for more details.

For more information about policy-based management, see the *LDD Today* article, "**Policy-based system administration with Domino 6**."

Automatic client upgrades with Lotus Notes Smart Upgrade
One of the costs of deploying Domino in the past has been upgrading all the desktops in a system. A new feature of Domino 6, Lotus Notes Smart Upgrade, lets you install upgrades at the desktop level with the push of a button.

Using a Smart Upgrade database on the server, the server Configuration document, and optionally, desktop policies, administrators control and maintain version deployment. When users connect to their home server, they are automatically prompted to upgrade to a new version of Notes. If they click OK, the new software is downloaded from the server, and the client is automatically shutdown, upgraded, and restarted.

xSP administration
Domino 6 enhances administration features to support both xSP administration of end users and organization administration of end users, securely. You also have the ability to generate bills and reports on a per organization basis. In addition, the new activity logging service provides consistent and complete reporting, which can easily be broken into organization reports. The HTTP log can also be easily broken into organization reports. (See the **Domino hosting features** section for more details.)

Deployment of corporate Welcome pages
You can create and automatically deploy corporate Welcome pages to your users. You create a corporate database to hold one or more Welcome pages and then link that database to the Desktop Policy document in the Domino Directory. You can control which Welcome page should be used and whether users can change their home page.

Client version reporting and license tracking
When a Notes 6 client connects to a Domino 6 server, it sends its Notes version, operating system platform, and machine name to the server. This information is added to the user's Person document, letting you see which version of Notes your users are running.

In addition, when a Notes client connects to a Domino 6 server through HTTP, IMAP, POP3, SMTP, or LDAP, client information is collected and stored in a User Licenses database. An administration process request updates the License Tracking document in the Domino Directory with information from the User Licenses database. The License Tracking document is updated daily, so you can monitor the number of active Notes clients in your domain.

Console innovations and improvements
For Domino 6, the Web Administrator client has been revamped and improved to look and function like the (Win32) Administrator client, making administration from a Web browser more intuitive.

In addition, Domino 6 includes a separate, Java-based Server Controller that lets you control the Domino server from either the Administrator (remote) server console or a separate Java-based console called the Domino Console. This architecture allows you to control the Domino server when it is unreachable directly from the remote server console and facilitates issuing one command to multiple servers in one or more domains. See the *LDD Today* interview "**Mallareddy Karra on the Domino Console**" for more information on the Domino Console.

Both the remote server console and the new Domino Console include user interface improvements. New customization allows you to set console text, color, and highlight attributes for both the local and remote server consoles, making it easier to read and interpret the information that appears.
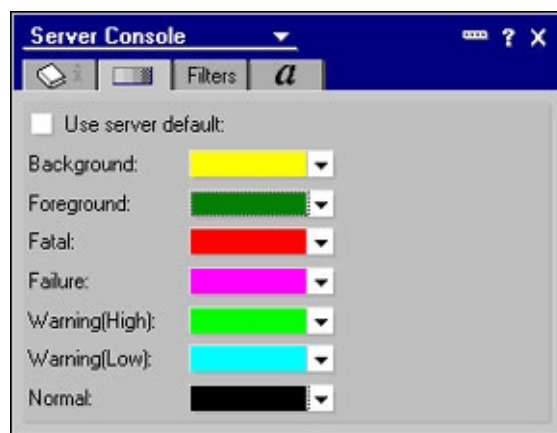
In the remote server console in the Server\Status panel of the Domino Administrator, you can filter status messages for particular status levels and set stop triggers so that critical information pauses on the console screen. You can set new event notifications to help you monitor troublesome events more closely, and if you need

more information on an error you receive, you can retrieve that information on-the-fly from the Domino Administrator. The server console can log to a text file, so you can look at the output off-line rather than tie up the machine. You also can view OS platform statistics along with Domino server statistics. Finally, command line help for most server tasks is now available.

**Statistics monitoring and analysis**

Statistics monitoring and analysis can help you plan and run individual systems, as well as your whole domain, more efficiently. In Domino 6, you can monitor performance statistic profiles using charts that display the statistics in real-time or historically. And the Domino Server Monitor includes server profiles that monitor tasks and processes specific to a certain subset of servers.

IBM Tivoli Analyzer for Lotus Domino

It can be hard to know which information to monitor on a server and what indicates exactly when a server is "healthy" or in need of attention. The IBM Tivoli Analyzer for Lotus Domino (a separate product offering from Tivoli Systems) includes two integrated system-management tools: the Server Health Monitor, which offers real-time assessment and recommendations for server performance, and Activity Trends, which provides data collection, data exploration, and resource balancing. Using these tools, you can manage servers and databases, ensure better server performance, and plan for current and future needs.

Note: The IBM Tivoli Analyzer for Lotus Domino requires a separate license to use.

Server Health Monitoring is available from the Server Monitoring or Real-time Charting tabs of the Domino Administrator. Health ratings also appear as color-coded thermometers in a new column to the left of the server name in the By State view of the Server Monitoring tab:
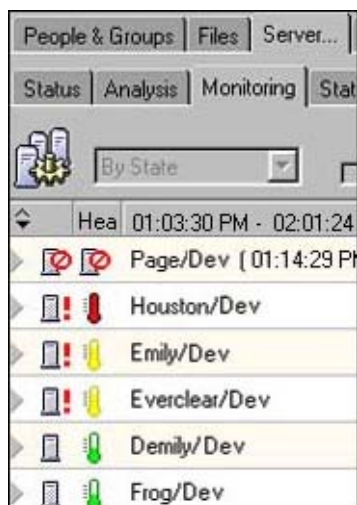
In addition, a Server Health Monitoring Report and the underlying metrics that contribute to a server's health rating are available, as well as Server Health Recommendation documents for servers with a Critical health rating.
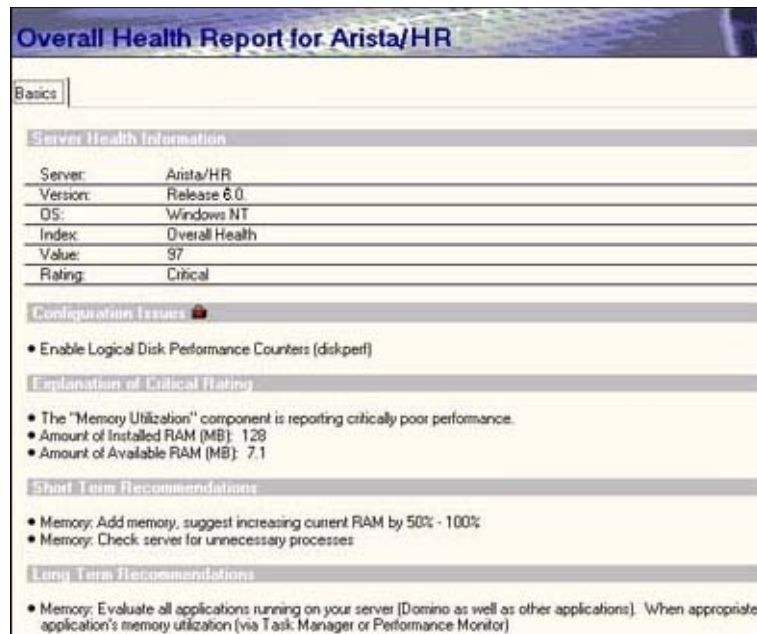
Integration of Server Health Monitoring with new historical charting features allows you to analyze the past server health values, giving you insight into a server's health over a longer period of time. Additionally, you can view operating system level platform statistics such as CPU, memory, and disk I/O. The full set of network level statistics is also available.

Activity Trends presents server workloads by user, database, and protocol over time; makes load balancing recommendations; and can determine growth rate trends.

For Domino 6, supported platforms include Windows NT, Windows 2000, Solaris Sparc (version 2.8), and pSeries (AIX 4.3.3). Some iSeries (AS/400) platform statistics are also available.

For more information about Server Health Monitoring, see the *LDD Today* article, "**Start using Domino 6 Server Health Monitoring now!**"

Server Activity Logging
Domino Server Activity Logging has also been enhanced to include more detailed information about Notes sessions, databases, scheduled agent activity, and POP3, HTTP, SMTP, IMAP, and LDAP activity. (See **Domino hosting features** for additional information.)

Other administrative features
Additional features that improve administration include the following:
- Managing users, groups, and servers
  In Domino 6, you can find a user, group, or server in a domain using the new Find Name in Domain administration request. In addition, you can change a Web user name using the Domino 6 Administrator client.
- Archiving
  Archiving in Domino 6 includes archiving to multiple archives, folder-based archiving, administrator control over archiving, and server-to-server archiving. See the **Archiving policies** section earlier for more information.
- Extended Administration server
  An extended administration server processes Domino Directory requests allowing you to specify more than one administration server per Domino Directory.

Web server enhancements
The improvements to the Domino 6 Web server are geared toward enhancing performance and scalability and expanding the capabilities for Web application development and deployment.

The rewritten HTTP server provides HTTP 1.1 persistent connections, improved session handling, better denial of service attack handling, and more administrative control over things like URL length and number of path segments.

The rearchitected Web server task supports an Internet Sites view with Internet Site documents in the Domino Directory. The Internet Site documents contain most of the information from the Domino 5 Server document that affects the HTTP stack as well as some new settings. All servers that share the same Domino Directory (that is, are in the same domain) share the same Internet Site documents in the Internet Sites view.
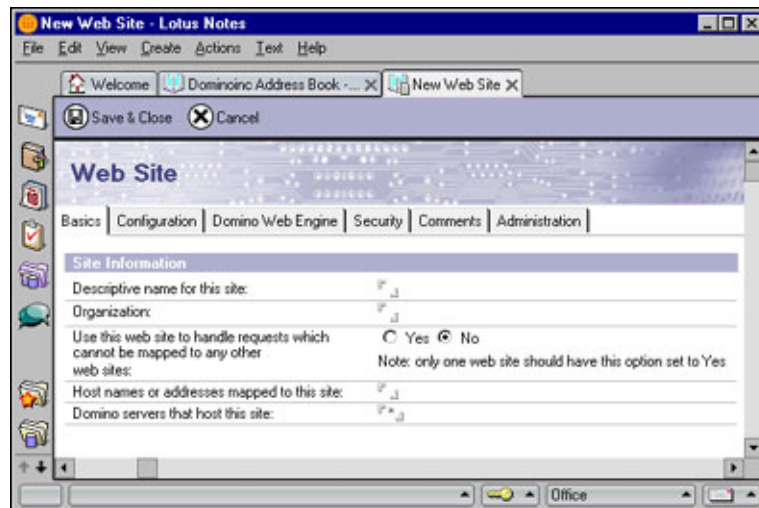
Also in Domino 6, there is a new Web Site Rule document: HTTP response header. Web Site Rules documents appear as responses to the Web Site documents in the Domino Directory. Web Site Rule documents let you relocate or reorganize your sites without breaking links or Web browser bookmarks. The HTTP response header rule type adds an Expires header or custom header to HTTP responses that match specified URL patterns and response codes.

For more details, see the *LDD Today* articles, **Building Web applications in Domino 6: A tutorial on Web site addressing**, **Building Web applications in Domino 6: Web site rules**, **Building Web applications in Domino 6: Accessing and protecting the file system**, and **Building Web Applications in Domino 6: Browser caching and response header rules**.

Additionally, the HTML generation engine is now more standards compliant and includes the ability to generate pages in XHTML.

WebDAV support
Domino 6 furthers your ability for collaborative application development by supporting WebDAV (Web Distributed Authoring and Version). WebDAV provides a development environment for controlled and safe simultaneous development efforts. Teams of developers using tools that support WebDAV can open, edit, and save file design elements to and from a Domino database without risk of overwriting code. This means that the NSF can serve as the common repository for elements developed in third-party tools as well as in Designer 6.

Note: Macromedia's Dreamweaver 4.01 is necessary for WebDAV support; this upgrade can be downloaded from the **Macromedia Web site**. Microsoft FrontPage 2000 is not a supported WebDAV client.

Domino Custom Tag library
Domino 6 provides a custom tag library for those developers developing J2EE applications in third-party tools. They allow quick access to Domino databases and Domino objects such as views, forms, and fields, so you have access to Domino data and services without having to write low-level Java code. The tags are based on the JSP 1.1 standard and so are usable with Web application servers that support that standard.

Web preferences
Web preferences include settings for time zone, date/time format, and number format that are stored in cookies in

a user's Web browser. You enable Web preferences in the Internet Site documents. Users set preferences via a URL similar to http://*servername*/$preferences.nsf.

Single sign-on
Single sign-on (SSO) for Web browsers allows you to sign on to a Domino or WebSphere server once and then have access to any SSO-enabled Domino or WebSphere server in your domain without signing on again. In addition, you can have multiple Web SSO Configuration documents in a Domino Directory or domain.

Support for WebSphere third-party Web server plug-ins
Domino 6 supports the WebSphere plug-ins that allow you to use a third-party Web server as a front-end to a Domino server. The initial release of Domino 6 supports the plug-ins for Microsoft IIS and the IBM HTTP Server. This feature replaces the "Domino for IIS" architecture that was provided in Release 5.

For more information about Web server enhancements, see the *LDD Today* interview "**Jeff Calow on new Web technologies in Domino 6**."

Server cluster enhancements
Many enhancements have been made to clusters, including:
- Making the Cluster Administrator a server thread, so it automatically starts the Cluster Replicator and Cluster Database Directory Manager
- Ensuring the server availability index gives a more accurate indication of the availability of each server in a cluster (You no longer need to use the Notes.ini setting Server_Transinfo_Normalize to improve accuracy.)
- Adding new settings to control the number of active Cluster Replicators
- Using the Domino 6 Server Monitor to monitor all servers in a cluster
- Allowing cluster replication to ignore database size quotas
- Making activities, like user registration and database replication and deletion, cluster-aware
- Adding new Cluster Replicator commands for better control over cluster replication and information gathering

Changes to directories
A major goal of Domino 6 is to make Domino easy to integrate in a multi-directory environment. Large enterprises are beginning to see the advantages of a centralized directory configuration, as it gives them more control and less overhead and is, in the end, easier to manage.

With Domino 6, you have the option of moving from a distributed directory architecture and making Domino the central directory. If you do this, you only need to store the complete Domino Directory, with all of its person and group information, on one central server. (You actually will want to reserve at least two servers to be used as central servers in the event that one server becomes unavailable. Automatic failover of directory servers is now completely built into the product.) You can then store the smaller configuration directories with Domino specific data on the other servers in your domain. The centralized directory information is available to all users, but you save on disk space because you no longer need to store the whole directory on each server. You also save on time, as you are no longer required to replicate your directory across all the servers in your domain.

We have also enhanced the implementation of LDAP capabilities and improved the performance of LDAP directory access. For example, a new Domino LDAP Schema database helps you maintain and extend the schema, there is an automatic schema maintenance process and true object class inheritance, and directory schema can be imported via LDIF files. The new LDAP upgrade service lets you migrate person and group entries directly from an LDAP directory server into the Domino Directory. Support of arbitrary distinguished names, new LDAP configuration settings, activity logging for the LDAP service, and multiple values in the Hostname field in the LDAP Directory Assistance document for LDAP server failover are among the many LDAP improvements we've made. In addition, you can now choose cluster failover as your mechanism of choice for directory assistance failover. Using this mechanism gives you the added capability of load balancing.

You can authenticate Internet clients for IMAP, POP3, LDAP, and NNTP clients as well as HTTP clients using a secondary directory (Domino or third-party LDAP). You can also use a secondary Domino Directory to maintain user names and groups that you don't want to store in names.nsf. Secondary Domino Directories also store groups used in database ACLs.

You can also create a multiple organization Domino Directory, using extended ACLs (xACLs) to ensure users have access to only their organization's information. See **Domino hosting features** for additional information. Also, the new extended ACL controls allow enterprises the ability to delegate administration to regional administrators without giving them manager access. You can configure these regional administrators to allow

them to administer only directory objects within their own organizational units.

We've also achieved more efficiencies in Domino 6 with a new directory lookup cache that is significantly better than previous caches. It's effectiveness for mail sending and routing lookups, for example, are over 95 percent.

Other directory changes to note are:
- Domino 6 can use LDAP, NameLookup, or both to serve up directories
- Additional LDAP server configuration settings are available on the Configuration Settings document
- A directory indexer task created by the database indexer task updates views in the Domino Directory

Working with Active Directory
If you are using Windows 2000, administering users and groups can be synchronized between the Domino Directory and Active Directory. ADSync lets you register, synchronize properties and passwords, and rename and delete users and groups in the Domino Directory when you perform such actions in Active Directory.

You can migrate users and groups from an Active Directory to a Domino Directory using the Active Directory Domino Upgrade Service (ADDUS). This migration tool uses a search base, attribute field mapping, or custom LDAP filters to migrate users and groups.

Domino hosting features
The Domino 6 server includes new hosting features that allow multiple organizations to be transparently hosted by a single logical Domino server. Clients from different hosted companies access their data from the same physical server securely, using standard Internet protocols. This new server feature simplifies server administration and application support and satisfies the needs of the xSP (Service Provider) market. The major Domino components have been modified to support the hosted organization environment.

Note: If you enable the xSP configuration, the entire domain runs in xSP mode to ensure the proper security environment. You may want to set up a separate test domain to try out Domino's hosting features.

Addressing models
xSPs can choose between two different IP address configuration models. For each server and protocol on a server, a hosted organization can have its own unique IP address, or a single IP address can be shared across multiple organizations.

Multiple organization Domino Directory
The multiple organization Domino Directory feature dramatically reduces the complexity of server administration. The administrator works with only one server, yet each organization on that server can function as if it is hosted by its own unique server. For example, each organization has its own HTTP application and file locations. The server also has organization-specific authentication controls.

The Domino Directory template has been modified to allow granular configuration control for each hosted organization. A new feature in Domino Administrator allows an xSP to register a new organization, creating the hosted configuration, producing a new certificate, creating a subdirectory, and implementing the security mechanisms (database ACLs, .ACL files, and extended ACLs) automatically.

Security
Because, in a hosted environment, the Domino Directory is a database that is shared between multiple organizations, security is a critical element. Each document in the Domino Directory is controlled by xACLs (extended ACLs) to allow or disallow access. The existing database Access Control Lists (ACLs) and the new .ACL file feature ensure that organization-private databases remain secure. In addition, file protection documents for the Domino Web server provide additional access control for files accessed via HTTP. Multiple organizations hosted by the logical server can also access shared databases.

Protocol support
For Domino 6, it is possible for xSPs to provide the following services to their customers: IMAP, POP3, LDAP, SMTP, HTTP, SSL, and IIOP.

DOLS
xSPs also support DOLS.

Mail routing
The Domino router has been modified to support multiple organizations simultaneously on the same

physical/logical server.

Activity logging for billing
Data about the Domino server is collected in the log.nsf file with a new Server Activity Logging feature. The xSP can access log.nsf via an API. Data is collected on a per server basis and can be configured per protocol. Each record contains the organization name, and the xSP can determine the appropriate billing model for its customers.

Database server utility programs
To provide more granular control, the database server utility programs such as compact, fixup, updall, and design now allow a directory to be specified. This means, for example, that an xSP administrator can configure program documents in the Domino Directory to have compact run on Company One's databases at 2 AM and Company Two's databases at 3 PM.

Scalability
Scalability features for a hosted environment include:
- Support for a configuration-only directory to improve server performance
- Qualified name lookups per organization in the Domino Directory to provide improved name lookup performance for any size directory
- Support for the use of a network sprayer to provide load balancing or failover capabilities

New security features

In the 1990s, Lotus was one of the first companies to use public key encryption, and we continue to lead the way in security. Domino 6 recognizes that today's computing environments are heterogeneous, using different clients (for browsing and messaging), different servers, different security protocols, and even different security vendors, each providing a different security component, such as certificate authorities, single sign-on servers, and firewalls. For example, a company might run both Notes and Outlook clients for secure messaging, with Domino and Exchange backends, respectively. Those clients might in turn be issued certificates from VeriSign.

To maximize this kind of environment, Domino 6 provides support for new security standards. For example:
- Support for the PKCS#11 standard for Smartcards. Smartcard support provides additional protection for your user credentials because the user's ID is locked such that both a Smartcard (with the ID's password) and a Smartcard PIN are required to unlock it. You can enable and disable Smartcard support in the User Security dialog box.
- Support for the S/MIME v3 feature, S/MIME capabilities. The Notes client can receive messages that have specified algorithms and key lengths and will use that information when sending encrypted mail.

New certificate authority
The Domino certificate authority for Domino 6 includes an optional certificate authorization (CA) process that provides both a unified mechanism for issuing Notes and Internet certificates and an integrated registration of Notes and Internet keys. The certificate authority process is a "locked box" task that runs on the server. Administrators enable Notes and Internet certifiers to use the CA process to take advantage of the following features:
- Ease of granting certificate authority
  Administrators select a few parameters, such as certificate duration, and designate administrators who are authorized to use that particular certifier. They then load the certificate authority server task to enable the new certifier to use the CA process.
- Separation of certificate authority and registration authority roles
  Administrators can delegate certificate approval/denial process to lower-echelon administrators (registration authorities), who can perform certification tasks without access to the certifier ID or password.
- Creation of Certificate Revocation Lists (CRLs)
  CRLs maintain information about expired certificates, and their use helps administrators maintain the integrity of their organization. Certificate revocation status can be checked before someone chooses to trust a certificate. A CA administrator can easily revoke a certificate if the subject of the certificate leaves the organization or if the certificate has been compromised. CRLs are published on a regular schedule and are posted in the CA's Certifier document in the Domino Directory.
- Simplified certificate request process
  There is a new Web interface for certificate request management.

Additionally, the Notes client has been extended to allow users to manage their certificates through the User Security dialog box.

A Site document (created for each Internet protocol so that a server can obtain the SSL security settings for that

protocol) contains settings controlling the use of CRLs. These settings are not part of the Server document, but are passed into trust policy code during certificate chain evaluation.

Delegated server administration
Domino now includes several levels of server administrators so that you can securely delegate different levels of administration to different administrators. For example, some administrators may have full access when using a remote console while others may not.

Notes and Internet password management
Domino's password management features provide the administrative functions you need to protect your Notes and Internet environment. You can automatically synchronize Internet passwords with Notes ID passwords by setting this in a security policy. In addition, you can more easily manage Notes and Internet password quality and length, as well as control expiration period, change intervals, and, in the case of Notes passwords, password history.

Admin ECLs
You can now push Admin ECLs to clients dynamically on an as-needed basis, making it easier to deliver timely updates and to update clients who get the default ECL during setup because they were disconnected from the directory. In addition, the key string <ECLOwner> is added to the Admin ECL to enable the current user to modify the ECL during the client ECL refresh.

Messaging
New products, including iNotes Web Access and Domino Everyplace Servers, extend access to Domino's messaging infrastructure, from desktop to laptop, to the Web, to cell phones and Personal Digital Assistants based on the Palm, Windows CE, and EPOC operating systems. In addition, Domino 6 includes new features for managing and controlling your messaging infrastructure. For example, in Domino 6:
- Using the server's Configuration document, you can set up system mail rules that let you specify message criteria and actions to be taken for all messages processed on the server. This allows you to deny and quarantine messages. You might filter mail contents to stop the flow of SPAM through your routers, for example.
- Mail journaling works with the system mail rules to save copies of messages to a Notes journal database. You can save all messages that pass through MAIL.BOX, or you can specify criteria for selecting certain messages to save. For instance, you can specify people, groups, or domains from which or to which you want to save messages.
- New mail file quota management options provide you additional tools to control the size of users' mail files so that you can better manage disk storage. You can specify that mail be held for users whose mail file exceeds a specified quota limit, with quota warning and error notification to the mail file owner.
- The IMAP server now supports the Namespace extension, so an IMAP client can now view folders in another user's mail file or the public folders in a shared database. This means that users can have delegated access to another user's mail via IMAP, in addition to access via the Notes client.
- You can track SMTP servers that permit third-party relay using DNS Blacklist (DNSBLs). You can specify which DNS Blacklists to check and which action to take when mail is received from a host listed in the DNSBLs. Mail from servers found on a DNS Blacklist can be tagged or rejected, giving you more control over mail from hosts that may be sending or relaying potential SPAM.
- A set of Extension Manager hooks are available for the SMTP protocol that can be used to process incoming SMTP messages. While primarily intended for third party tool vendors, you can use the API to develop custom tools and applications that process incoming SMTP mail prior to it being processed by the Domino Messaging server.
- Anti-relay restrictions prevent unauthorized relays on your Domino SMTP servers. The inbound relay controls define the hosts from which and to which an SMTP server can relay messages.
- Shared mail now supports configuration of multiple shared mail databases and directories and can associate a user mail file with more than one shared mail database. When you install Domino 6, it automatically creates a shared mail database.

Domino Off-Line Services
There are many new enhancements for Domino Off-Line Services (DOLS) to help users work more efficiently off-line, including:
- Taking the directory catalog off-line
- Encrypting a subscription
- Loading customized subscriptions onto the DOLS Client Pre-Installer CD
- Sharing files among subscriptions
- Preventing compaction and full-text indexing of subscriptions
- Pushing settings off-line to users, so users don't need to reinstall a subscription to update their settings

- Preventing users from modifying synchronization schedule settings
- Using a passthru server to connect to the DOLS server
- Providing an optional or secondary TCP/IP address configuration to access the DOLS server
- Overwriting the user's off-line ID each time the user installs a subscription to keep IDs updated and consistent
- Supporting Domino xSP server configuration
- Supporting single sign-on authentication to the DOLS server
- Supporting the Linux server platform
- Providing cleaner integration with iNotes templates
- Improving external authentication coverage
- Improving proxy server configuration coverage, such as reverse proxy, DMZ, Passthru server, and dual IP addresses
- Enabling accessibility features

In addition, DOLS supports the Notes multi-user configuration. And Web Control and iNotes Sync Manager provide keyboard shortcuts for nearly every option.