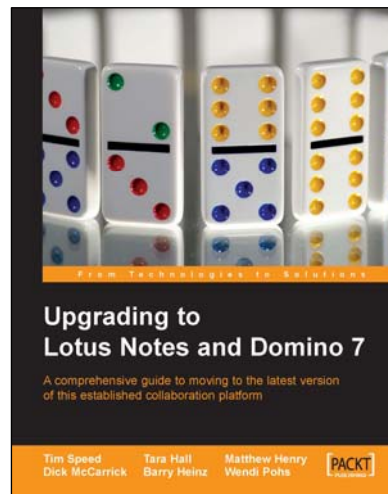




# Upgrading to Lotus Notes and Domino 7

**Tim Speed**  
**Dick McCarrick**  
**Tara Hall**  
**Matthew Henry**  
**Wendi Pohs**  
**Barry Heinz**



## Chapter 3 "Domino Domain Monitoring"

## In this package, you will find:

A Biography of the authors of the book

A preview chapter from the book, Chapter 3 "Domino Domain Monitoring"

A synopsis of the book's content

Information on where to buy this book

## About the Authors

**Timothy Speed** is an IBM Certified IT Architect working for the IBM Lotus Brand (ISSL). Tim has been involved in Internet and messaging security since 1992. He has also participated with the Domino infrastructure team at the Nagano Olympics, and with the Lotus Notes systems for the Sydney Olympics. His certifications include CISSP, MCSE, A+ Plus Security from CompTIA, Lotus Domino CLP Principal Administrator, and Lotus Domino CLP Principal Developer. (Notes/Domino certifications in R3, R4, R5, ND6, and Notes and Domino 7.)

**Dick McCarrick** is a content developer for IBM's developerWorks Lotus website ([www.ibm.com/developerworks/lotus](http://www.ibm.com/developerworks/lotus)). Dick joined the Lotus Notes team in 1990 as a documentation writer, and moved over to developerWorks Lotus in 2001.

**Tara Hall** is the Web Content Manager for IBM's developerWorks Workplace and developerWorks Lotus (formerly the Lotus Developer Domain/Notes.net) websites. She has been writing and editing technical documentation since graduating from New Mexico State University in 1997 with a Masters of Art degree in Creative Writing.

**Matthew Henry** is a Technical Architect working for KEMET Electronics Corporation. Matthew has worked with Lotus Notes since release 3.0, when he led the rollout of Lotus Notes as KEMET's email and collaborative platform of choice. He has served with various Lotus Notes and Domino activities and customer councils including presenting at Lotusphere for several years.

**Wendi Pohn** is CTO at InfoClear Consulting, a company that specializes in taxonomy management and toolkit integration. Prior to that, she was a consulting IT specialist on IBM's intranet user experience team. Wendi is the author of a book about knowledge management methodologies, *Practical Knowledge Management: The Lotus Knowledge Discovery System*, published by IBM Press. Wendi joined IBM/Lotus in 1996, and has worked on various projects as a spec writer, online help designer, user assistance manager, and lead for search and taxonomy for w3, IBM's corporate intranet. Prior to joining IBM, Wendi worked at the American Mathematical Society and at Digital Equipment Corporation. She received her BA and MILS degrees from the University of Michigan.

For More Information: [www.packtpub.com/upgrading\\_lotus/book](http://www.packtpub.com/upgrading_lotus/book)

# 3

## Domino Domain Monitoring

This chapter, along with the ones that follow, discusses the many new features found in the Domino 7 server. Here is a list of the features:

- Domino Domain Monitoring (DDM)
- DB2 support and administration
- Autonomic data collection
- Policy improvements, including new management features and mail policies
- AdminP enhancements
- Rename reversion
- SMTP improvements
- Client lock down
- Smart Upgrade enhancements
- Linux/Mozilla Web Administration client
- New ID and password recovery features
- CA process improvements
- Support for additional standards, including IPV6, CIDR, and IOCP
- Improvements and additions to rules, configuration, backup and restore, and server administration

For More Information: [www.packtpub.com/upgrading\\_lotus/book](http://www.packtpub.com/upgrading_lotus/book)

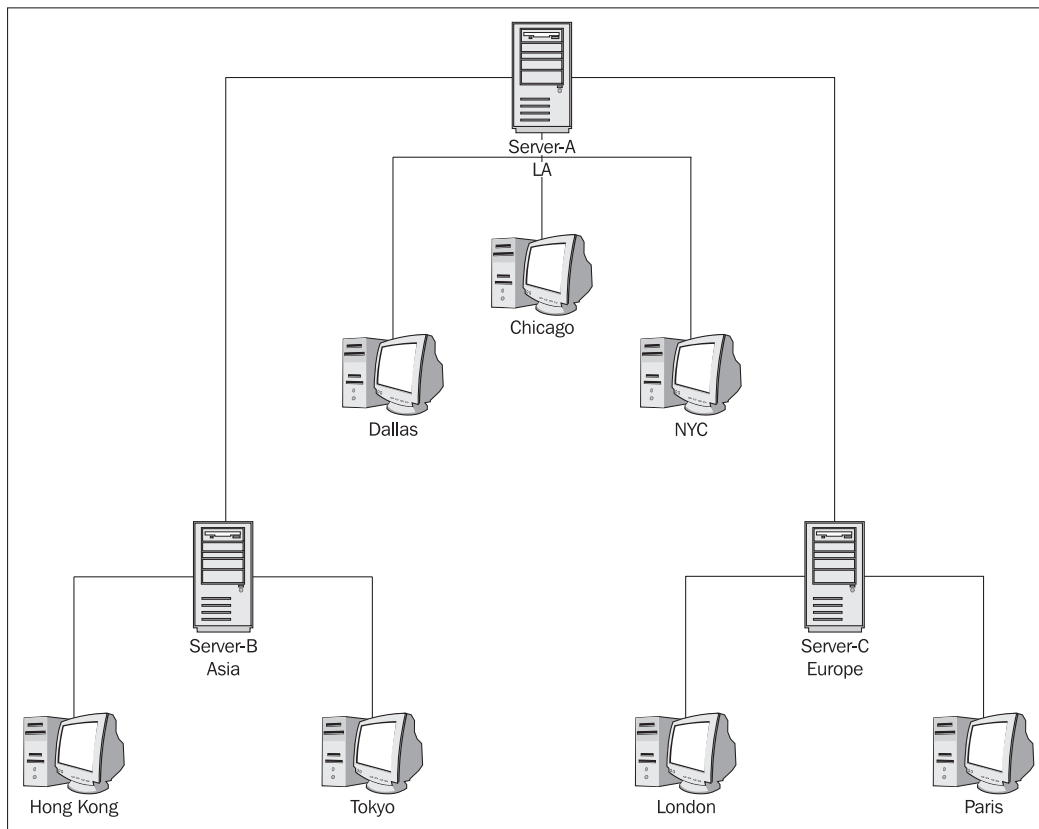
## Domino Domain Monitoring (DDM)

One of the most significant new Domino 7 features—one that's gotten a lot of attention throughout the early beta programs—is Domino Domain Monitoring (DDM). This feature allows you to monitor the status of multiple servers in one or more domains, all from a single location.

DDM uses a set of preconfigured probes to gather status and process information about the servers being monitored. These probes collect data relating to applications, databases, directories, messaging, the operating system, replication, security, the server, and the Web. Special filters allow you to select the type and level of data recorded by the probes. After this data has been collected, it is consolidated, organized, and processed into easy-to-read summary reports. The data is then entered automatically into the Event Resolution Center (ERC). Each event that is processed and placed into the ERC database has a document link back to the specific monitor that generated the event. The ERC is updated with a status document each time a probe detects an error, or a particular threshold is exceeded. By viewing DDM events recorded in the ERC, you can identify (and in some cases even predict) systemic Domino events. The ERC is automatically created when you start the first server. The ERC database is based on the new template `ddm.ntf`; by default its file name is `ddm.nsf`.

By default, results generated by DDM probes are placed in the ERC on each server that runs the probes. You can create a DDM server collection hierarchy to aggregate data from several servers to a single server. By using this collection hierarchy, you can designate that a single server can collect all DDM-based event data (and thus use this single server to monitor multiple servers in your domain). Alternately, you can set up several servers to collect data across a domain.

The following figure shows how you can set up servers to collect DDM data in a worldwide domain. In this case, we use a multi-tiered collection model. The top server in our example is Server A in Los Angeles. This server collects data from itself and three other collection servers located in the USA. Collection Server B, located in a data center in Asia, collects data for itself and two other servers in Hong Kong and Tokyo. Collection Server C collects data from itself and two servers located in London and Paris.



Reported data is generated in each ERC based on its location in the collection architecture. To review data about the London server, an administrator can open the ERC on Server C, where data for the London and Paris servers is stored. It's also possible to view London data by opening the ERC on Server A, which contains all DDM data for all servers in the hierarchy.

This collection hierarchy is possible because each Domino 7 server writes its own probe results into a local ERC replica on each collection server. As a result, the ERC maintains data about its own probes as well as the probe data from every server that is monitored by this server. As you can see from the preceding figure, data is rolled up and pushed into the collection server that represents the next higher level in the tree. This process is managed by Lotus Notes **replication**. Selective replication formulas are automatically created when you create the DDM server hierarchy. Using this simple technique, you see the rolled up data where you want to see it—for instance, in the figure, data from Hong Kong exists on Server B (the Asia server) and Server A (the top-level server), but not on Server C (the Europe server).

## Probes

Probes are the internal engines that make DDM work. There are nine types of probes available in Domino 7:

- **Application code** monitors an agent's schedule and resource (CPU and memory) usage.
- **Database** monitors database status and various activities.
- **Directory** monitors various directory functions.
- **Messaging** monitors the Domino-based messaging infrastructure.
- **Operating System** monitors operating system statistics and events.
- **Replication** monitors various replication activities. Replication probes can be configured to monitor all database replication, or specific databases.
- **Security** monitors the overall security of servers and databases in the domain.
- **Server** monitors the administration process for errors and reports them back to the ERC database.
- **Web** monitors web field settings and HTTP configuration fields.

Each of these probes is described in more detail later in this section.

## Configuring Probes

You can select which probes you want to run, and what data these probes collect, through Probe documents. These documents reside in the Events database (events4.nsf).

Through Probe documents, you can specify when the probe runs. Many probes can be configured to run on a schedule, on an event, or real-time. The function of the probe will dictate what type of schedule can be executed. For example, if you select the Schedule option, you can choose to run the probe:

- Multiple times per day (including the time between each probe execution)
- Daily (including the days of the weeks and the time when the probe will execute)
- Weekly (including the day and time for the probe to run)
- Monthly (including the calendar day number that the probe will execute; for example, if you want the probe to run on the fifteenth day of each month, enter 15)

In some cases (for example, the Security probe), you can enable the probe to run when a particular event occurs, such as when a Person, Server, and/or a Configuration document has changed. This can provide a very quick alert back to an administrator. You can also determine how missed probes are handled—you can ignore the missed probe, run the missed probe on startup, or run it at the next time range.

One very convenient feature is the ability to assign probe events based on server type. For many probes, you can select an option called **Special Target Servers**, which offers a set of server types, including:

- The Administration server of the Domino Directory
- LDAP server
- POP3 server
- IMAP server
- SMTP server
- Mail server
- Scheduled directory catalog aggregation servers

For instance, if you select the type as mail server, the probe will run on *all* mail servers in your domain.

## Filters

You can create DDM filters to control the event type and event severity of events generated inside and outside of DDM. These filters determine what data is included in the DDM log file. You can specifically include all DDM events or include/exclude specific type of events. The DDM filter is created in the `events4.nsf` database. After the filter document has been created, you can determine the following for each filter document:

- **Description:** Provides explanatory information about this filter.
- **Event Filter Type selection:** Offers two choices: apply filter to DDM and non-DDM events, and apply filter only to non-DDM events.
- **Event Types and Severities to Log:** Determines which event types are recorded in the ERC. You can choose to log all event types, which would record all the types of events and all severity levels shown in the following figure. Or you can choose to log selected event types. If you choose this option, you can then select the types of events and their levels of severity.
- **Servers on which the filter will be applied:** Identifies the servers on which this filter will apply. You can choose all servers in the domain, or select the option **Special Target Servers** to specify the type of server for this filter (as described in the preceding section). You can also identify individual servers by name.

## The Event Resolution Center (ERC) Database

The Event Resolution Center (ERC) database (`ddm.nsf`) contains the data generated by active DDM probes. When a probe runs, it records all the relevant data that it finds (if any) to a report that is placed in the ERC. This report contains the results of the specific probe, the probable cause that generated the result, suggested solutions for each event, and a link to the probe that was used to generate this event.

The ERC includes seven navigator views and a link to `events4.nsf`. Each view can help you find and/or diagnose a particular problem. The views are as follows:

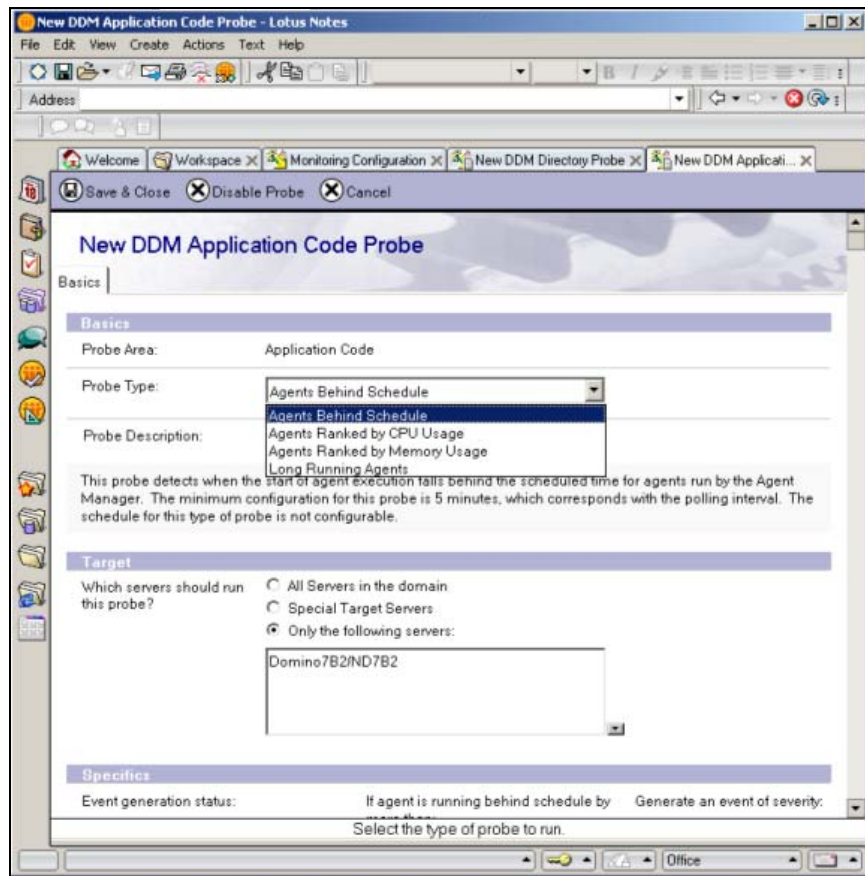
- By Severity shows a list of probe results documents organized by severity level (Fatal, Failure, Warning (high), Warning (low), and Normal).
- By Type shows the probe results by the probe type (Application Code, Messaging, and so on).
- By Server displays results based first on the domain names, and then by a list of servers that the probes reported on.
- By Date shows all probe events in chronological order.
- By Assignment provides you with the ability to assign events to people and/or groups.
- My Events shows the events that are assigned to your username. This is a formula-based view (`@Name([Abbreviate]; @UserName)`).
- Open Monitoring Configuration provides a link to `events4.nsf`.

## Types of Probes

As we mentioned earlier, there are nine types of probes. You select the type of probe you want to create in the Probe document:

### Application Code

This probe monitors an agent's schedule and resource usage. It also checks for agent-related conditions and events such as agents that are disabled by the design server task, agent security errors, and agent full-text index errors resulting from search operations.



## Database

The Database probe monitors database status and activities such as database compacting errors and design errors, as well as status on the ability to actually open this database. This probe has four different probe types that you can enable:

- Compact reports errors about the status of many server-based database compaction activities.
- Design reports any errors that occur during the design process.
- Error Monitoring is a very powerful database probe type. This monitors a number of database activities, including the internals of the **Notes Storage Facility (NSF)** and the **Notes Indexer Function (NIF)**. The following screen shows the configuration document for this probe option:

The screenshot shows a configuration window for a probe. The 'Basics' section includes 'Probe Area: Database', 'Probe Type: Error Monitoring', and a 'Probe Description' field. Below this is a text box explaining that the probe monitors key locations in the database software layer (NSF/NIF) and generates event documents for any errors that occur. The 'Target' section has three radio button options: 'All Servers in the domain', 'Special Target Servers', and 'Only the following servers:'. The third option is selected, and a text box below it contains 'Domino7B2/ND7B2'. The 'Specifics' section has a 'Severity' dropdown menu set to 'Warning (high)'. At the bottom, there are two buttons: 'Add Error Codes To List' and 'Remove Error Codes from List'.

Note the option to remove error codes from the list of errors that are to be recorded. By default, a number of error codes are automatically ignored, such as "Document has been deleted", "Entry not found in index", "File does not exist", and so on.

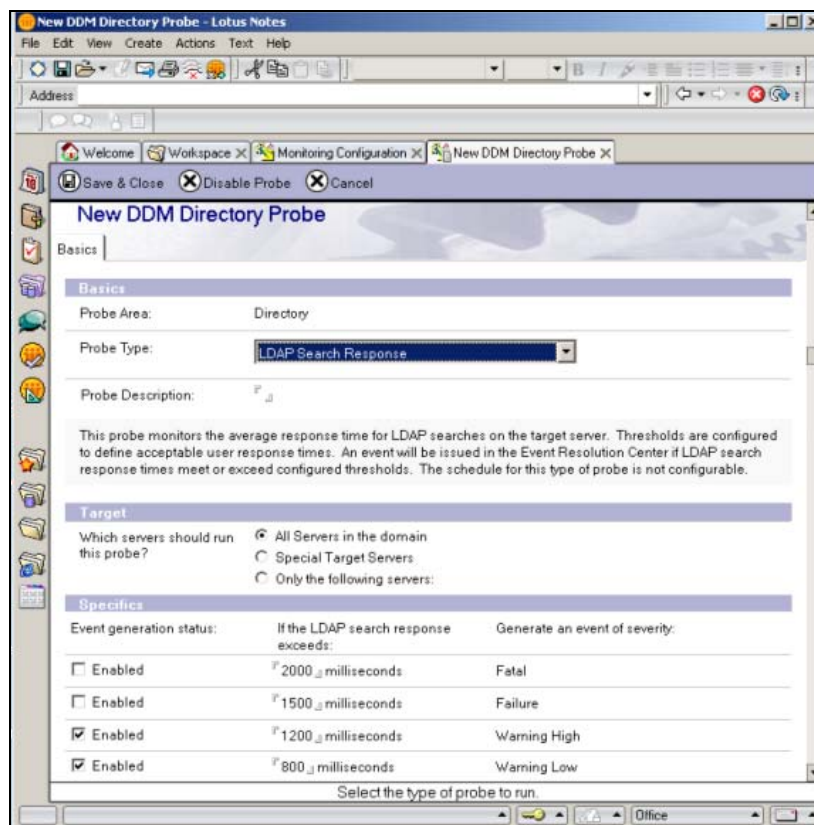
- Scheduled Database Checks 'pings' each database to check whether the selected database can be opened. Additional options for this include the ability to check for unused space in the targeted database and for any database inactivity.

## Directory

The Directory probe is one of our favorites. This powerful probe monitors many different directory functions:

- Directory Availability monitors the availability of all directories being hosted and then reports any identified errors. The directories that are monitored can include the primary Domino Directory (names.nsf), Domino configuration directories, directory catalogs, directories enabled via directory assistance, and LDAP directories.

- Directory Catalog Aggregation Schedule monitors the scheduling of the Directory Catalog. The Directory Catalog is maintained by the DirCat Domino server tasks. This option monitors the schedule status of the task looking for scheduling elements, including missed directory aggregation and any aggregations that are taking too long to process.
- Directory Catalog Creation monitors the server-based DirCat Directory Catalog task process that creates the directory catalogs. This helps you take quick action to get this task back online.
- Directory Indexer Process State monitors the running status of the Directory Indexer.
- LDAP Process State monitors the status of the LDAP Domino server task.
- LDAP Search Response monitors the server's average search response time for LDAP searches. This can be configured via a set of thresholds. The following figure shows that there are four different events that can be generated based on each threshold, Warning Low, Warning High, Failure, and Fatal:



- LDAP TCP Port Health monitors the TCP port response for both the standard LDAP TCP port (389) and the LDAP-SSL port (636).
- LDAP View Update Algorithm monitors the algorithms that are used to update the LDAP server directory views. This algorithm can be tuned by using the LDAPBatchAdds NOTES.INI setting.
- NAMELookup Search Response monitors the average search response time of directory NAMELookups performed on the Domino server.
- Secondary LDAP Search Response monitors the average search response time of searches of secondary LDAP servers that are performed on the probed server.

## Messaging

The Messaging probe monitors the Domino-based messaging infrastructure. Features include the ability to monitor SMTP activity, Notes (NRPC) mail routing, and various mail-routing statistics. There are currently ten options that you can choose from:

- Mail DSN tests the SMTP mail flow using a Delivery Status Notification (DSN) technique. This can help you determine whether a particular site is online. This can be effective if the target domain supports DSN extensions.
- Mail Flow Statistic Check uses a metric known as the 'slack percentage' to monitor a series of messaging-based statistics, including Mail.Total.Pending, Mail.Dead, Mail.Held, and Mail.Waiting. This lets you monitor the quantity of mail moving through the Domino server. The slack percentage is a representative indication of how the router is processing mail.
- Mail Reflector provides a mechanism to test mail flow to a variety of mail systems. You specify a mail recipient as part of this configuration, but you also will need to configure the recipient to send the message back to the originating server. One method is to enable auto-forward messages from the mail recipient to an ISpy mail-in database on the server that is executing the probe.
- Message Retrieval Process State verifies that the IMAP and POP3 server tasks are executing properly on the server being probed.
- Message Retrieval TCP Port Health monitors the Domino Internet Message Access Protocol (IMAP) and Post Office Protocol (POP3) messaging protocols, and reports service status on each process. Additional options include the ability to monitor POP3SSL and IMAPSSL.
- NRPC Routing Status tests the status of the Notes NRPC mail router by placing a message in the mailbox. This message will then route to a mail-in database. This can report status based on a set of thresholds.

- Router Process State monitors the status of the Domino router server task.
- SMTP Process State monitors the status of the Domino SMTP server task.
- SMTP TCP Port Health verifies that the SMTP mail routing services are working correctly.
- Transfer Queue Check tests SMTP- and/or NRPC-based mail to individual destinations. This can be configured via a set of thresholds and can report when messages are not being delivered.

POP3 is defined in RFC-1725, and IMAP4 is defined in RFC-1730.

## Operating System

One of the many challenges that an administrator must deal with is the status of system resources. Operating System probes provide a mechanism to alert you about potential problems at the OS level. There are four types of Operating System probes that you can enable: CPU, Disk, Memory, and Network.

- CPU monitors the CPU performance status on a variety of operating systems. The following operating systems and statistics can be monitored:

OS	Statistics monitored
AIX	Processor utilization percentage Processor queue length
zOS	Processor utilization percentage
Linux, zLinux	Processor utilization percentage
Solaris	Processor utilization percentage Processor Queue Length
OS400	Processor utilization percentage
Windows	Processor utilization percentage

Each selection can be configured with a high/low threshold based on each statistic percentage.

- Disk monitors and analyzes disk activity on each Domino server. The following table shows operating systems and statistics that can be monitored:

OS	Statistics monitored
AIX	Disk utilization percentage
Linux, zLinux	Disk utilization percentage Disk Service Time (ms)
OS400	Disk utilization percentage
Solaris	Disk utilization percentage Disk service time (ms)
Windows	Disk queue length

- Memory monitors and analyzes memory performance on each Domino server:

OS	Statistics monitored
AIX	Scan rate
OS400	Fault rate formula
ZOS	Available frames Out ready queue length Paging rate
Solaris	Scan rate
Windows	Available physical memory (MB)

- Network monitors and analyzes network performance on each Domino server:

OS	Statistics monitored
AIX	Network bandwidth utilization percentage Network collision rate percentage
Linux; zLinux	Network collision rate percentage
OS400	Network bandwidth utilization percentage
Solaris	Network bandwidth utilization percentage Network collision rate percentage
Windows	Network bandwidth utilization percentage

## Replication

The Replication probe lets you monitor various replication activities within your Domino domain. Replication probes can be configured to monitor all database replication, or

replication on specific databases. There are two options available with this probe: Errors and Replication Check.

- Errors monitors replication events for errors. Any errors found are captured in a report that can include a document link for any document that did not replicate. There are several associated configuration settings that you can enable, including:
  - Which servers should run this probe?
  - Which servers should be probed?
  - Select one or more databases to probe:
  - Select one or more databases not to probe:

You can also monitor push- and/or pull-type replication events.

- Replication Check monitors specified database replication activities. Previous releases of Domino offered similar functionality, but this included replications, which resulted in the replication history being updated. Therefore, only successful replications were indicated. This new probe type takes null replication into consideration. You can enable the same configuration settings that you can with the Errors probe type, described in the preceding paragraph. In addition, you can generate an event if the included databases have not replicated within the following interval, and choose to attempt to diagnose problems:

Replication Probe: DADN-6AB3VT	
Basics   Schedule	
<b>Basics</b>	
Probe Area:	Replication
Probe Type:	Replication Check
Probe Description:	asdf
<p>This probe monitors configured database(s) to ensure that replication occurs on the target servers within the configured time interval. If a database has not replicated within the configured time interval, it will generate an event in the Event Resolution Center database. <b>Note:</b> This probe takes into account replication attempts which did not actually replicate notes (i.e. databases which are up to date).</p>	
<b>Target</b>	
Which servers should run this probe?	All servers in the domain
Which servers should be probed?	All servers in the domain
Select one or more databases to probe:	All Databases
Select one or more databases not to probe:	
<b>Specifics</b>	
Severity:	Warning (high)
Generate an event if the included databases have not replicated within the following interval:	6 Hours
Check the following	<input checked="" type="checkbox"/> Push

## Security

You can create a Security probe to assess the overall security of servers and databases in your domain. A Security probe can identify a security-related server configuration problem and/or security issues with specific databases.

One significant variable with security probes is how the event severity is assigned. Severity is assigned during runtime and is calculated based on the number of various potential issues found. This severity is a percentage-level score that is generated for each Server Configuration document analyzed. (Consult the product documentation for details about how these percentages are calculated.) The basic percentages are shown in the following table:

Probe percentage	Severity level
0.00	Normal
< = 50%	Warning (low)
> 50%	Warning (high)

There are five Security probe types: Best Practices, Configuration, Database ACL, Database Review, and Review.

- **Best Practices** compares a set of baseline security configuration settings to the existing configuration in a Notes domain. You can modify the default values assigned to the security configuration. The following options are available for the Best Practices probe type:
  - Compare Notes public key against those stored in directory
  - Check password
  - Allow anonymous Notes connections
  - Required change interval
  - Check passwords on Notes IDs
  - Check for existence of ID file in the person document
  - Internet authentication
  - Check the security of SSL settings
  - Check the security of Web settings
  - Check the security of Domino Directory settings
  - Check the security of Mail settings
  - Check the security of DIIOP settings
  - Check the security of the Remote Debug Manager

- Use more secure internet passwords
- Security settings in my Configuration document
- Internet password
- Verify all Server Document Security Tab sections. (This includes the Admins, Program, Web, Security Settings, Server Access, and Passthru Use sections.)

**Security Probe: TSPD-67MPKD**

Basics | Specifics | Schedule

**Basics**

Probe Area: Security

Probe Type: Best Practices

Probe Description: The probe

This probe can be configured to audit various security settings found on Server documents, Server Configuration documents, and Person documents. A best practices probe will review & analyze key fields in these documents and generate detailed reports, recommending settings that might improve Security for the configured areas.

**Target**

Which servers should run this probe?

All Servers in the domain

Special Target Servers

Only the following servers:

Domino7B2ND7B2

Which servers' security configurations should be probed?

All Servers in the domain

Only the following servers:

Domino7NSFND7B2

Select one or more databases not to probe:

TheBaseFishingDatabase.nsf

**Basics TAB**

- Configuration compares a known 'good' Domino server document and a target server document, and then reports any differences or discrepancies. This type of security probe also has a Specifics section that you can configure. This allows you to compare a known good server configuration to the server being probed. Options include:
  - Which server should be used as the guideline server?
  - Which server settings should be compared to the guideline server's settings? You have several options here: Directory Profile Note, Security settings in the Server Configuration document, Server document (all sections or individual sections such as Admins, Program, Web, and so on).
- Database ACL monitors the Access Control List (ACL) of individuals and groups in various databases. You can set this up to monitor specific databases and list access levels in the probe configuration document. You can also

check the access level status of any particular group. For instance, suppose you have a group known as 'External Contractors'. This group needs access to the 'Bass Fishing' Database with read-only access. You can configure a probe to monitor this critical database and report whether this group has been given an access level greater than Reader. This particular probe has the ability to monitor all basic ACL access levels, including Designer, Editor, Author, Depositor, Reader, and Default.

- **Database Review** is the 'inverse' of Database ACL. This monitors changes in access levels for all ACL members against a specific ACL level. You can create a probe and then select a database for it to monitor. You can then select a base level to monitor, for example review all ACL members whose privileges are equal or greater than Editor. You can also select one of the following parameters:
  - Review the following database properties: enforcing consistent ACLs across replicas, enabling of extended ACLs, encryption settings, and the Administration server of the database.
  - Review agents defined as restricted or unrestricted.
- Review creates a report on the security settings specified in the Specifics tab of the Security Probe document. You can select the same settings available for the Configuration type of security probe.

## Server

The Server probe monitors the administration process for errors, and reports the errors back to the ERC database. The following administration requests can be monitored:

- Change HTTP password in Domino Directory
- Change user password in Domino Directory
- Initiate rename in Domino Directory
- Initiate web user rename in Domino Directory
- Recertify Certificate Authority in Domino Directory
- Recertify Cross Certificate in Domino Directory
- Rename in person documents
- Rename person in calendar entries and profiles in mail file
- Rename person in Domino Directory
- Rename web user in Access Control List
- Set Password Information

## Web

The Web probe monitors Web-related statistics and events. You can select from two probe types, Web Best Practices and Web Configuration:

- Web Best Practices monitors HTTP configuration fields in the domain by comparing these fields to recommended base 'best practices' values. Fields that don't match these values are recorded in a report in the ERC database. This allows you to:
  - Verify that server is using the most current web server configurations
  - Verify basic web server configuration settings
  - Verify web server performance settings
  - Verify web server debug-log settings
  - Verify web server security settings
- Web Configuration monitors web field settings in relation to a base configuration document. As with Web Best Practices, settings that do not match the base configuration are reported to the ERC. The settings you can monitor are similar to Web Best Practices settings.

After you open the configuration setting for a Web probe, you will notice that you cannot assign severity levels. The severity of an event generated by Web probes is determined using a percentage formula. This score is based on the number of potential problems that are found. After this calculation is complete, a 'severity percentage score' is calculated and logged to the ERC.

## Event Notification Using an Agent

Domino has the ability to monitor and execute specific actions based on a large variety of events. These events can be the results of normal processing activities or can be error-type events. Event examples include:

- AdminP
- Agent
- Comm/Net
- Compiler
- Database
- Directory (LDAP)
- Mail

- Misc
- Monitor
- Network
- News (NNTP)
- Replica
- Resource
- Security
- Server
- Statistic
- Update
- Web (HTTP/HTTPS)

With Notes/Domino 7, the Domino administrator now has several new options that can be triggered by an event. When an event takes place, an administrator now has the option to run an agent, run a program (with new parameters), send a console command to the server, or send a Java controller command.

Domino 7 includes processes called 'event generators'. These generators gather information by monitoring Domino tasks and statistics. Also, there is a built-in probing system that can be enabled and linked into the event generators. Specific conditions and/or thresholds can initialize event generators. Once an event generator has been started, it can pass data into the event monitor task. The event monitor task can be loaded manually at the Domino server console, or can be set to load each time the server is started via the NOTES.INI file, in the servertasks line. Once the event has been passed into the event monitor task, it will be processed against event handler configuration documents in the events4.nsf database. If there are no configuration documents defined, then no actions are executed when an event is passed into the event handler.

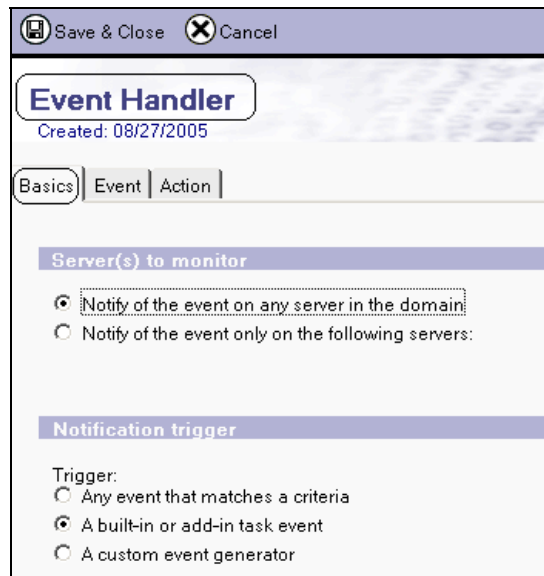
The Domino Administrator includes a set of default event generators; these are shown in the Event Generators view of the Monitoring Configuration database (events4.nsf). The following table lists the types of event generators that can be created:

<b>Event generator</b>	<b>Description</b>
Database event generator	Monitors database activity and free space. Monitors frequency and success of database replication. Reports on ACL changes, including those made by replication or an API program.
Domino server response event generator	Checks connectivity and port status of designated servers in a network.
Mail routing event generator	Sends a mail-trace message to a particular user's mail server and gathers statistics indicating the amount of time, in seconds, it takes to deliver the message.
Statistic event generator	Monitors a specific Domino or platform statistic.
Task status event generator	Monitors the status of Domino server and add-in tasks.
TCP server event generator	Verifies the availability of Internet ports (TCP-based services) on servers and generates a statistic indicating the amount of time, in milliseconds, it takes to verify that the server is responding on the specified port.

Each event document can have a severity assigned. The severity levels can be assigned to each event as needed. Examples of these are shown below:

<b>Severity level</b>	<b>Meaning</b>
Fatal	Imminent system crash
Failure	Severe failure that does not cause a system crash
Warning (high)	Loss of function, requiring intervention
Warning (low)	Performance degradation
Normal	Status messages

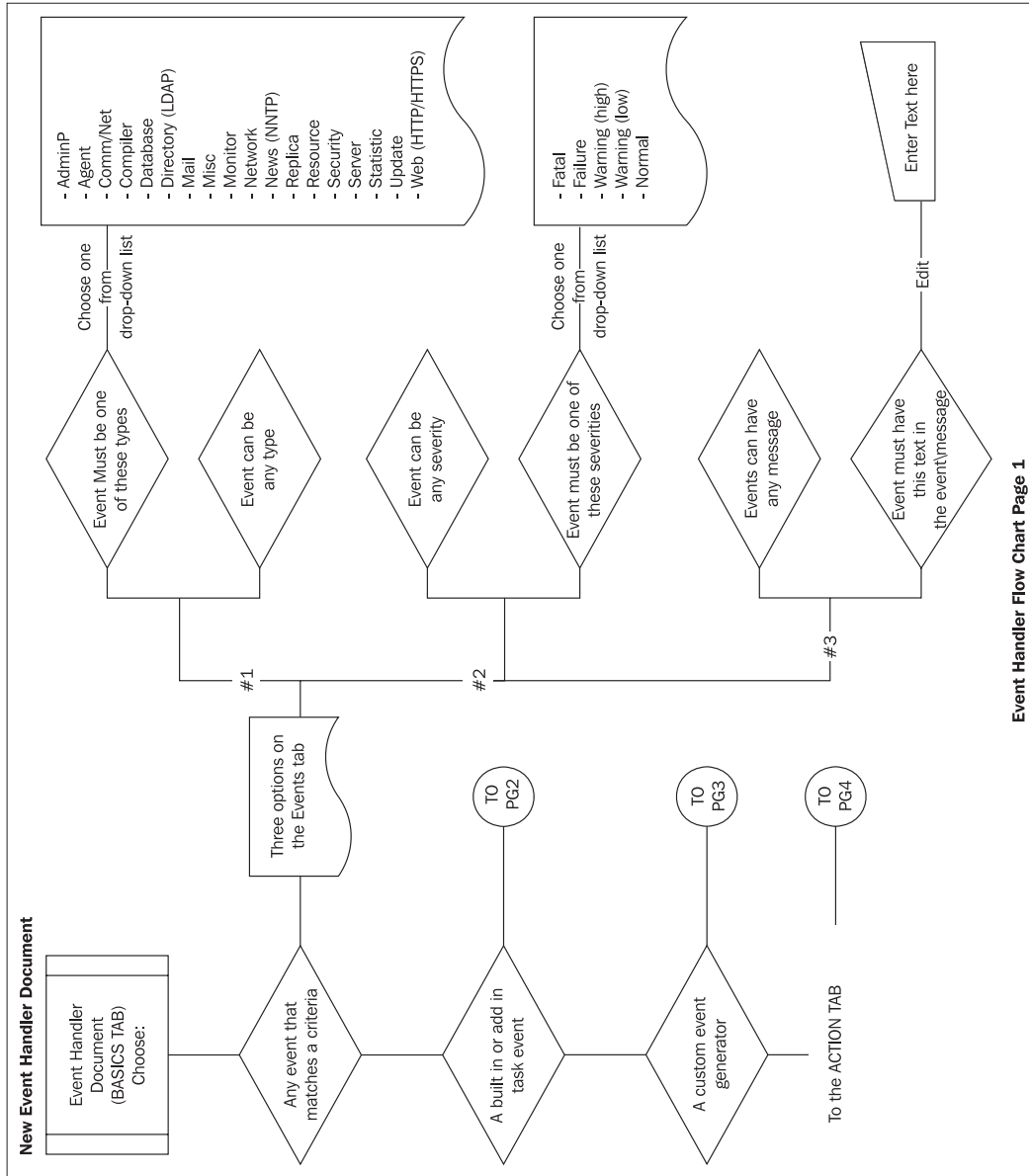
To create a new event, just open the events4.nsf and select New Event Handler. The following screenshot shows how this looks:



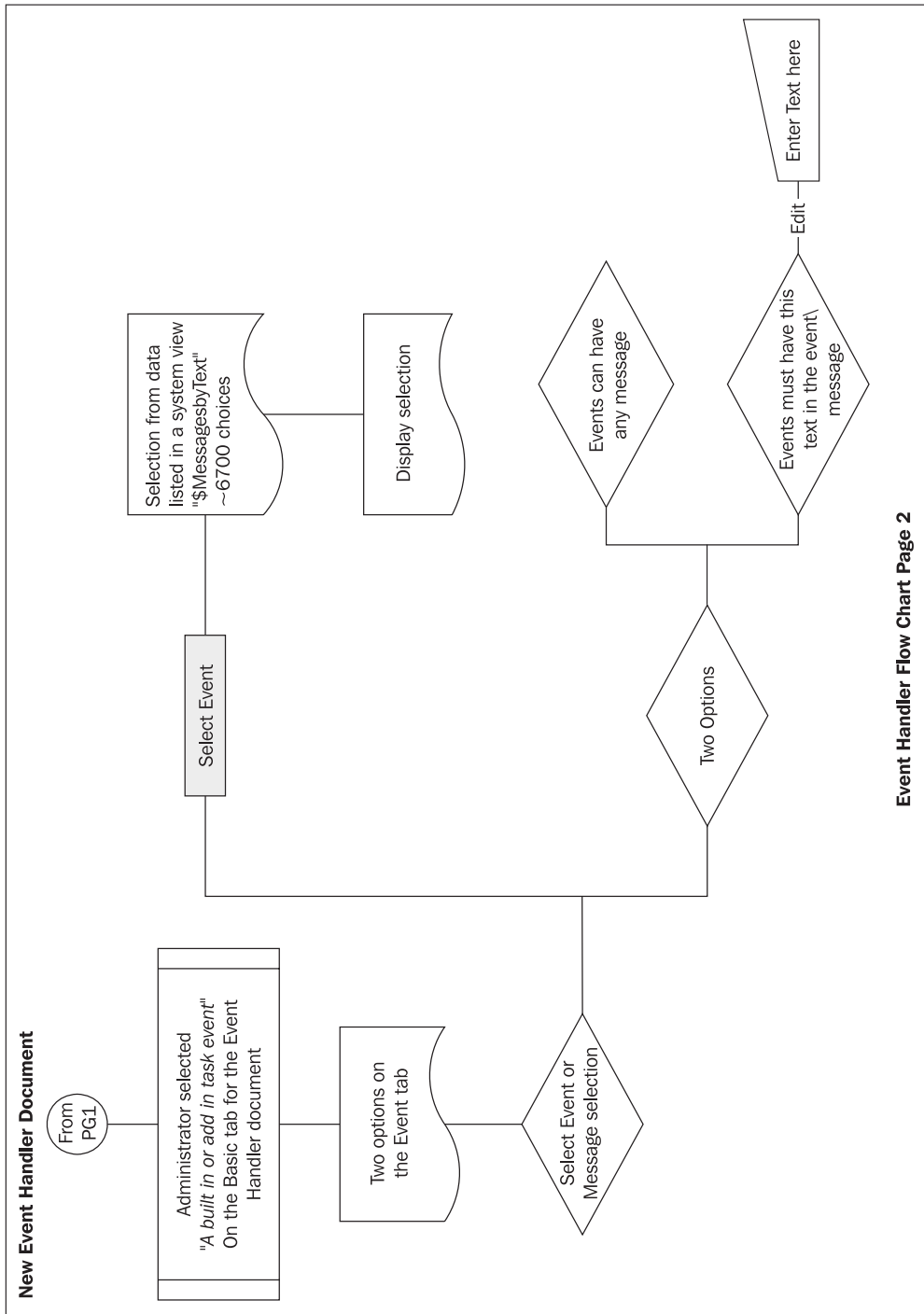
There are three tabs: Basics, Event, and Action. The Basics tab provides two basic sections: Server(s) to monitor and Notification trigger. The first section is where the servers to monitor are set. The second section has three choices:

- Any event that matches a criteria
- A built in or add in task event
- A custom event generator

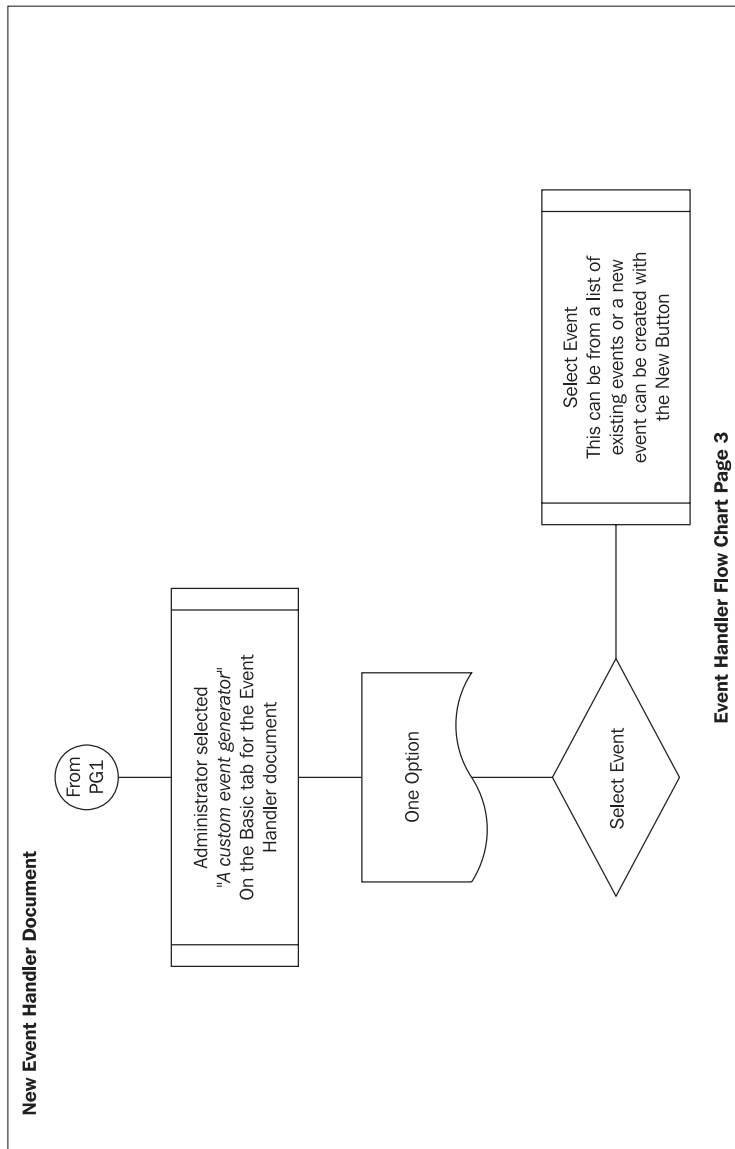
Each choice will display additional choices on the Event tab. The following illustration shows these choices:

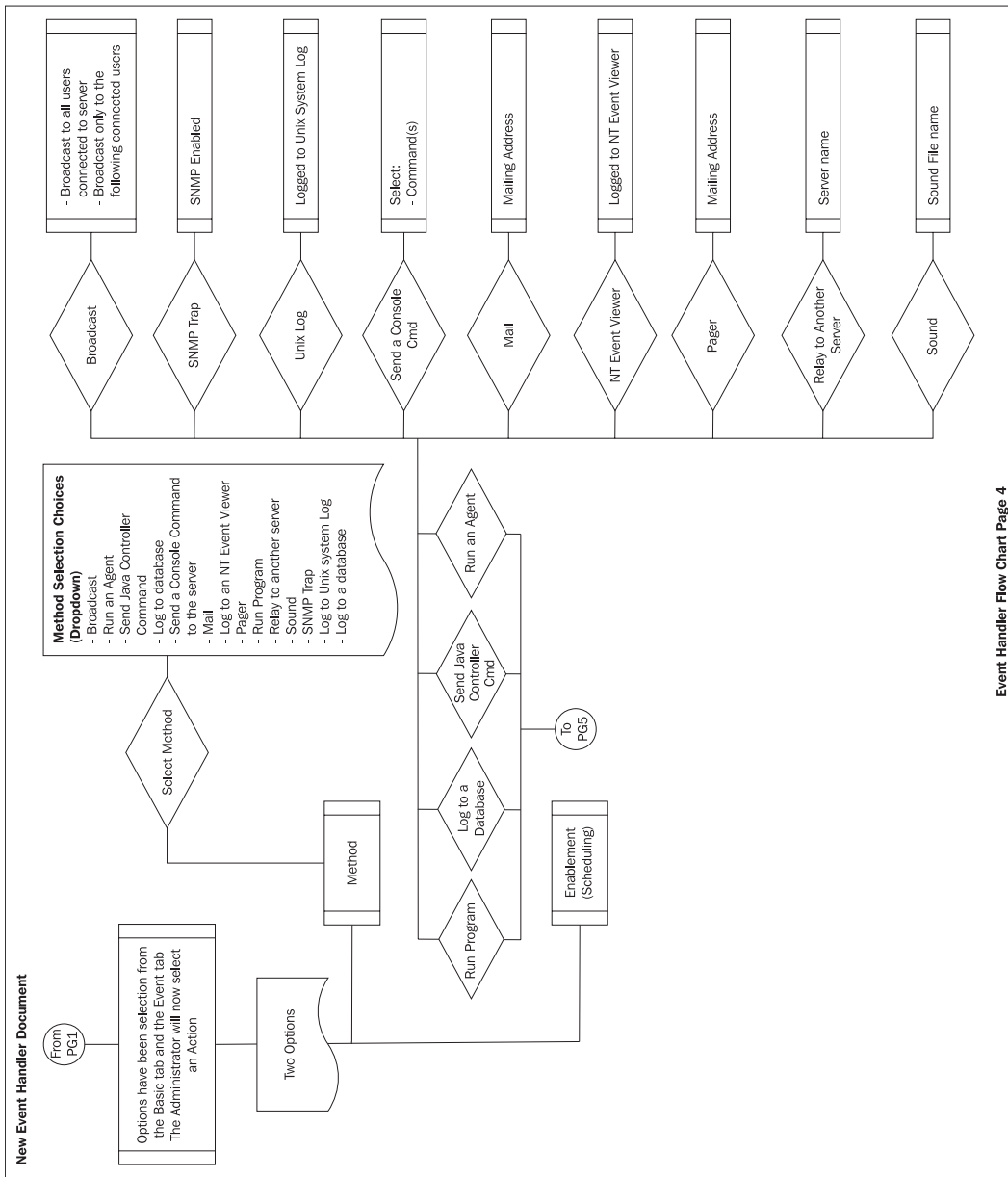


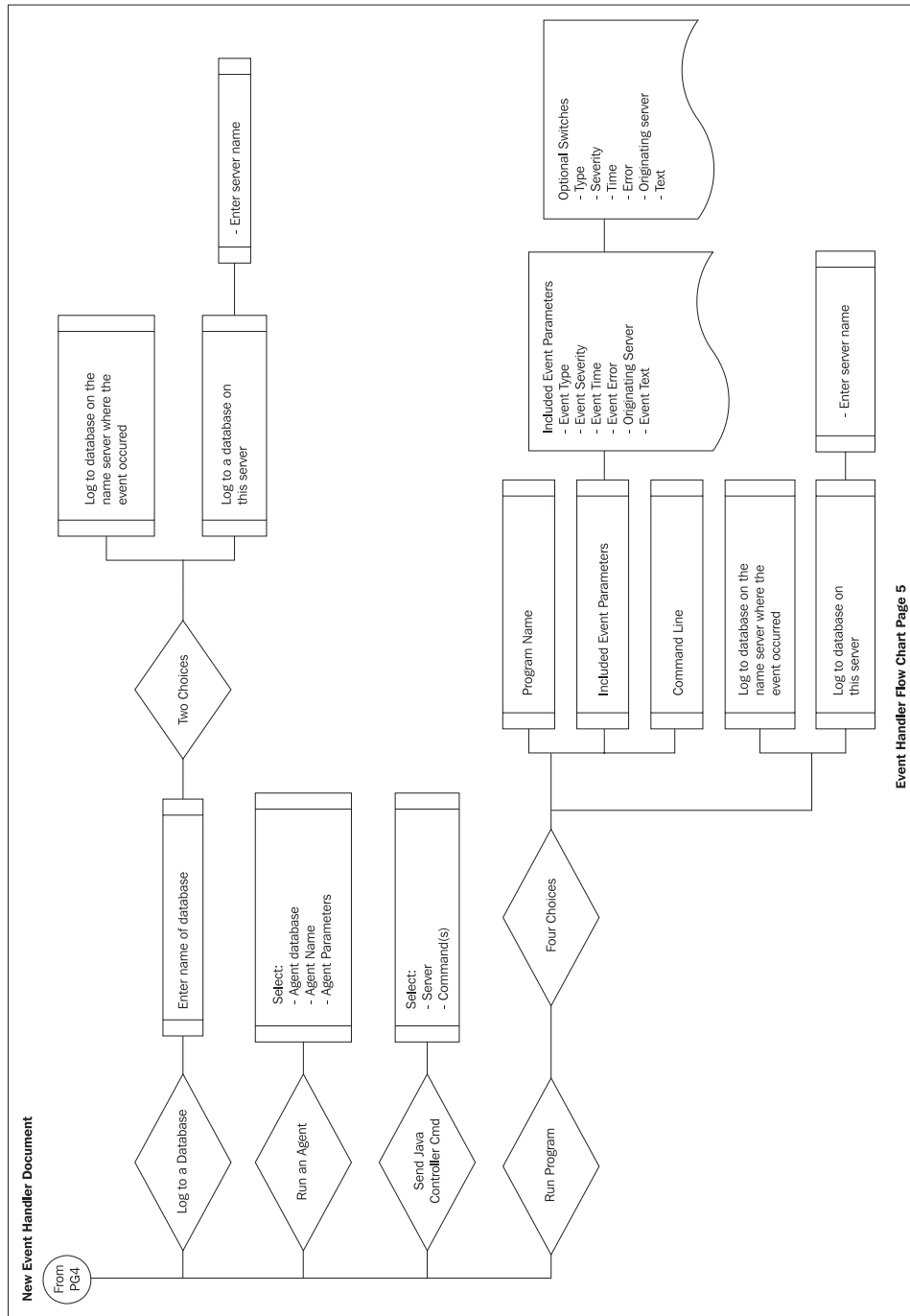
Event Handler Flow Chart Page 1



Event Handler Flow Chart Page 2







Event Handler Flow Chart Page 5

The administrator can create an event handler document to specify how to log the event to a specified destination. Also, administrators can prevent events from being logged or handled in any circumstance.

At this point, you might be asking, "What is this scripting stuff that I keep hearing about?" Let's start with an example and a goal. The goal is to send a notification and track ACL notifications in a log database. Use the following steps:

1. Create a tracking database.
2. Create a simple agent, view, and form in the tracking database.
3. Create a database event generator document in events4.nsf.
4. Create an event handler (run an agent).
5. Enable the event handler and the event generator.

## Create a Tracking Database

Overall, almost any database format will work. Once the database has been created, you will need to create a form, agent, and a view.

## Create a Simple Agent, View, and Form in the Tracking Database

The form can have the following fields defined:

Field name	Field Data Type	Field Description
EventText	TEXT	Text of event
TargetServer	TEXT	Target server for this event
EventTime	TIMEDATE	Time and date stamp of event
EventType	NUMBER	Type of event
EventSeverity	NUMBER	Severity of event
EventPrms	TEXT	Text parameters in event
ErrorCode	TEXT	Event type error code
OriginatingServer	TEXT	Server that originated the event
EventSeverityText	TEXT	Textual representation to Severity
EventTypeText	TEXT	Textual representation to Type

Here's a screenshot example of a form:

Event Results from Event Agent	
Event Information for server = <input type="text" value="OriginatingServer_1"/>	
Event Severity Data:	<input type="text" value="SeverityText T"/> <input type="text" value="EventSeverity T"/>
Time of Event:	<input type="text" value="EventTime T"/>
Target Server	<input type="text" value="TargetServer T"/>
Event Parameters	<input type="text" value="EventPrms T"/>
Target Database	<input type="text" value="TargetDatabase T"/>
Event Severity Text / Type:	<input type="text" value="EventSeverityText T"/> / <input type="text" value="EventTypeText T"/>
Event Type error code	<input type="text" value="ErrorCode T"/>
Event type name:	<input type="text" value="EventType T"/>
Event Informational Text	
<input type="text" value="EventText T"/>	

Create a default view as well. Any view will do; you can customize it as you like.

Next up is the agent. Below is a sample agent that you can base your agents on. Name the agent EventAgent. This agent uses the DocumentContext method. This method is a Read-only property. Basically, an in-memory document is created when an agent starts. This method is defined in the NotesSessi on class, and uses NotesDocument as its data type.

The basic syntax for the DocumentContext is:

To get: `Set notesDocument = notesSessi on.DocumentContext`

```
Sub Initialize
    Dim session As New NotesSessi on
    Dim doc As NotesDocument
    Set doc = sessi on.DocumentContext
    Print "Event Text = " & doc.Eventtext(0)
    Print "Event Error Code = " & doc.errorcode(0)
    ' Document Information
    Call Doc. Save(True, True)
    Set db = sessi on.CurrentDatabase
    Set tardoc = db.CreateDocument
    tardoc.form = "EventForm"
    tardoc.Subject = "Event Information"
    tardoc.EventText = doc.Eventtext(0)
    tardoc.EventPrms = doc.EventPrms(0)
    tardoc.ErrorCode = doc.ErrorCode(0)
    tardoc.EventSeveri ty = doc.EventSeveri ty(0)
    tardoc.EventSeveri tyText = doc.EventSeveri tyText(0)
End Sub
```

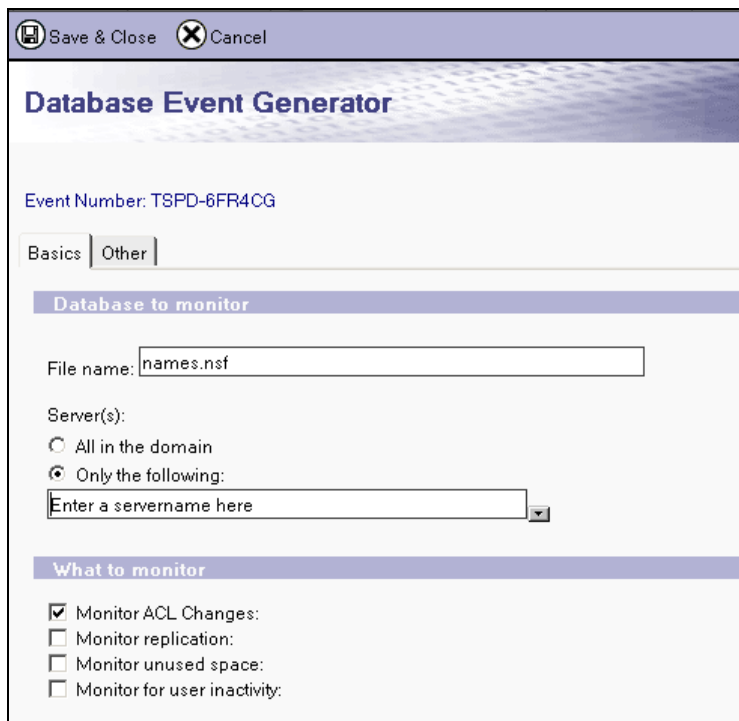
```
tardoc.EventTime = doc.EventTime(0)
tardoc.EventType= doc.EventType(0)
tardoc.EventText = doc.EventText(0)
tardoc.EventTypeText = doc.EventTypeText(0)
tardoc.OriginatingServer = doc.OriginatingServer(0)
tardoc.EventErrorCode = doc.errorcode(0)
Call tardoc.Save( True, True )
Print "Agent Complete ! ! ! "
End Sub
```

Don't forget to:

- Sign the agent
- Add the correct permission into the security document in order for the agent to run
- Make sure the events process is loaded on the server

## Create a Database Event Generator Document in events4.nsf

Open the events4.nsf database on the server and select New Database Event Generator. Enable the event generated to monitor ACL changes for names.nsf. Here's an example screenshot:



Notice the TSPD-6FR4CG string in the screenshot. You will see a similar string, and it can be used as a reference point for the event handler.

## Create an Event Handler (Run an Agent)

In events4.nsf, you can also create the event handler document. Using the flowchart as a reference, select New Event Handler. We'll now take a look at the changes/settings to be made.

### Basics Tab

Select and complete the following fields (refer to the first screenshot under the *Event Notification Using an Agent* section):

- Notify of the event only on the following servers
- A custom event generator

### Event Tab

Select the event using the reference string from the event generator. Once this is selected, you will be able to see details on that document.

### Action Tab

Select Run an Agent. Complete the following fields:

- Agent Database (use the name of your new database)
- Agent Name: EventAgent (from the preceding example)
- Agent Parameters (any specific parameters and/or field names from your form)

## Enable the Event Handler and the Event Generator

On the Action tab, enable the event handler and set a schedule if needed.

### Testing

It is now time to test your event handler, agent, and event generator. Open the names.nsf database on the server where you have enabled each of the event handlers and the generator. Make a simple change to the ACL of the names.nsf database. As soon as this happens, you should see a display on the server console and a document created in your database. An example is shown in the following screenshot:

Event Results from Event Agent	
Event Information for server = Domino7NSF/ND7B2	
Event Severity Data:	3
Time of Event:	11:03:51 PM Yesterday
Target Server	
Event Parameters	
Event Severity Text / Type	Warning (high) / Security
Event Type error code	Event Monitor0x33A3
Event type name:	2
Event Informational Text	
The ACL in database names.nsf has been changed by Tim Speed/Dallas/IBM.	

## Summary

In this chapter, we have taken a detailed look at Domino Domain Monitoring (DDM), one of the major new administration features introduced in Domino 7. We reviewed the set of pre-configured probes that gather status and process information (applications, databases, directories, messaging, the operating system, and so on) about the servers being monitored. We discussed the Event Resolution Center (ERC), where processed events are placed. We also talked about event monitoring, Domino 7's ability to monitor and execute specific actions based on a large variety of events. These events can be the results of normal processing activities and/or error-type events. The next chapter discusses the Administration process.

# Upgrading to Lotus Notes and Domino 7

If you're reading this book, you're probably already familiar with Lotus Notes/Domino. You know about all the powerful productivity features offered by this product (actually multiple products, although most of us in the Notes/Domino universe still think of it as one). You know how much your company relies on it to communicate, collaborate, and manage its collective store of corporate knowledge. (An industry analyst once described Notes as something you can't quite define, but within 15 minutes of using it you realize you can't live without it.) And you realize (perhaps all too well) that upgrading from one major release to the next can be a significant undertaking, especially if you maintain a 'mixed' environment that includes multiple versions of Notes and/or is integrated with other third-party products.

This book is intended to help you with that task. It is specifically intended for upgrading to Notes/Domino 7, the latest release of the product. But much of the information we provide is also applicable to any Notes/Domino version, and can be used as a general guide whenever it comes time to upgrade to the next major release.

This book has been written by Notes/Domino 'insiders'. Collectively, we possess decades of Notes/Domino experience; we've been with the product since Notes 1.0, and since then have worked directly with customers to help them with their Notes/Domino upgrade and deployment issues. This book represents a compendium of what we've learned during that time. It addresses all the major issues that we've seen customers wrestle with during their upgrades. Our goal is to help you avoid these issues when possible, and work around them when it's not. At the same time, we identify considerations that are unique to Notes/Domino 7, to help you understand and prepare for all the exciting new capabilities offered in this release.

## What This Book Covers

*Chapter 1* puts Notes and Domino into their historical contexts, showing how Notes turned from college students' dreams into a major business product.

*Chapter 2* takes you on a tour of the new features of Notes and Domino, laying a foundation for the chapters that follow.

*Chapters 3-6* take a deeper look at the new features: DDM and event monitoring, AdminP, Policy Management, and the Smart Upgrade process.

*Chapter 7* looks at performance issues. *Chapter 8* moves the focus to the Notes/Domino 7 clients, while *Chapter 9* looks at how users can access Notes/Domino through Domino Web Access 7.

For More Information: [www.packtpub.com/upgrading\\_lotus/book](http://www.packtpub.com/upgrading_lotus/book)

*Chapters 10-12* deal with the technical issues of programming Notes/Domino, managing security, and then bring the topics so far together with a practical look at the upgrading process.

*Chapters 13-15* look even further into the new features of domino. *Chapter 13* explores WebSphere integration, and *Chapter 14* shows how and why Domino/Notes 7 works with directories to maintain its data. *Chapter 15* concludes the feature exploration with a look at integrating Notes/Domino 7 with Microsoft Outlook.

*Chapters 16-17* round off the book by looking at some troubleshooting methods, followed by a case study that shows how developerWorks Lotus team made their Notes/Domino 7 upgrade work for them.

## **Where to buy this book**

You can buy *Upgrading to Lotus Notes and Domino 7* from the Packt Publishing website: [http://www.packtpub.com/upgrading\\_lotus/book](http://www.packtpub.com/upgrading_lotus/book).

Free shipping to the US, UK, Europe, Australia, New Zealand and India.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.



[www.PacktPub.com](http://www.PacktPub.com)

**For More Information: [www.packtpub.com/upgrading\\_lotus/book](http://www.packtpub.com/upgrading_lotus/book)**