Scenarios of Use for SecurTrac Auditing

For Domino/Notes Applications

1 West Pearce Street, Suite 400
Richmond Hill, Ontario, Canada L4B 3K3
Tel: 1 (905) 709-8602 Fax: 1 (905) 709-8604
www.extracomm.com
DOCID SOUST0207

Background

As a Notes Administrator or Application Developer, you may come across some situations or requests from users that there isn't an easy solution or workaround, or no solution at all. SecurTrac is designed to fill those gaps and make your life easier. Described below are some of the most commonly asked questions or scenarios that sound familiar to you in your daily work, let's see how SecurTrac handle them.

Scenarios

How can I get notified of a Group document change, Who did it, and What has been changed?

People tend to use groups to maintain the mailing list, server, database or document access control because groups management provides flexibility and easy maintenance.

There are difficulties gathering information on group document changes in an existing environment if you do not have an efficient monitoring system.

Example 1:

If someone is added to the Administrator's or Directors group, then that person will have the access rights of Administrator or Directors respectfully. As a result, the sensitive information that originally should be read by Administrator or Director, may also be read/modified by this added person.

Example 2:

If someone is added to the Director group, that person will receive the email which is addressed to the Directors group. It is not easy to observe by the sender or receivers because the recipient list (To, CC, BCC) displays only the group name.

In the normal situation, it is very difficult to trace which individuals in the group received the mail. No one will monitor the group change because there may be hundreds or thousands of groups in the network.

You may have the time to monitor group changes, but you can only look at document $UpdatedBy and $Revisions to find the modification history. The real problem is that you know somebody updated it but you don't know what has been updated. If the group modifier is added to the group and restores the original value later, then you will never know about the changes.

1 West Pearce Street, Suite 400
Richmond Hill, Ontario, Canada L4B 3K3
Tel: 1 (905) 709-8602 Fax: 1 (905) 709-8604
www.extracomm.com

How do I know when a user is added or deleted or modified from the Domino Directory and Who did it?

There may be hundreds or thousands of users in your Domino Directory. It is difficult to keep track of when a new user is added or when a user is deleted. In addition, you may also want to know when a user name, Internet email address or password is changed.

If you are a regional or country administrator, you may only be interested in your region or country's users. The flexibility of selective monitoring is important so that only relevant information is displayed.

My Domino Server behaves differently, what has been changed and who did it? What value should I restore?

A network may have many administrators all over the world. Another administrator may intentionally or unintentionally modify another administrator's Domino settings. Items that could be changed include Server document, Configuration, Connection document. Modifying this document may result in changing your server security settings or even crash your server.

For example, some inexperienced administrator may even delete documents mistakenly. If the administrator deleted your server document, then your server will be down immediately. It is really difficult to determine who made the deletion. Furthermore, modifying the connection documents may result in undelivered mail or returned mail.

In addition, it is also difficult to trace the change of Notes.ini file. If you misspell some of the parameters, your server cannot reboot. In addition, the Notes.ini file also contains security settings such as who is the administrator and who can access the TCPIP, COM ports and other resources.

Keeping track of settings and related changes are important, but this change tracking is difficult within the confines of a dynamic, functioning network environment.

My document has been changed, what has been changed, what was the original value? My document disappeared, who deleted it? I don't have a backup, can I get it back?

Users may say, "hey…something is wrong with the databases, some documents have suddenly disappeared."

What can you do?

The normal interrogation process is to find out:

- Who did it? (so that you can talk to the user to avoid this disaster to happen again.)
- What documents were modified or deleted? (so that you can restore the documents from backup)

This can be a time consuming challenge that may not yield all the answers required.

Some mails in my mailbox suddenly disappeared? Have the user received and read my mail?

Some users may mistakenly delete messages in their mailboxes and blame the mail system. Some users may pretend they never receive the read the mail.

1 West Pearce Street, Suite 400
Richmond Hill, Ontario, Canada L4B 3K3
Tel: 1 (905) 709-8602 Fax: 1 (905) 709-8604
www.extracomm.com

How can I monitor a particular event without scanning the Notes Log manually?

There are huge amount of messages generated in the Notes Log everyday. However, you may want to review some of messages that appear in the Notes Log. For example, you may want to know:

- Who tried to open a sensitive database but was not successful?
- Whose mailbox threshold or quota was exceeded?
- Who started and closed a particular Notes user session?
- Who is using POP3 to retrieve email?
- How many servers not responding messages have been detected?
- Notes and Internet password does not match
- Attempts to guess the Internet password
- Who did create a new or replica database on the server
- Who did delete a database on the server

How can I monitor specific user mail traffic?

You may suspect one of your staff is communicating with your competitor or sending some sensitive information out of the office. And you are asked to monitor a user's incoming and out going mails of the user. However, looking through the Notes Log will be a pain and the information provided is very limited.

How can I gather statistics and generate statistics report on mail traffic and document activity?

You may be asked to generate some statistics report on mail or database usage. You may also be asked to count the number of hits of a certain document.

How can I get notified when documents are opened, added, updated, or deleted from my database?

For example, if a request is approved, an email notification will be sent to alert the application owner. If someone posts a question to the forum, alert the forum owner.

How can I enable audit trail on the selected applications? But I don't want to modify the existing applications' design.

Existing application may not have audit requirements in the past. Adding audit trail requires understanding the whole application logic and modification of the existing application design.

1 West Pearce Street, Suite 400
Richmond Hill, Ontario, Canada L4B 3K3
Tel: 1 (905) 709-8602 Fax: 1 (905) 709-8604
www.extracomm.com