Full Access Administration – Is it a threat in your Domino Environment?

Find out how you can use SecurTrac to monitor usage of Full Access Administration in IBM Lotus Domino.

Extracomm Inc.

12/10/2012

Full Access Administration – Is it a threat in your Domino Environment?

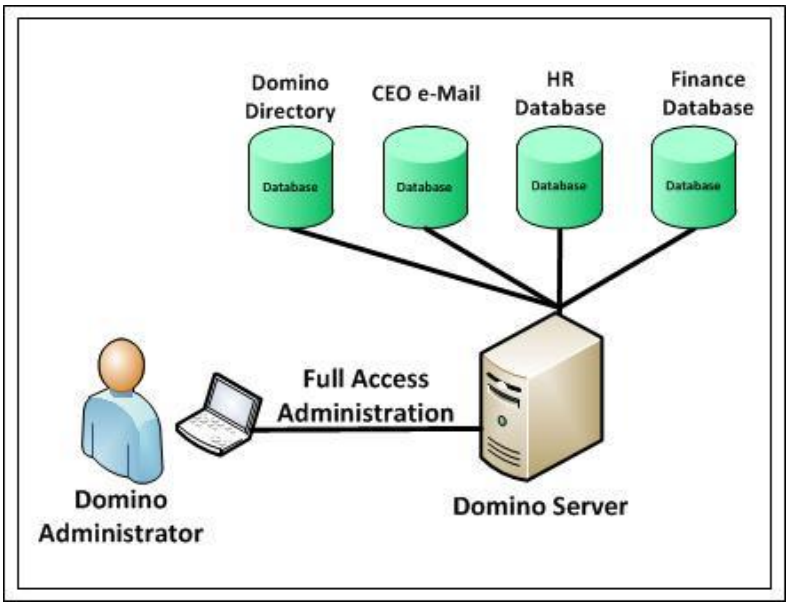
The Full Access Administration privilege is a very useful and powerful security privilege which allows Lotus Domino Administrators to correct many administration related problems such as misconfigured database ACLs, Domino Directory issues and user mail database problems. The Full Access Administration privilege is so powerful in fact; that it can actually be used to circumvent Lotus Domino server security and allow Domino Administrators to access and possibly make changes to Domino server configurations and even user mail database and/or application database content, without authorization.

With corporate governance and regulatory compliance being more prominent in companies, is yours able to account for each administrator's actions while the Full Access Administration privilege is active? If an audit was to be performed, are you able to provide detailed logging of everyone's activity? How can we control and audit this very powerful tool?

Have you ever wondered what exactly your Domino Administrators are doing when they invoke the powerful Domino server Full Access Administration privilege? Though every IT employee likely has a clause in their employment contract which states that they will never abuse their powers which might allow them to access information for which they are not authorized, how do you really know if employees are complying? Companies put a trust into their employees, fully expecting them to comply with company data access policies. Even with employment contracts and employee trust, this brings to light some very important questions:

Could they be using Full Access Administration to ……..

1) access the e-mail database of the CEO or another high profile executive? What are they doing while they are in there? Reading confidential email?, Deleting e-mail? Sending e-mail? or even altering the content of existing e-mails?
2) access the Domino Directory and make unauthorized changes to Person documents, Group documents or even Server configurations?
3) get access to Domino applications databases to Create, Open, Update or even worse Delete documents without authorization?
4) make unauthorized database ACL changes?



The fact of reality is in many cases who really knows what it is that they are doing when using Full Access Administration?

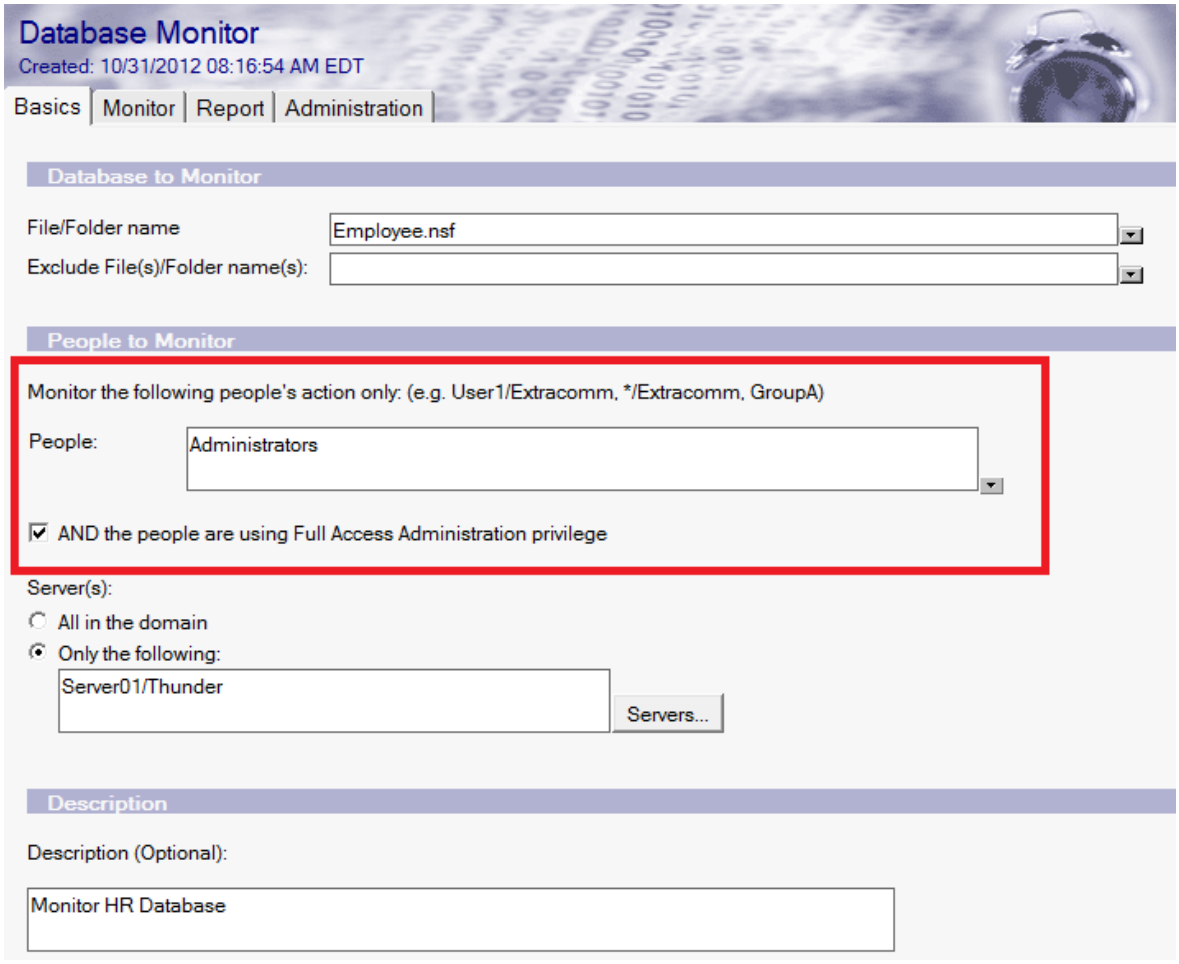
While Lotus Domino does allow you to log every time someone invokes the Full Access Administration privilege, what the basic logging mechanism does not provide is a full audit trail of the specific actions that were invoked while the Full Access Administration privilege was activated.

Extracomm's SecurTrac product fills this void and provides detailed audit trail logging of what exactly the Domino Administrator did while the Full Access Administration privilege was being used.

With SecurTrac you can……..

- Log Full Access Administration activity in Mail databases, Domino application databases as well as the Domino Directory for Create, Open, Update & Delete actions.
- Log the simple fact that a database was opened, even if no documents were ever accessed. This is especially important since every database has a default view, where document information is displayed in view columns, potentially exposing confidential information without someone ever needing to open a database document.
- Log exactly which database views were accessed in a particular database while using Full Access Administration.

SecurTrac Monitor Configuration



SecurTrac Log - Detected Usage of Full Access Administration

Log Information

Action Details

Initiator :	Notes Admin/Thunder	Time :	12/10/2012 11:09:41 AM EST
Database Title:	Employee Record Database	Database Path:	Employee.nsf
Form :	FEmployee	Action :	Open
Document ID :	OF8A26B18A:52CDE38B-ON852571DA:0058B1B7		
Last Updated By :	Billy Black/Thunder	Last Updated Time :	12/10/2012 11:08:48 AM EST
Triggered by Monitor :	Monitor HR Database	Used Full Access Admin privilege:	Yes

Connection Details

Service :	nserver		
Port Name :	TCPIP	Address :	192.168.0.145:54893

Document Details

Monitor Fields | RichText | Attachment

Field Name	Value
Comments	CEO
Details	
EmpDateOfBirth	08/30/1978
EmpDateOfHire	08/30/2006
EmpLeave	0
EmpName	Janet Smith
EmpNo	12345
EmpSalary	8000000
EmpSickLeave	0
Form	FEmployee
RichText	

To learn more about how SecurTrac can help monitor the use of Full Access Administration within your Domino environment, please visit our web site http://www.extracomm.com/SecurTrac/.

Extracomm Inc.

1 West Pearce St, Suite 400

Richmond Hill, Ontario

Canada, L4B 3K3

Tel: 905-709-8602

Fax: 905-709-8604

http://www.extracomm.com