Audit Manager

Project Chef: Neil Gower

Overview

- Audit Manager is designed to monitor and log changes to specific documents in Lotus Notes and Domino applications.
  - Configuration documents etc
  - Sensitive documents etc
  - Not designed to monitor every document in an .nsf
- It requires the installation of 2 templates, creation of 1 nsf, a server add-in, and a notes.ini change on the server.

Overview (cont)

- Requires an agent to be deployed in each .nsf to be audited (deployed by audit manager)
- Audit Manager supports Windows servers only

Suggested Uses

- Monitoring of changes in names.nsf
- Monitoring system configuration, keyword documents
- Monitoring business configuration, keyword documents
- Monitoring workflow documents
- Monitoring access to sensitive documents

Design

- Audit Manager is based on “Trigger Happy” by Damien Katz
  - http://www.openntf.org/Projects/pmt.nsf/ProjectLookup
  - http://damienkatz.net/
- Logging routine written by Julian Robichaux)
  - http://www.nsftools.com/

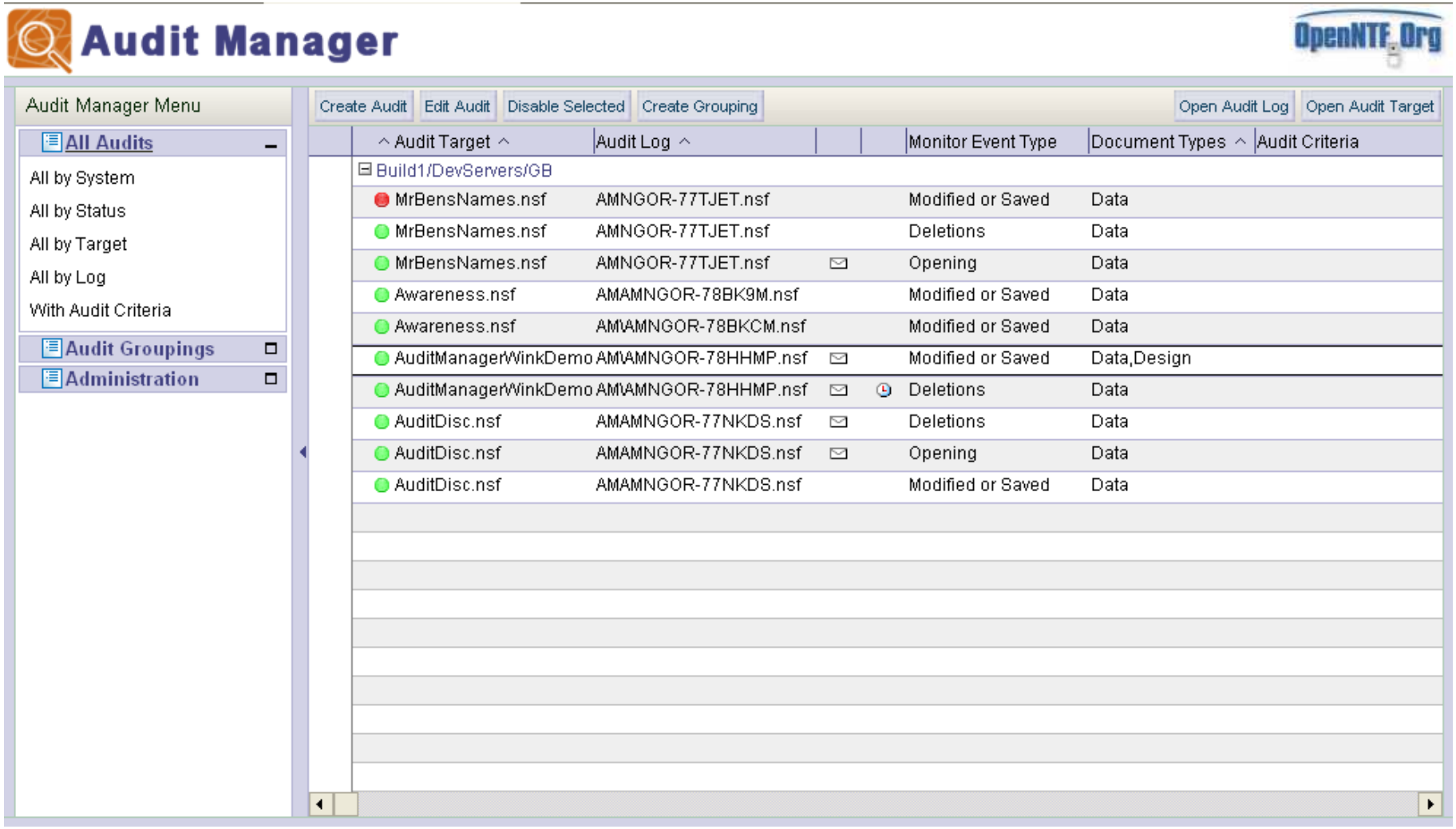
Design (cont)

- In reality Audit Manager is an extension of some excellent work done by other members of the Notes community designed to perform a specific task.

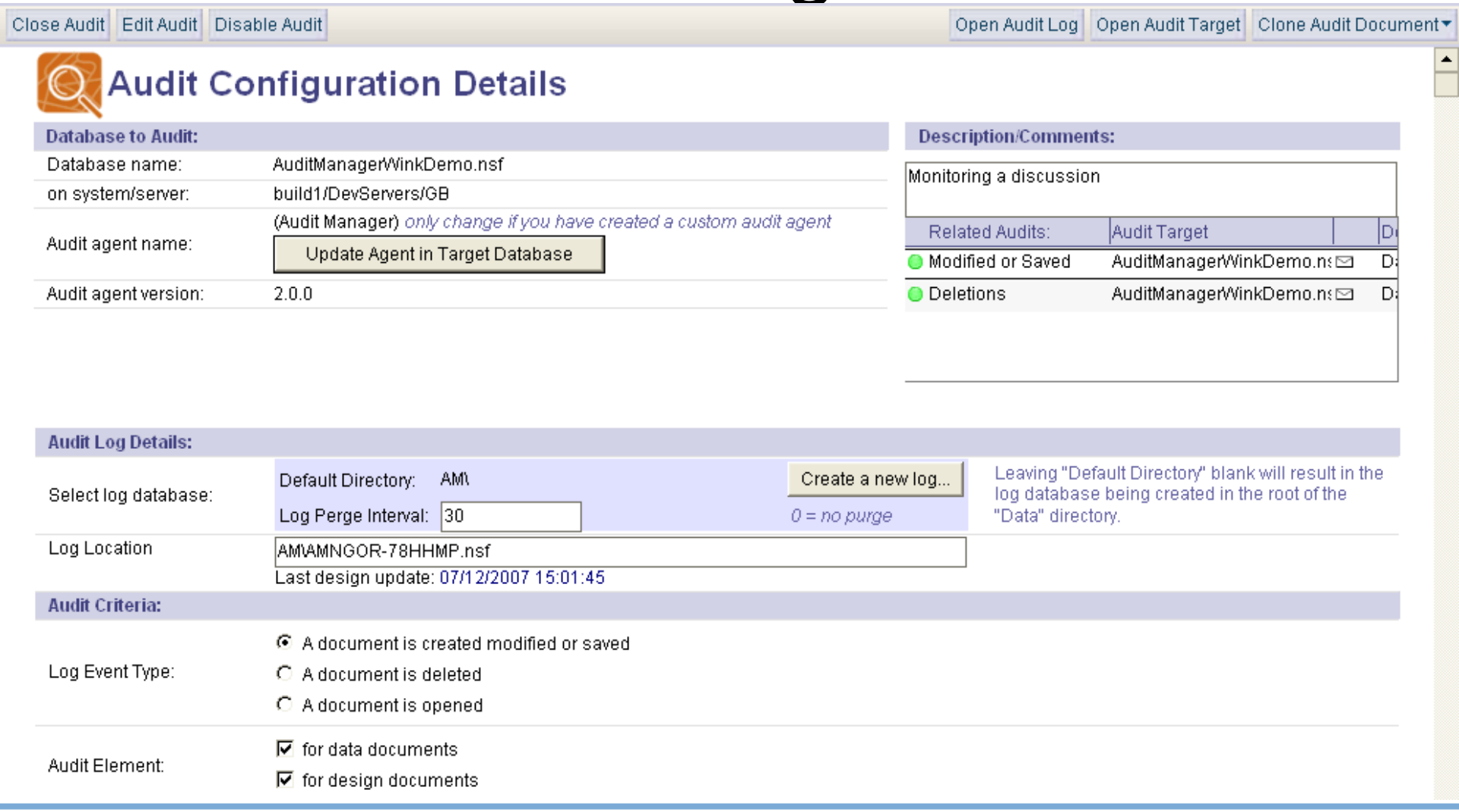
Functionality

- Create multiple “audits” to log document changes (create, open, update, delete) in a notes database.
  - Documents for auditing can be selected based on a standard note formula e.g. (Form=“payment” & Status=“Complete”)
  - All field changes on a document audited and recorded
  - Single document for each log

Multiple Audits



Audit Configuration



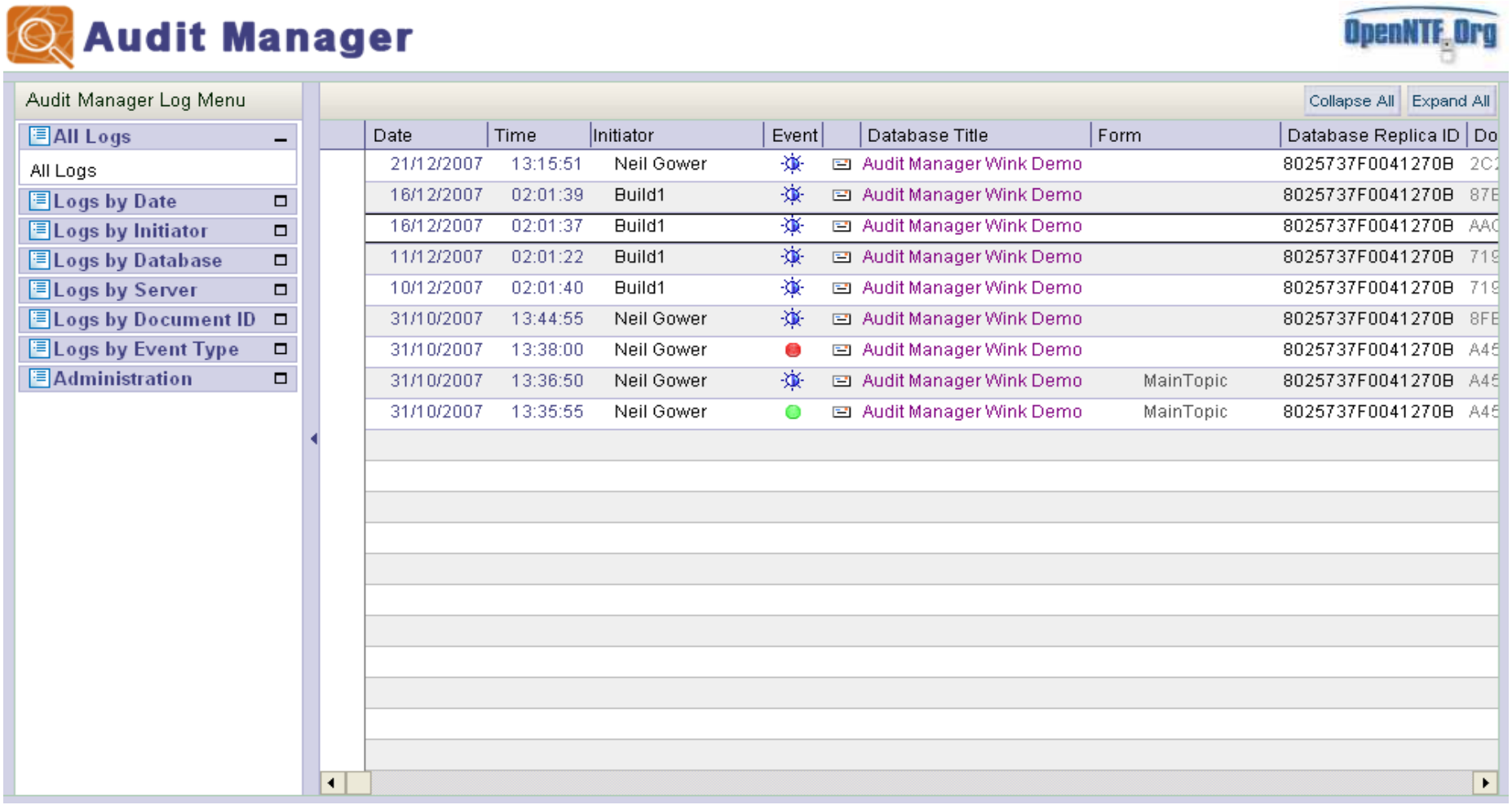
Audit Configuration (cont)

Audit Criteria:	☐ and only when this formula is true:	Monitoring all docments can have an impact on server performance, it is recommended that 'Audit Criteria' are used
Audit Exclusions:		If an 'auditable' event is triggered by anyone named in this field (people, or servers) then the event will **NOT** be audited.
Audit Notification:		
Email Notification:	Neil Gower/	If blank no email notifications will be sent
Notification Exclusions:		If the 'auditable' event is triggered by anyone named in this field (people, or servers) then the event will **STILL** be audited, but an email notification will not be sent.
Audit LifeCycle:		
Audit Start Date:	16	The audit will automatically be enabled on this date (blank for no start date)
Audit End Date:	16	The audit will automatically be disabled on this date (blank for no end date)

Functionality (cont)

- Automatic deployment and update of “Audit” agent in .nsf files.
- Automatic creation of “Audit Log” databases to store log documents
  - Created as part of defining an audit
  - Purge interval can be set upon creation, or changed at a later date

Log Database



Functionality (cont)

- Creation of a log document for each event, information recorded includes
  - All field changes (details content before and after change)
  - Who performed the change
  - What server the change occurred on
  - Event type
  - Document UNID
  - NoteID
  - Date /Time

Log Document

Close Log | Open Related Logs | Open Target Document | Open Audit Target

Audit Log Details

Log Details:	
Initiator:	CN=Neil Gower[redacted]
Database Title:	Audit Manager Wink Demo
Replica ID:	8025737F0041270B
Form Name:	
Server:	CN=Build1/O=DevServers/C=GB
Database Path:	AuditManagerWinkDemo.nsf
Document UNID:	2C2F7D9FA44AD3F8802573B5003AE0C7
Document NoteID:	386
Event Type:	Saved or Modified
Action Time:	21/12/2007 13:15:51
Email Notification:	Neil Gower[redacted]

Field '$AssistVersion' changed text value:
OLD: 18/12/2007 10:35:52
NEW: 21/12/2007 13:15:49
Field '$Comment' changed text value:
OLD: 2.0.0
NEW: 1.0.0
Field '$UpdatedBy' changed type:
OLD: NAMES
NEW: TEXT

Deployment

- Copy the two .ntf's into the root of the servers data directory.
- The "AuditManager.nsf" database is deployed in the root of the data directory on the server.
- The "ntrigger.dll" file is installed on the server
- The dll is then added to the servers .ini file
  - extmgr_addins=trigger.dll

Deployment (cont)

- Restart the server and you are ready to go
- Addition of a Notes agent in each “audited” database (automated)
- Full deployment documentation is provided in the “About” and “Using” this database documents in the configuration .ntf

Further Information

- OpenNTF
  - http://www.openntf.org/Projects/pmt.nsf/ProjectLookup/Audit%20Manager
- My Blog
  - http://www.ngower.me.uk
- Email me.
  - neil_gower@dominoconsultants.com