Modulo AUDIT di DocWay4

- Modulo attraverso il quale tutte le azioni svolte da operatori o processi sull'applicazione DocWay vengono tracciate e registrate all'interno di uno specifico database su MongoDB
- In caso di modifica di record (documenti XML su eXtraWay), all'interno del record di audit verranno registrate tutte le differenze (calcolate in formato JSON per successivo salvataggio su MongoDB) rispetto alla versione precedente del record
- La registrazione delle differenze in salvataggio avviene con una procedura a 2 step per avere la certezza di non perdere informazioni di audit (e garantire quindi un tracciamento completo delle modifiche) anche in caso di arresto del server Tomcat:
    - Prima del salvataggio del record su eXtraWay, viene prodotto un file di lavoro dell'autit (contenente tutte le informazioni necessarie alla registrazione su MongoDb) e salvato su una specifica directory su file system come "*lavoro in attesa*"
    - Se il salvataggio su eXtraWay restituisce errore, il file di lavoro in attesa viene rimosso dal disco
    - Se il salvataggio su eXtraWay si completa con successo, il file di lavoro in attesa viene riversato su MongoDB (specifica chiamata di save al client MongoDB) e rimosso dal disco
- In caso di errore riscontrato in salvataggio dell'audit su MongoDB (es. database MongoDB non raggiungibile) il file in attesa viene rinominato come "*fallito*". E' presente uno specifico JOB su DocWay che si occupa di analizzare la directory di lavoro dell'audit e verifica la presenza di file di errore e ritenta il salvataggio su MongoDB.
- La registrazione dell'audit sul salvataggio di record (calcolo delle differenze con la versione precedente) può essere abilitata anche su tutte le applicazioni integrate con DocWay, ad esempio 3diWS o MSA
- In caso di fallimento della registrazione dell'audit (o di altri errori ritenuti gravi) è possibile attivare l'invio di email di notifica ad amministratori di sistema. In questo modo sarà possibile riabilitare il tracciamento nel più breve tempo possibile
- E' possibile configurare l'audit in modo da ignorare interventi su interi archivi eXtraWay o specifiche tipologie di record o operazioni

N.B.: Visto che la registrazione temporanea dei dati di audit viene fatta su una specifica directory su file system, **è importante tenere conto della velocità di scrittura su questa directory per mantenere delle performance accettabili**.

Configurazione

- Per attivare il modulo di audit su DocWay (o altre applicazioni integrate con esso, quali 3diWS o MSA) occorre abilitarlo attraverso uno specifico set di properties definite all'interno del file *it.highwaytech.broker.properties*:

```
audit.enabled=false

# Parametri di connessione a MongoDB
#audit.mongodb.uri=mongodb://localhost:27017/dw4audit?safe=true&w=1
audit.mongodb.uri=
#audit.mongodb.dbName=dw4audit
audit.mongodb.dbName=

# Directory all'interno della quale registrare i dati temporanei e gli errori riscontrati sulla
registrazione dell'audit. Se non viene specificata alcuna directory, verra'
# creata ed utilizzata una directory 'dw4audit' all'interno della directory dei temporanei.
audit.workDir=

# Regular Expression da utilizzare per identificare eventuali seriali presenti all'interno
dell'XML aggiornato dall'utente e che saranno poi assegnati tramite eXtraWay. Nei
# casi previsti dalla regex il documento XML verra' ricaricato dopo il salvataggio su eXtraWay in
modo da registrare il seriale asssegnato all'interno dell'archivio
# di audit. Se non viene specificata alcuna regex si disabilitera' questo controllo
audit.serial.regex=(num_prot|numero)[ ]{0,1}=[ ]{0,1}\"\\S*-\\.\"

# Definizione di xpath conosciuti per i quali e' possibile definire un set di attributi (o
sottoelementi testo) che definiscono la chiave del nodo all'interno della
# ripetizione. In questo modo le differenze possono essere valutate sul singolo nodo di elementi
ripetibili e non sull'intera lista. Tutti i classici xpath ripetibili
# di docway e acl sono gia' gestiti a livello di codice (occorre definire eventuali xpath
ripetibili di campi custom).
# Il formato di definizione e' il seguente:
# audit.repeatableXPath.know.N=XPATH_DOT_NOTATION|KEY_VALUE[,KEY_VALUE]
```

```
# dove:
# - N rappresenta il numero progressivo di definizione del path
# - XPATH_DOT_NOTATION rappresenta l'xpath con separatore il punto (/doc/rif_esterni/rif ->
doc.rif_esterni.rif)
# - KEY_VALUE corrisponde ad un attributo o un sottoelemento di tipo test del nodo. E' possibile
specificare piu' valori separandoli con la virgola
# - la definizione del path deve essere separata dalle chiavi tramite pipe
# Esempio (in realta' gli xpath seguenti sono gia' gestiti di default):
# audit.repeatableXPath.know.1=doc.postit|@cod_operatore,@data,@ora
# audit.repeatableXPath.know.2=doc.link_interno|@href
# audit.repeatableXPath.know.3=fascicolo.link_interno|@href

# Tempo (in minuti) di sleep del thread di che si occupa di ritentare il salvataggio dell'audit su
MongoDB in caso di precedenti errori (default = 1 min)
audit.errorsJob.sleep=1

# Configurazione della casella per l'invio di email di notifica
# host
#audit.email_host=localhost
# porta
#audit.email_port=2525
# credenziali di accesso
#audit.email_username=
#audit.email_password=
# protocollo di invio
#audit.email_protocol=smtp
# indirizzo email utilizzato per l'invio
#audit.email_from_address=notifier@audit.3di
# nome alternativo dell'indirizzo email di invio
#audit.email_from_nickname=Audit Notifier
# indirizzo email al quale inviare le notifiche
#audit.email_to_address=admin@audit.3di

# Eventuale elenco di tipologie di record da ignorare su uno specifico archivio. Il formato di
definizione e' il seguente:
# audit.pne.ignore.N=DB_NAME|ROOT_NAME[,ROOT_NAME]
# dove:
# - N rappresenta il numero progressivo
# - DB_NAME corrisponde all'archivio sul quale applicare le esclusioni di tipologie di record
# - ROOT_NAME corrisponde al nome dell'elemento radice dei record da non registrare in audit. E'
possibile specificare piu' valori separandoli con la virgola
# - la definizione del nome db deve essere separata dagli xpath tramite pipe
# Esempio:
# audit.pne.ignore.1=acl|comune

# Elenco di archivi che devono essere ignorati dalla procedura di audit (nessun intervento sugli
archivi specificati verra' tracciato)
audit.dbNames.ignore=

# Elenco di azioni che devono essere ignorate dalla procedura di audit
audit.actions.ignore=

# Elenco di diritti (codici separati da virgola) per i quali deve essere mappata una specifica
azione in fase di audit delle attivita' degli utenti. Verranno analizzati
# tutti gli interventi svolti su diritti e identificate le variazioni su diritti speciali o
diritti di amministrazione
audit.acl.rights.dirittiSpeciali=ACL-16,ACL-30,ACL-DL01,ACL-SP01,ACL-AU01
# Per quanto riguarda i diritti di amministrazione, sono stati inseriti i codici degli applicativi
classici, vanno aggiunti tutti i casi specifici dell'installazione
# presso il cliente
audit.acl.rights.amministrazione=ACL-25,ACL-24-ACL,ACL-24-ACLCRAWLER,ACL-24-DW,ACL-24-TO,ACL-24-
SOGINSAP
```

- *audit.enabled* deve essere settato per abilitare l'audit sull'applicazione. Con l'attivazione occorre sicuramente settare anche le properties di connessione al database MongoDB

- *audit.workDir* corrisponde al percorso assoluto alla directory sulla quale verranno salvati i file temporanei di elaborazione dell'audit (prima di essere riversati su MongoDB)

Accesso da DocWay

Il pacchetto di distribuzione della console di Audit è disponibile su Nexus

Attenzione: le configurazioni della audit console il sistema le caricherà da /opt/<TOMCAT_HOME>/webapps/auditConsole/WEB-INF/classes

L'accesso alla console di Audit deve essere abilitato anche per alcuni operatori di DocWay, in base ad uno specifico diritto definito in ACL.

Il link di accesso alla console è visibile dal menù in altro di DocWay, sezione '*ALTRE FUNZIONI*' → '*Console di Audit*'.

Per poter abilitare il link occorre configurare le necessarie properties sul file *it.highwaytech.apps.generic.properties*:

```
# Abilita il link di accesso alla console di audit dall'applicativo docway ('si', 'no' - Default =
'no')
abilitaConsoleAudit=si

# Eventuale URL di accesso alla console di audit dall'applicativo docway (se non specificato non
verra' visualizzato il link per l'accesso alla
# console di audit direttamente da docway)
auditConsole.url=http://HOST[:PORT]/auditConsole/login
```

Oltre alle properties occorre verificare la presenza del diritto di accesso alla console sul file dei diritti *acl.xml*:

```
...
<group label="Diritti speciali">
  ...
  <right cod="ACL-AU01" label="Accesso alla console di Audit applicativo"></right>
</group>
...
```

N.B.: Se il file è stato personalizzato per la specifica installazione, occorre aggiungere la porzione XML relativa al diritto al file acl.xml presente all'interno della directory del configuratore (es. '*/opt/3di.it/confDocWay4-service/base/acl/diritti*')

Nota sui criteri di controllo relativi alle modifiche fraudolente dei record di audit

N.B: la presente nota è stata prodotta per fornire informazioni al Cliente SOSE.

- Quello che può garantire la 3D, anche per iscritto, è il software dell'Audit, e in particolar modo una sua componente interna sviluppata ad hoc dalla 3D.
- Questa componente tramite un sistema di chiavi crea un hash immodificabile per ogni oggetto del sistema (ovvero un info in formato json - registrazione di audit), utilizzando dei specifici criteri di sicurezza basati proprio sull'hash e sulla chiave utilizzata.
- Viene creato un hash utilizzando una chiave di n caratteri random (la chiave di default è 12, ma può essere selezionato di quanti caratteri farla: la sicurezza consiste proprio nel non sapere quanti caratteri vengono utilizzati).
- Gli algoritmi sono standard, per aumentare la sicurezza inseriamo gli n caratteri della chiave usati per creare l'hash in testa all'oggetto, e vengono messi davanti all'hash stesso.
- Si estrapolano gli stessi caratteri della chiave utilizzata per calcolare l'hash e si ricalcola l'hash esattamente nello stesso modo.
- Il confronto fra i due hash permette di verificare che siano uguali: se sono diversi, vuol dire che qualcuno ha modificato i dati dell'oggetto json direttamente nel db di mongo.
- Qualora l'oggetto del sistema (ovvero la registrazione dell'audit) venisse modificata direttamente nel database di mongo, il suo hash non corrisponderebbe più a quello originario calcolato dal sistema. Confrontando i due hash, emergerebbe immediatamente una modifica e dunque una manomissione del record tracciato dall'audit.
- Non possiamo garantire il db Mongo, in quanto non siamo amministratori delle macchine su cui è installato, e un utente di root potrebbe modificare le password del database ed accedere allo stesso. Quello che garantiamo è che se qualcuno

accede al db e modifica o cancella i record, tramite il sistema di confronto degli hash descritto sopra, l'ente sia a conoscenza che i dati nel database sono stati modificati direttamente nel database, in quanto garantiamo anche che non ci sono altri applicativi in grado di scrivere o sovrascrivere dati nel db di mongo usato dal modulo di Audit.