

Logování přístupů

Jak hlídat čtení dokumentů uživateli.
Včetně možností reakce...



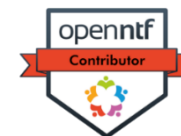
Představení



Ondřej Kostruh

NTF Factory

kostruh@ntf-factory.com



Proč logovat čtení?

- GDPR
 - ochrana osobních údajů
- NIS2
 - logování přístupů
 - detekce incidentů
 - Zpětná analýza útoků
 - audit
- Audit přístupů, práv
- Proaktivní zabezpečení
 - limit čtení
 - Cut & Lock – odpojení a zamčení

Jak logovat?

- Dokument jako nosič informace
- Logování přístupu – tedy zaznamenání akce uživatele
- Zabezpečení samotného logu
- Doba uchování logu
- Pozor na nadměrné logování
- Uložení logu
 - NSF (Notes DB)
 - TXT soubory (CSV, XML, ...)
 - Externí aplikace (SIEM)

Interní nástroje

- Usage v log.nsf
- User Activity v DB

Usage v log.nsf

- Jen souhrn za časový úsek
- Lze strojově číst, ale ...
- ... tabulka je komplet txt poli
Body
- Limit dle nastavení log.nsf
 - 7 vs. 30 dní ?

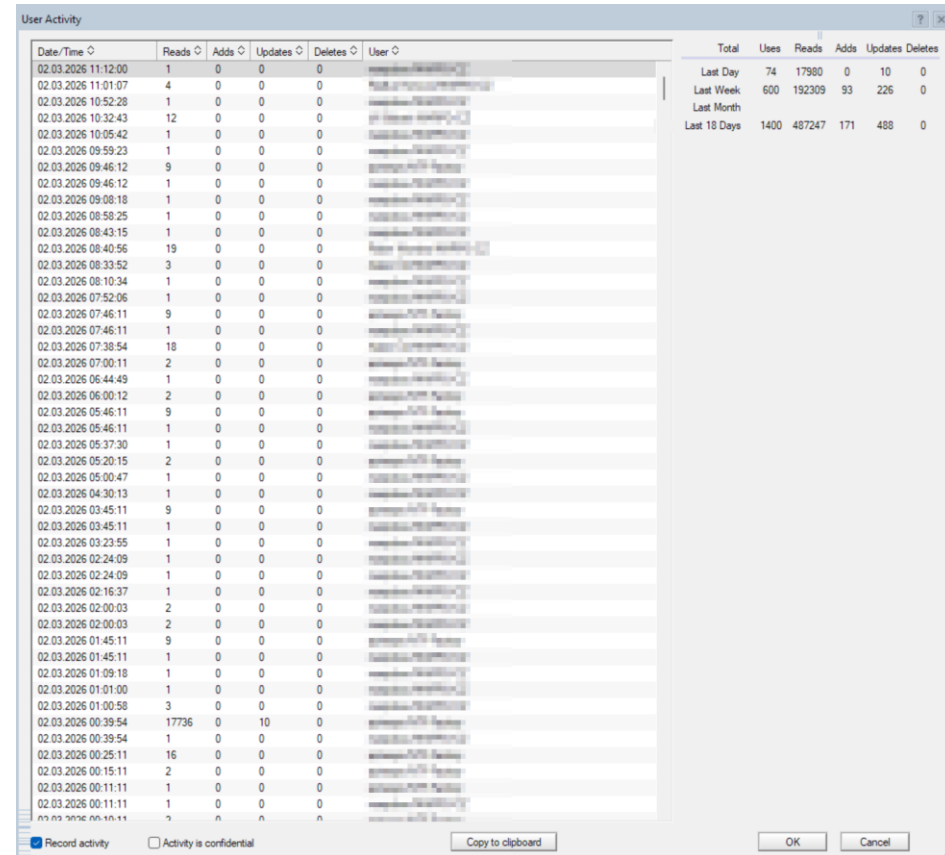
Session Activity

Server: prime/NTF-Factory
Time: 02.02.08:42 - 02.02.13:43
User: Ondřej Kostruh/NTF-Factory
Elapsed Time: 301 minutes
Documents Read: 183
Documents Written: 3306
Network Port: TCP/IP
Network Usage: 3610.4 KBytes transferred
Transactions: 4907

Database(s)	Docs Read	Docs Written	Time Open (sec)	Bytes Read	Byte Written	Transactions
...	12	0	1	32386	0	38
...	1	0	0	2828	0	10
...	2	0	0	9900	0	24
...	0	0	0	2832	0	8
...	2	0	0	12646	0	21
...	1	0	0	9914	0	20
...	26	0	0	24624	0	20
...	23	0	0	55702	0	20
...	32	0	1	21712	0	30
...	4	0	0	11378	0	20
...	1	0	0	11206	0	21
...	0	0	0	2776	0	8
...	5	0	1	15694	0	32
...	0	0	0	2906	0	8
...	0	0	0	482	0	7
...	0	0	0	2710	0	8
...	15	0	38	35162	0	66
...	0	0	0	556	0	6
...	59	3306	89	2856672	0	4123

User Activity

- je třeba zapnout (předem)
- vidíme jen aktuální DB
- nelze strojově číst
- jen export a „ruční“ zpracování
- Limit:
 - ~1000-1400 záznamů, 64KB



Date/Time	Reads	Adds	Updates	Deletes	User
02.03.2026 11:12:00	1	0	0	0	...
02.03.2026 11:01:07	4	0	0	0	...
02.03.2026 10:52:28	1	0	0	0	...
02.03.2026 10:32:43	12	0	0	0	...
02.03.2026 10:05:42	1	0	0	0	...
02.03.2026 09:59:23	1	0	0	0	...
02.03.2026 09:46:12	9	0	0	0	...
02.03.2026 09:46:12	1	0	0	0	...
02.03.2026 09:08:18	1	0	0	0	...
02.03.2026 08:58:25	1	0	0	0	...
02.03.2026 08:43:15	1	0	0	0	...
02.03.2026 08:40:56	19	0	0	0	...
02.03.2026 08:33:52	3	0	0	0	...
02.03.2026 08:10:34	1	0	0	0	...
02.03.2026 07:52:06	1	0	0	0	...
02.03.2026 07:46:11	9	0	0	0	...
02.03.2026 07:46:11	1	0	0	0	...
02.03.2026 07:38:54	18	0	0	0	...
02.03.2026 07:00:11	2	0	0	0	...
02.03.2026 06:44:49	1	0	0	0	...
02.03.2026 06:00:12	2	0	0	0	...
02.03.2026 05:46:11	9	0	0	0	...
02.03.2026 05:46:11	1	0	0	0	...
02.03.2026 05:37:30	1	0	0	0	...
02.03.2026 05:20:15	2	0	0	0	...
02.03.2026 05:00:47	1	0	0	0	...
02.03.2026 04:30:13	1	0	0	0	...
02.03.2026 03:45:11	9	0	0	0	...
02.03.2026 03:45:11	1	0	0	0	...
02.03.2026 03:23:55	1	0	0	0	...
02.03.2026 02:24:09	1	0	0	0	...
02.03.2026 02:24:09	1	0	0	0	...
02.03.2026 02:16:37	1	0	0	0	...
02.03.2026 02:00:03	2	0	0	0	...
02.03.2026 02:00:03	2	0	0	0	...
02.03.2026 01:45:11	9	0	0	0	...
02.03.2026 01:45:11	1	0	0	0	...
02.03.2026 01:09:18	1	0	0	0	...
02.03.2026 01:01:00	1	0	0	0	...
02.03.2026 01:00:58	3	0	0	0	...
02.03.2026 00:39:54	17736	0	10	0	...
02.03.2026 00:39:54	1	0	0	0	...
02.03.2026 00:25:11	16	0	0	0	...
02.03.2026 00:15:11	2	0	0	0	...
02.03.2026 00:11:11	1	0	0	0	...
02.03.2026 00:11:11	1	0	0	0	...
02.03.2026 00:11:11	2	0	0	0	...

	Total	Uses	Reads	Adds	Updates	Deletes
Last Day	74	17980	0	10	0	0
Last Week	600	192309	93	226	0	0
Last Month	1400	487247	171	488	0	0

Interní nástroje - shrnutí

- Jen souhrny počtu dokumentů
 - dle datumů (času), DB a uživatele
- Rozlišení skutečného čtení dokumentů a replikace nebo práce agenta/funkce
- Jak poznat co skutečně uživatel četl?

Výchozí body – bude se programovat ...

- Uložení záznamu na základě akce uživatele
 - údaje, které jsou potřeba – identifikace času, uživatele, DB, dokumentu, ...
 - jak rychle ?
 - kam ? (přístupová práva)
- Zpracování & agregace
- Reakce
- Knihovna LS, JS

SPS - Log				
Lokální		DB Uživatel	Počet čtení	Access Days
▼ 2026				
▼ 2			2	2
▼ 17.02.2026			1	1
▼ Obchod			1	1
▼ Ondřej Kostruh			1	1
▼ 16.02.2026			1	1
▼ Obchod			1	1
▼ Ondřej Kostruh			1	1
▼ 2024			369	2
▼ 1			369	2
▼ 24.01.2024			30	1
▼ SPS - Obchod			30	1
▼ Lukáš Desejve			30	1
▼ 23.01.2024			339	1
▼ SPS - Obchod			339	1
▼ Tomáš Holčák			339	1
▼ 2023				
▼ 11			289	17
▼ 08.11.2023			9	2
▼ SPS - Obchod			5	1
▼ Ondřej Kostruh			5	1
▼ 06.11.2023			5	1
▼ SPS - Obchod			4	1
▼ Ondřej Kostruh			4	1
▼ 10			9	1
▼ 02.10.2023			9	1
▼ SPS - Obchod			9	1
▼ Ondřej Kostruh			9	1
▼ 8			5	1
▼ 31.08.2023			5	1
▼ SPS - Obchod			5	1
▼ Ondřej Kostruh			5	1
▼ 6			92	2
▼ 14.06.2023			62	1
▼ SPS - Obchod			62	1
▼ Ondřej Kostruh			62	1

Schéma – požadavek na uložení

- Notes / Nomad klient
 - Postopen událost na formuláři
 - volá LS funkci v LS knihovně
- xPages
 - postOpenDocument v dominoDocument
 - volá JS funkci v JS knihovně

... nebo agent ...

Schéma – uložení

- Dva způsoby zpracování volání
 1. rychlý - jen uloží
 2. kompletní zpracování
- Je třeba vyřešit kam uložit
 - přístupová práva (k uložení, ke zpracování, k reakci, ...)
 - na serveru, lokálně, replikace, ...

Porovnání způsobů uložení

Rychlé uložení

- jen uloží „někam“ dokument
- řeší jen to kam ho může uložit
 - Přístupová práva

Zpracování a uložení

- informaci uloží na správné místo
- to místo musí najít (ověřit)
- případně zařadit na konec
- připočítat čítače

Porovnání způsobů uložení

Rychlé uložení

test1 Profile

02.03.2026 09:59:14 CET
Elapsed time: 0 msec
Methods profiled: 10
Total measured time: 0 msec

Class	Method	Operation	Calls	Time
Document	[expandedname]	Set	5	0
Database	Title	Get	1	0
Document	ParentDatabase	Get	1	0
Document	Save		1	0
Session	UserName	Get	1	0
Session	CurrentDatabase	Get	1	0
Database	Server	Get	1	0
Database	CurrentAccessLevel	Get	1	0
Database	GetProfileDocument		1	0
Document	[expandedname]	Get	1	0

Zpracování a uložení

test2 Profile

02.03.2026 10:40:40 CET
Elapsed time: 15 msec
Methods profiled: 15
Total measured time: 15 msec

Class	Method	Operation	Calls	Time
View	GetDocumentByKey		1	15
Document	[expandedname]	Get	13	0
Document	[expandedname]	Set	8	0
Database	Title	Get	2	0
Database	FilePath	Get	1	0
Database	Search		1	0
Database	GetView		1	0
Document	HasItem		1	0
Document	Remove		1	0
Document	Save		1	0
Document	CreateRichTextItem		1	0
Session	CurrentDatabase	Get	1	0
DocumentCollection	GetFirstDocument		1	0
RichTextItem	AppendText		1	0
Database	GetProfileDocument		1	0

Porovnání způsobů uložení

Rychlé uložení

- + Rychlé uložení
- Je třeba následné zpracování
- Pomalejší reakce až během zpracování
 - Rozdělení přístupových práv

Zpracování a uložení

- složitější uložení se zpracováním
- + po zpracování je hotovo

Uložení – přístupová práva

- Přímě do aktuální DB
 - Reader
 - \$PublicAccess dokument
- Uložit do jiné DB
 - LOG nebo log
- Lokální replika nebo na serveru (on-line)
 - částečné replikace – na základě vzorce nebo formuláře
- Paradox přístupu
 - (každý) uživatel musí umět uložit záznam, ale jen málokterý se k němu může dostat
 - Depositor ?

Kód - uložení



- live demo

```
accessLog
1 %rem
2   zapiše access log
3
4   nová funkce (2020):
5   - co přístup k dokumentu to jeden záznam
6   - nebudou konflikty, protože se jen zapiše a po zpracování smaže
7   - na lboxu vznikne cca 200 za den
8
9 %end rem
10 Sub accessLog(uidoc As NotesUIDocument, info As String)
11
12   On Error GoTo chybka
13
14   If Not profile.access_log(0) = "" And Not uidoc Is Nothing Then
15
16     Dim xDB As NotesDatabase
17     Set xDB = uidoc.Document.ParentDatabase
18
19     Dim logDoc As NotesDocument
20
21     If xDB.CurrentAccessLevel >= ACLLEVEL_EDITOR Then ' 4 - editor a více může přímo zapisovat
22       Set logDoc = New NotesDocument(xDB)
23
24     ElseIf xDB.IsCurrentAccessPublicWriter Then ' má write public docs
25       Set logDoc = New NotesDocument(xDB) ' vyrobim ho přímo v aktuální db
26       Call logDoc.ReplaceItemValue("PublicAccess", "1")
27
28     Else ' má malé práva - vyrobim ho v LOGu
29       If Not mamLOGdb Then Call initLOG
30       If mamLOGdb Then
31         Set logDoc = New NotesDocument(LOGdb)
32         logDoc.db = xDB.filepath
33         logDoc.dbName = xDB.Title
34       End If
35     End If
36
37     If Not logDoc Is Nothing Then
38       Dim session As New NotesSession
39       With logDoc
40         .form = aLog_Form
41         .username = session.Username
42         .dt = Now
43
44         If xDB.Server = "" Then ' L - local, S - server, W - web
45           .server = "L"
46         Else
47           .server = "S"
48         End If
49
50         If uidoc.IsNewDoc Then .newDoc = "N"
51         If uidoc.Inpreviewpane Then .preview = "P"
52
53         .info = info
54
55         Call .Save(False, False, False)
56       End With
57     End If
58
59     End If ' access_log = ""
60
61   Exit Sub
62
63 chybka:
64   Call ErrorLog("SL: log / accessLog", Err, Err, Error$, 0)
65   Exit Sub
66
67 End Sub
68
```

Zpracování & reakce

- Součty
 - uživatel, DB, den, týden, měsíc, apod.
 - dle typu dokumentů, hodnot (firmy, zakázky, apod.)
- Limity
 - hlídání limitů
 - odeslání upozornění na překročení
 - odebrání přístupu
 - odebrání role v ACL (`notesACLEntry.DisableRole`)
 - zavření otevřené DB (`notesUIDatabase.Close`)
 - příkaz do konzole (`drop`)

Kód - zpracování



- live demo

```
aclog_zpracujDoc
10
11 Dim key As String, key1 As String, Ldoc As NotesDocument, dbFilePath As String, dbTitle As String
12
13 If doc.db(0) = "" Then
14     dbFilePath = xdb.filepath
15     dbTitle = xdb.Title
16 Else
17     dbFilePath = doc.db(0)
18     dbTitle = doc.dbName(0)
19 End If
20
21 key1 = doc.username(0) & "," & dbFilePath ' první část klíče
22
23 Dim rtitem As NotesRichTextItem
24
25 If doc.HasItem("dt") Then ' nový access log - pro každý přístup samostatný dokument
26     key = key1 & "," & Format$(doc.dt(0), "yyyymmdd")
27
28     Set Ldoc = najdiAclog(key) ' hledám kam bych to zapsal
29     If Ldoc Is Nothing Then ' ještě neexistuje - založím ho
30         Set Ldoc = New NotesDocument(thisdb)
31         With Ldoc
32             .form = "ac-log"
33             .username = doc.username
34             .db = dbFilePath
35             .dbName = dbTitle
36             .datum = CDate(Format(doc.dt(0), "General Date"))
37             .mykey = key
38             .cteni = 0
39
40             Set rtitem = .CreateRichTextItem("historie_RTF")
41         End With
42     Else
43         Set rtitem = Ldoc.GetFirstItem("historie_RTF")
44         If rtitem Is Nothing Then
45             Set rtitem = Ldoc.CreateRichTextItem("historie_RTF")
46             If Not Ldoc.historie(0) = "" Then
47                 Call rtitem.AppendText(Ldoc.historie(0))
48                 Call Ldoc.RemoveItem("historie")
49             End If
50         End If
51     End If
52
53 If Not Ldoc Is Nothing Then ' konečně zapíšu samotný záznam
54     Dim zapis As String
55     zapis = Format$(doc.dt(0), "dd.mm.yyyy hh:mm:ss") & aLog_Sep
56
57     If doc.newDoc(0) = "" Then
58         zapis = zapis & "0" & aLog_Sep
59     Else
60         zapis = zapis & doc.newDoc(0) & aLog_Sep
61     End If
62     If doc.preview(0) = "" Then
63         zapis = zapis & "-" & aLog_Sep
64     Else
65         zapis = zapis & doc.preview(0) & aLog_Sep
66     End If
67     zapis = zapis & doc.server(0) & aLog_Sep
68     Call rtitem.AppendText(zapis & doc.info(0) & Chr$(10))
69     'Ldoc.historie = Ldoc.historie(0) & zapis & doc.info(0) & Chr$(10)
70
71     Ldoc.cteni = CLng(Ldoc.cteni(0)) + 1
72     If Not cstr(profile.aclog_warning(0)) = "" Then ' má se hledat překročení
73         If CLng(Ldoc.cteni(0)) > CLng(profile.aclog_warning(0)) And Ldoc.warning(0) = "" Then ' je jich moc
74             Ldoc.warning = "1"
75             Call aclog_pridejkuPO(Ldoc) ' přidá k upo ...
76         End If
77     End If
78     Call Ldoc.Save(False, False, False)
79 End If
80
81 Call doc.Remove(True) ' záznam smažu
82 aclog_zpracujDoc = True
83
84
```

Závěrem

- HCL Notes/Domino je (a vždy byla) bezpečná platforma
 - Domino 14.5 prošlo certifikací BSI (v DE, ISO 27001)
 - má potenciál být zabezpečená
 - ALE - nabízené prostředky a nastavení je třeba využít

Zdroje

- NIS2
<https://portal.nukib.gov.cz/pruvodce-smernici-nis2>
- HCL Product Documentation – Domino Designer
https://help.hcltechsw.com/dom_designer/14.0.0/basic/wpd_whatsnew.html
- OpenLog
<https://www.openntf.org/main.nsf/project.xsp?r=project/OpenLog>
- Aplikace Log od NTF Factory
<https://ntf-factory.com/apps/log/>