Journaux et traces

L'Université de Nantes comme toute entreprise a une obligation légale de conserver les traces de tous les accès à ses services informatiques dans ses journaux d'évenements. Sa politique de gestion de journaux informatiques est basée sur le document officiel suivant. Ce document a été visé et validé par la CNIL.

Les journaux informatiques constitués par l'université sont conforme à la loi du 6 janvier 1978 modifiée par la loi du 6 août 2006 dite loi “Informatique et Liberté” et ont fait l'objet d'une déclaration auprès de la CNIL. Pour toute information sur ce point, les correspondants informatique et liberté de l'université sont M. Michel Allemand et Mme Christelle Durand.

Durée de conservation

L'université conserve les journaux pendant un an maximum.

Utilisation

Les journaux informatiques sont indispensables pour la sécurité et la supervision du système d'information de l'université. La DSI peut les utiliser pour les raisons suivantes:

- contrôler les volumes d'utilisation et pouvoir ainsi détecter les anomalies
- contrôler la sécurité des systèmes, détecter les intrusions, les failles, les pannes
- confirmer le bon fonctionnement du système et répondre aux demandes d'information des utilisateurs (mon mail a-t-il bien été envoyé?)
- fournir des élements de preuve en cas d'enquête interne ou policière.

Informations conservées

Ainsi par soucis de transparence nous allons lister ici les informations que nous concervons:

Messagerie électronique

Envoi:

- Date de réception
- expéditeur
- destinataires
- adresse du PC d'envoi
- date de transfert au serveur suivant
- status de l'opération (echec/succès)
- réponse du serveur suivant

exemple (les xxxx sont rajouté ici pour cacher les identifiants des message, des utilisateurs, etc):

```
May 22 23:37:29 smtp1.univ-nantes.prive postfix/smtpd[19100]: connect from
webmail-1.U10.univ-nantes.prive[172.20.10.107]
May 22 23:37:29 smtp1.univ-nantes.prive postfix/smtpd[19100]: xxxxxxxxxx:
client=webmail-1.U10.univ-nantes.prive[172.20.10.107]
May 22 23:37:29 smtp1.univ-nantes.prive postfix/cleanup[16848]: xxxxxxxxxx:
message-id=<xxxxxxxxxxxxx.squirrel@webmail.univ-nantes.fr>
May 22 23:37:30 smtp1.univ-nantes.prive postfix/qmgr[24377]: xxxxxxxxxx:
from=<xxx.xxx@univ-nantes.fr>, size=17171265, nrcpt=1 (queue active)
May 22 23:37:30 smtp1.univ-nantes.prive postfix/smtpd[19100]: disconnect
from webmail-1.U10.univ-nantes.prive[172.20.10.107]
May 22 23:37:32 smtp1.univ-nantes.prive postfix/smtpd[12395]: connect from
localhost[127.0.0.1]
May 22 23:37:32 smtp1.univ-nantes.prive postfix/smtpd[12395]: xxxxxxxxxx:
client=localhost[127.0.0.1]
May 22 23:37:32 smtp1.univ-nantes.prive postfix/cleanup[16848]: xxxxxxxxxx:
message-id=<xxxxxxxxxxxxx.squirrel@webmail.univ-nantes.fr>
May 22 23:37:33 smtp1.univ-nantes.prive postfix/smtpd[12395]: disconnect
from localhost[127.0.0.1]
May 22 23:37:33 smtp1.univ-nantes.prive postfix/qmgr[24377]: xxxxxxxxxx:
from=<xxx.xxx@univ-nantes.fr>, size=17171729, nrcpt=1 (queue active)
May 22 23:37:33 smtp1.univ-nantes.prive postfix/lmtp[16803]: xxxxxxxxxx:
to=<xxxx@hotmail.com>, relay=127.0.0.1[127.0.0.1]:10024, delay=4.1,
delays=1.2/0/0/2.9, dsn=2.0.0, status=sent (250 2.0.0 Ok, id=18110-06, from
MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as xxxxxxxxxx)
May 22 23:37:33 smtp1.univ-nantes.prive postfix/qmgr[24377]: xxxxxxxxx:
removed
```

Réception:

- Date de réception
- expéditeur
- destinataires
- adresse du serveur d'envoi
- date de transfert au serveur suivant
- status de l'opération (echec/succès)
- réponse du serveur suivant

```
May 23 17:08:44 mx1.univ-nantes.fr postfix-out/smtpd[15921]: connect from
localhost[127.0.0.1]
May 23 17:08:44 mx1.univ-nantes.fr postfix-out/smtpd[15921]: xxxxxxxxxx:
client=Smtp1.univ-nantes.prive[172.20.12.55]
May 23 17:08:44 mx1.univ-nantes.fr postfix-out/cleanup[16092]: xxxxxxxxxx:
message-id=<xxxxx.xxxxxx@smtp.univ-nantes.prive>
May 23 17:08:44 mx1.univ-nantes.fr postfix-out/qmgr[864]: xxxxxxxxxx:
from=<xxxxxxxxxx@univ-nantes.fr>, size=2227, nrcpt=1 (queue active)
May 23 17:08:44 mx1.univ-nantes.fr postfix-in/smtp[12745]: 4F01C29463:
to=<xxxxxxxxxx@univ-nantes.fr>, relay=127.0.0.1[127.0.0.1]:10024,
conn_use=2, delay=0.12, delays=0.03/0/0/0.09, dsn=2.0.0, sta
```

```
May 23 17:08:44 mx1.univ-nantes.fr postfix-in/qmgr[876]: 4F01C29463: removed
```

Antispam:

- Date de réception par l'antispam
- expéditeur, destinataire
- détail du temps passé dans chaque brique de l'antispam
- score et détail du score
- date de transmission du message au serveur suivant
- status de l'opération (echec/succès)
- réponse du serveur suivant

```
May 23 06:49:42 mx1.univ-nantes.fr amavis[15437]: (15437-20) ESMTP::10024
/var/lib/amavis/tmp/amavis-20110523T063318-15437: <xxxxxxx@sfr.fr> ->
<xxxxxx@univ-nantes.fr> SIZE=21869 Received: from mx1.d101.univ-nantes.fr
([127.0.0.1]) by localhost (univ-nantes.fr [127.0.0.1]) (amavisd-new, port
10024) with ESMTP for <xxxxxxx@univ-nantes.fr>; Mon, 23 May 2011 06:49:42
+0200 (CEST)
May 23 06:49:42 mx1.univ-nantes.fr amavis[15437]: (15437-20) Checking:
XWSo2Wxx90Kl [93.17.128.13] <xxxxxx@sfr.fr> -> <xxxxxx@univ-nantes.fr>
May 23 06:49:42 mx1.univ-nantes.fr amavis[15437]: (15437-20) p003 1 Content-
Type: multipart/alternative
May 23 06:49:42 mx1.univ-nantes.fr amavis[15437]: (15437-20) p001 1/1
Content-Type: text/plain, size: 2240 B, name:
May 23 06:49:42 mx1.univ-nantes.fr amavis[15437]: (15437-20) p002 1/2
Content-Type: text/html, size: 16126 B, name:
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) SA info:
FuzzyOcr: Processing Message with ID "<xxxxxx@sfr.fr>" (<xxxxxx@sfr.fr> ->
<xxxxxx@univ-nantes.fr>)
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) SPAM-TAG,
<xxxxxx@sfr.fr> -> <xxxxxx@univ-nantes.fr>, Yes, score=14.615
tagged_above=-1000 required=5 tests [CRM114_UNSURE=0.1, HTML_MESSAGE=0.001,
J_BACKHAIR_22=1, J_CHICKENPOX_73=0.6, MIME_QP_LONG_LINE=0.001,
MR_NOT_ATTRIBUTED_IP=0.2, NO_REAL_NAME=1, RCVD_IN_DNSWL_NONE=-0.0001,
RCVD_IN_SORBS=1, RCVD_IN_SORBS_WEB=0.614, SPF_PASS=-0.001, UN_CADOVIS=10,
UN_PHISHING_PW=0.1] autolearn=disabled
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) FWD via SMTP:
<xxxxxx@sfr.fr> -> <xxxxxx@univ-nantes.fr>,BODY=7BIT 250 2.0.0 Ok,
id=15437-20, from MTA([127.0.0.1]:10025): 250 2.0.0 Ok: queued as
58621201DD74
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) Passed SPAMMY,
[xx.xx.xx.xx] [xx.xx.xx.xx] <xxxxxx@sfr.fr> -> xxxxxx@univ-nantes.fr>,
Message-ID: <xxxxxx@sfr.fr>, mail_id: XWSo2Wxx90Kl, Hits: 14.615, size:
21869, queued_as: xxxxxx, 858 ms
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) TIMING-SA total
760 ms - parse: 3 (0.4%), extract_message_metadata: 26 (3.4%),
get_uri_detail_list: 4 (0.5%), tests_pri_-1000: 13 (1.6%), tests_pri_-950:
1.10 (0.1%), tests_pri_-900: 1.16 (0.2%), tests_pri_-400: 0.97 (0.1%),
tests_pri_0: 615 (81.0%), check_dkim_adsp: 4 (0.5%), check_spf: 8 (1.0%),
poll_dns_idle: 3 (0.3%), check_pyzor: 0.03 (0.0%), tests_pri_500: 18 (2.4%),
tests_pri_899: 60 (7.9%), check_crm114: 58 (7.7%), tests_pri_900: 1.68
```

```
(0.2%), get_report: 4 (0.5%)
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) TIMING [total
861 ms] - SMTP greeting: 1 (0%)0, SMTP EHLO: 0 (0%)0, SMTP pre-MAIL: 0
(0%)0, SMTP pre-DATA-flush: 1 (0%)0, SMTP DATA: 36 (4%)5, check_init: 0
(0%)5, digest_hdr: 1 (0%)5, digest_body_dkim: 0 (0%)5, gen_mail_id: 0 (0%)5,
mime_decode: 9 (1%)6, get-file-type2: 15 (2%)8, parts_decode: 0 (0%)8,
check_header: 1 (0%)8, AV-scan-1: 2 (0%)8, spam-wb-list: 1 (0%)8, SA parse:
3 (0%)8, SA check: 751 (87%)96, update_cache: 8 (1%)96, decide_mail_destiny:
0 (0%)97, fwd-connect: 4 (0%)97, fwd-xforward: 0 (0%)97, fwd-mail-pip: 1
(0%)97, fwd-rcpt-pip: 0 (0%)97, fwd-data-chkpnt: 0 (0%)97, write-header: 1
(0%)97, fwd-data-contents: 0 (0%)97, fwd-end-chkpnt: 14 (2%)99, prepare-dsn:
1 (0%)99, main_log_entry: 6 (1%)100, update_snmp: 2 (0%)100, SMTP pre-
response: 0 (0%)100, SMTP response: 0 (0%)100, unlink 2-files: 0 (0%)100,
rundown: 0 (0%)100
May 23 06:49:43 mx1.univ-nantes.fr amavis[15437]: (15437-20) Requesting
process rundown after 20 tasks (and 20 sessions)
May 23 06:49:43 mx1.univ-nantes.fr amavis[16841]: TIMING [total 4 ms] - bdb-
open: 4 (100%)100, rundown: 0 (0%)100
```

Relève de son courrier universitaire:

- Date de l'opération
- opération: connexion ou déconnexion
- status de l'opération
- identifiant de l'utilisateur
- adresse IP du PC
- protocole utilisé,

```
May 22 23:38:01 perdition1.univ-nantes.prive perdition[1683]: Connect:
xxx.xxx.xxx.xxx->172.20.12.60
May 22 23:38:01 perdition1.univ-nantes.prive perdition[1683]: Auth:
xxx.xxx.xxx.xxx->172.20.12.60 user="xxxxxx" server="xxxxxx.univ-
nantes.prive" port="143" status="ok"
May 22 23:38:06 perdition1.univ-nantes.prive perdition[30141]: Close:
xxx.xxx.xxx.xxx->172.20.12.60 user="xxxxxx" received=47982 sent=108630
```

proxy pop/imap sortant:

- Date de l'opération
- opération: connexion, déconnexion, suppression, etc.
- protocole utilisé: pop, pops, imap, imaps
- serveur distant interrogé
- nom d'utilisateur distant utilisé
- status de l'opération (echec/succès)
- réponse du serveur distant

```
May  9 16:00:53 proxyimap.univ-nantes.fr DeleGate[31196]: 113127+0: (2)
accepted [37] -@[xxx.xxx.xxx.xxx]xxx.xxx.xxx.xxx:49727 (0.001s)(9)
May  9 16:00:53 proxyimap.univ-nantes.fr DeleGate[31196]: 113127+0: PATH:
pop://-:110!proxyimap.d108.univ-
nantes.fr:110!xxx.xxx.xxx.xxx:49727!anonymous@xxx.xxx.xxx.xxx;1336572053
```

```
May  9 16:00:53 proxyimap.univ-nantes.fr DeleGate[31196]: 113127+0: POP C-S:
USER prenon.nom@sereurdistant.fr@pop3.serveurdistant.fr^M
```

Site web de l'université (webmail, site de l'université, forum, intranet, site de composante, etc)

- Date de l'opération
- site consulté
- adresse IP du client
- page consultée
- status de l'opération
- taille de l'élement consulté
- page de provenance s'il s'agit d'un lien cliqué
- user-agent du navigateur

```
May 22 23:37:22 revaccess1.u10.univ-nantes.prive apache2-access-
www.math.sciences: xxx.xxx.xxx.xxx - - [22/May/2011:23:37:21 +0200] "GET
/jeanleray/exposes/emmanuel-schenck-cea-decroissance-de-lenergie-pour-
lequation-des-ondes-amorties HTTP/1.1" 200 4194 "-" "Mozilla/5.0 (Windows;
U; Windows NT 5.1; fr; rv:1.8.1) VoilaBot BETA 1.2"
```

Navigation internet

- Date de l'opération
- site consulté
- adresse IP du client
- page consultée
- status de l'opération
- taille de l'élement consulté

```
May 22 23:37:27 proxy1.univ-nantes.fr squid[13693]: 1306100247.451   3415
172.20.10.62 TCP_MISS/200 51764 GET http://xxxxxxxxxxxx/page/truc.html -
DIRECT/xxx.xxx.xxx.xxx text/html
```

Messagerie Instantanée

- Date de l'opération
- opération (connexion ou déconnexion)
- status de l'opération
- nom d'utilisateur
- adresse IP du client

```
Sep  4 23:38:44 jabber.d101.univ-nantes.fr ejabberd:
I(<0.454.0>:ejabberd_listener:232) : (#Port<0.951423>) Accepted connection
{{xxx,xxx,xxx,xxx},45823} -> {{193,52,101,32},5222}
Sep  5 09:44:48 jabber.d101.univ-nantes.fr ejabberd:
I(<0.22712.21>:ejabberd_c2s:580) :
({socket_state,tls,{tlssock,#Port<0.975165>,#Port<0.975167>},<0.22711.21>})
```

```
Accepted authentication for prenom.nom by ejabberd_auth_ldap
Sep  5 09:44:48 jabber.d101.univ-nantes.fr ejabberd:
I(<0.22712.21>:ejabberd_c2s:839) :
({socket_state,tls,{tlssock,#Port<0.975165>,#Port<0.975167>},<0.22711.21>})
Opened session for prenom.nom@univ-nantes.fr/Univ'Tchat
Sep  5 09:44:48 jabber.d101.univ-nantes.fr ejabberd:
I(<0.22712.21>:mod_shared_roster:807) : unset_presence for "prenon.nom" @
"univ-nantes.fr" / "Univ'Tchat" -> [] (1 resources)
```

Wifi

univ-nantes

- Date de l'opération
- opération (connexion, renouvellement, déconnexion, expiration)
- identifiant de l'utilisateur
- l'adresse IP
- adresse materielle

```
Jun  7 16:40:26 portail1.wifi.univ-nantes.fr wifidog: xxx.xxx.xxx.xxx
yy:yy:yy:yy:yy:y xxxxxxxxxxxxxxxxxxx_identifiant-p - Inactive for more than
300 seconds, removing client and denying in firewall
Jun  7 16:40:26 portail1.wifi.univ-nantes.fr wifidog: Got manual logout from
client ip xxx.xxx.xxx.xxx, mac yy:yy:yy:yy:yy:yy, token
xxxxxxxxxxxxxxxxxxxxxx_identifiant-p - redirecting them to logout message
Jun  7 16:40:35 portail1.wifi.univ-nantes.fr wifidog: Got ALLOWED from
central server authenticating token xxxxxxxxxxxxxxxxxxxxx_identifiant-p
from xxx.xxx.xxx.xxx at yy:yy:yy:yy:yy:yy - adding to firewall and
redirecting them to portal
```

eduroam

- borne wifi utilisée

Proxy FTP

- Date de l'opération
- opération (connexion, commande ftp, déconnexion)
- adresse IP du client
- adresse IP du serveur distant
- nom d'utilisateur sur le serveur distant
- résultat de l'opération

```
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF connect
from xxx.xxx.xxx.xxx
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF 'USER
univ-nantes' dest yyy.yyy.yyy.yyy:21 from xxx.xxx.xxx.xxx
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF reading
data for 'identifiant' from cfg-file
```

```
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF 'PASS
****' from 172.20.12.79
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF 'PORT
yyy.yyy.yyy.yyy:54228' from xxx.xxx.xxx.xxx
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: USER-INF 'NLST .'
from xxx.xxx.xxx
May  9 01:49:01 ftproxy.univ-nantes.fr ftp-child[29958]: TECH-INF 'PORT
193.52.108.56:46542' for xxx.xxx.xxx.xxx
```

Accès nomade (VPN)

- Date de l'opération
- opération (connexion, opération du client VPN, etc.)
- nom d'utilisateur
- composante de l'utilisateur
- adresse ip du client

```
00.univ-nantes.prive Juniper: 2012-05-09 06:09:40 - ive - [xxx.xxx.xxx.xxx]
Root::nom-p(Default)[] - Primary authentication successful for nom-
p/ldapauth.ha.univ-nantes.prive from 90.59.64.40
00.univ-nantes.prive Juniper: 2012-05-09 06:09:50 - ive - [xxx.xxx.xxx.xxx]
Root::nom-p(Default)[] - Host Checker policy 'Antivirus Process' passed on
host xxx.xxx.xxx.xxx  for user 'nom-p'.
00.univ-nantes.prive Juniper: 2012-05-09 06:09:50 - ive - [xxx.xxx.xxx.xxx]
Root::nom-p(Default)[] - Host Checker policy 'Antivirus MAJ' passed on host
xxx.xxx.xxx.xxx for user 'nom-p'.
00.univ-nantes.prive Juniper: 2012-05-09 06:09:50 - ive - [xxx.xxx.xxx.xxx]
Root::nom-p(Default)[] - Host Checker policy 'Anti-virus' passed on host
xxx.xxx.xxx.xxx  for user 'nom-p'.
00.univ-nantes.prive Juniper: 2012-05-09 06:09:50 - ive - [xxx.xxx.xxx.xxx]
Root::nom-p(Default)[MSH] - nom-p/Default logged out from IP
(xxx.xxx.xxx.xxx) because user started new session from IP (xxx.xxx.xxx.xxx)
```