

# 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'événements. 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, contactez [le délégué à la protection des données](#).

## 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 éléments de preuve en cas d'enquête interne ou policière.

## Informations conservées

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

### 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

## 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

## 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

## 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,

## 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

## 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'élément consulté
- page de provenance s'il s'agit d'un lien cliqué
- [user-agent](#) du navigateur

## Navigation internet

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

## Messagerie Instantanée

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

## Wifi 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

## Consulter l'historique de ses connexions

L'Université de Nantes met à disposition de ses utilisateur l'[historique des ses connexions](#) aux services web. L'utilisateur peut ainsi s'assurer que son compte n'est pas utilisé anormalement:

From:  
<https://wiki.univ-nantes.fr/> - Wiki

Permanent link:  
<https://wiki.univ-nantes.fr/doku.php?id=personnels:securite:journaux>

Last update: 2026/02/13 14:07



