Mode Opératoire

Restauration de la zone DNS publique lurcat.fr EuroDNS : messagerie M365 et anti-usurpation

Code :	MO-NET-010
Version :	1.1
Date :	2 novembre 2026
Auteur :	Cédric LEGRAND
Classification :	USAGE INTERNE — Équipe BTS SIO

Historique des révisions

Version	Date	Modifications
1.0	06/10/2026	Création initiale, à partir des constats du jour (zone EuroDNS réinitialisée vers le 20/07/2026 : MX, SPF et tokens de vérification Microsoft disparus) comparés à l'état sain de l'audit DNS du 12/03/2026.
1.1	02/11/2026	Dénouement : zone restaurée après re-validation du contact ICANN (restauration automatique), wildcard et A de parking supprimés, mail externe validé. P2 (DKIM/DMARC) bloqué sur l'attribution d'un rôle administrateur M365.

1 Objet

Ce mode opératoire décrit, étape par étape, la **remise en état de la zone DNS publique `lurcat.fr`** hébergée chez EuroDNS. La zone a perdu ses enregistrements de messagerie Microsoft 365 au cours de l'été 2026, ce qui coupe la réception des mails externes vers les adresses `@lurcat.fr` des étudiants et des personnels.

La procédure couvre quatre objectifs, dans l'ordre :

1. **rétablir le mail externe** (MX, SPF, autodiscover) ;
2. **supprimer le wildcard** de parking qui capte tous les sous-domaines (remédiation R-034 de l'audit) ;
3. **poser l'anti-usurpation** (DKIM puis DMARC, en progression prudente) ;
4. **préparer l'émission d'un certificat public** Let's Encrypt pour le Wi-Fi (chantier `radius.lurcat.fr`, sans aucun enregistrement à créer manuellement).

2 Contexte et constats

2.1 À qui appartient lurcat.fr

Le domaine `lurcat.fr` **appartient au lycée** : le whois AFNIC [1] indique le titulaire « Lycée Jean Lurçat » (contact Emmanuel Coupet, adresse académique `ce.0660011d@ac-montpellier.fr`), le registrar **EURODNS S.A.**, une création le 18/05/2021 et une échéance au **18/05/2027**. Il n'est **pas** fourni par l'abonnement Microsoft : le tenant Microsoft 365 l'utilise comme domaine personnalisé, mais l'enregistrement, l'hébergement DNS et le renouvellement relèvent du compte EuroDNS de l'établissement.

2.2 État constaté au 06/10/2026

Comparaison entre l'audit DNS du 12/03/2026 (état sain) et les mesures du jour (requêtes `dig` publiques) :

Enregistrement	12/03/2026 (audit)	06/10/2026 (mesuré)
MX	`lurcat-fr.mail.protection.outlook.com`	**absent**
TXT (SPF)	`v=spf1 include:spf.protection.outlook.com -all`	**absent**
TXT (vérif. MS)	`MS=ms37403205`, `MS=ms30706699`	**absents**
Wildcard `*`	CNAME vers parkingcrew.net	CNAME vers parking EuroDNS (`80.92.65.214`)

Le serial SOA de la zone (`2026072001`) et la date de modification de la fiche contact whois situent le changement autour du **20/07/2026** : la zone a vraisemblablement été réinitialisée à un gabarit de parking EuroDNS.

Impact en production

Sans enregistrement MX, les serveurs de messagerie extérieurs retombent sur l'enregistrement A du domaine — une adresse de parking — et les mails vers `@lurcat.fr` aboutissent en erreur. Teams et la messagerie interne au tenant continuent de fonctionner, ce qui explique que la panne soit passée inaperçue depuis juillet.

2.3 Qu'est-ce qu'un wildcard « de parking » ?

Le terme *parking* ne désigne pas une propriété du joker lui-même, mais sa **destination**. Un *parking de domaine* est le gabarit par défaut qu'un bureau d'enregistrement applique à un domaine sans site : une page d'attente générique, parfois publicitaire. La cible constatée en mars (`parkingcrew.net`) est une société dont c'est le cœur de métier ; celle mesurée en octobre (`80.92.65.214`) est le serveur de parking d'EuroDNS.

Or le wildcard `*.lurcat.fr` est un enregistrement **attrape-tout** : tout sous-domaine non défini explicitement (`autodiscover`, `_dmarc`, n'importe quel nom inventé) est résolu par ce joker, et aboutit donc sur la page de parking. Vérifié le 06/10/2026 : une requête HTTP sur un sous-domaine aléatoire reçoit une réponse `200` du serveur de parking, avec une page intitulée du nom demandé. Le joker a vraisemblablement été réintroduit avec le gabarit par défaut lors de la réinitialisation de la zone, autour du 20/07/2026.

Trois problèmes concrets :

— **anti-usurpation neutralisée** : les requêtes `_dmarc.lurcat.fr` et `*._domainkey.lurcat.fr`, qui devraient répondre NXDOMAIN, retournent le parking — DKIM et DMARC sont inévaluables par les destinataires, usurper `@lurcat.fr` reste facile ;

— **nom de l'établissement prêté à du contenu tiers** : une page servie sur `intranet.lurcat.fr` paraîtrait officielle (surface de phishing et risque de reprise de sous-domaine — finding R-034 de l'audit) ;

— **erreurs masquées** : une faute de frappe dans un sous-domaine ne produit plus d'erreur visible, juste la page parking.

La suppression du joker (étape 2 de la procédure) rétablit le comportement sain : les noms inexistants répondent NXDOMAIN, et DKIM comme DMARC redeviennent évaluables.

2.4 Dénouement réel au 02/11/2026



Ce qui s'est réellement passé

La zone n'avait pas été simplement modifiée : elle était suspendue pour contact ICANN expiré (statut `CONTACT_VALIDATION_EXPIRED` dans l'API EuroDNS, erreur « Cette zone ne peut pas être gérée » dans la console). La reconstruction manuelle des enregistrements (sections suivantes) n'a donc PAS été nécessaire : la re-validation du contact (lien envoyé par email au

titulaire, puis code SMS) a déclenché la restauration automatique de la zone en une dizaine de minutes, avec tous ses anciens enregistrements — MX, SPF, autodiscover, tokens Microsoft, mais aussi Lync (`sip`, `lyncdiscover`, SRV) et Intune (`enterpriseregistration`, `enterpriseenrollment`), absents de l'audit de mars.

Actions effectivement réalisées le 02/11/2026 :

— re-validation du contact ICANN (email `ce.0660011d@ac-montpellier.fr` + code SMS) ;

— suppression du wildcard `*` et de l'enregistrement A de l'apex (`185.53.179.145`, parking) via l'API de la console EuroDNS (PUT de la zone filtrée, validé au préalable par l'endpoint `/check`) ;

— vérifications `dig` conformes sur les autoritaires `ns1/ns2.eurodns.com` et les résolveurs `1.1.1.1` et `8.8.8.8` ;

— **test de mail externe bidirectionnel validé** (réception et émission `@lurcat.fr`) ;

— activation du **renouvellement automatique** du domaine (était `AUTOEXPIRE` ; 20 euros/an, avant le 16/05/2027) ; la 2FA email était déjà active sur le compte ;

— transfer lock toujours déverrouillé : **non activable dans la nouvelle console**, à demander au support EuroDNS ;

— accès consigné dans le coffre Vaultwarden de l'équipe (élément « EuroDNS — lurcat.fr », dossier Réseau).

Reste à faire : P2 bloqué sur les droits M365

Le compte `c.legrand@lurcat.fr` n'a aucun rôle d'administration dans le tenant (vérifié le 02/11/2026 : `Get-DkimSigningConfig` et `Get-ManagementRoleAssignment` filtrés par le RBAC Exchange, `Set-Mailbox -EmailAddresses` refusé). DKIM (section 4) et DMARC (section 4) sont donc bloqués en attendant l'attribution d'un rôle *Exchange Administrator* ou *Security Administrator* par le chef d'établissement ou la DSI académique. Le tenant initial est identifié : `ljl66.onmicrosoft.com`. Reprise possible par PowerShell Exchange Online (`Get-DkimSigningConfig -Identity lurcat.fr`) ou par le portail Defender (`https://security.microsoft.com/dkimv2`).

La procédure détaillée ci-dessous reste la référence pour reconstruire les enregistrements si la zone devait être recréée manuellement, et pour le P2 une fois le rôle attribué.

3 Prérequis

Prérequis

— **Accès au compte EuroDNS détenteur de la zone `lurcat.fr`. S'il est introuvable, engager la récupération via le contact titulaire enregistré à l'AFNIC (Emmanuel Coupet, `ce.0660011d@ac-montpellier.fr`) auprès du chef d'établissement.**

— **Accès administrateur au tenant Microsoft 365 (pour DKIM, section 4) — à demander au chef d'établissement ou à la DSI académique si besoin.**

— **Un poste avec `dig` pour les vérifications (les résultats attendus figurent en section 5).**

Toutes les modifications se font dans la console EuroDNS : **Mes domaines** → `lurcat.fr` → **Gérer les DNS** (*Manage DNS*). TTL conseillé : 3600 pour tous les enregistrements.

4 Procédure

1 Sécuriser le compte EuroDNS

Avant toute modification de la zone :

1. **vérifier que le domaine `lurcat.fr` figure bien dans le compte ;**
2. **activer la double authentification sur le compte ;**
3. **activer le renouvellement automatique du domaine (échéance 18/05/2027) et vérifier le moyen de paiement — si le domaine expire, il retombe dans le domaine public ;**
4. **activer le verrou registre (*transfer lock*) ;**
5. **consigner l'accès dans le coffre Vaultwarden de l'équipe (`https://10.0.112.10`).**

2 Supprimer le wildcard de parking

1. **Supprimer l'enregistrement `*` (CNAME vers le parking). C'est lui qui capte `_dmarc`, `_domainkey` et tout sous-domaine inexistant vers un service tiers non maîtrisé — remédiation R-034 de l'audit.**
2. **Supprimer l'enregistrement A de l'apex (`@` → `80.92.65.214`, parking EuroDNS), sauf si une redirection web est prévue : il n'existe aucun site sur `lurcat.fr`.**

> **Note**
>
> **Sans wildcard, les requêtes vers des sous-domaines inexistants répondront NXDOMAIN — c'est le comportement souhaité, et il est indispensable pour que DKIM et DMARC (étapes 4 et 4) soient évalués correctement par les destinataires.**

3 Restaurer l'enregistrement MX

Créer :

Nom	Type	Valeur
`@`	**MX**	`0 lurcat-fr.mail.protection.outlook.com`

C'est la valeur constatée lors de l'audit du 12/03/2026. Si le tenant a changé entre-temps, la valeur à jour figure dans le centre d'administration Microsoft 365 (Paramètres → Domaines → `lurcat.fr`) [3].

4 Restaurer le SPF

Créer :

Nom	Type	Valeur
@	TXT	v=spf1 include:spf.protection.outlook.com -all

Le qualificateur `-all` (échec strict) limite l'émission aux serveurs Microsoft 365, conformément au guide de sécurisation de la messagerie de l'ANSSI.

5 Créer l'enregistrement autodiscover

Créer :

Nom	Type	Valeur
autodiscover	CNAME	autodiscover.outlook.com

Cet enregistrement n'existait pas en mars (il était masqué par le wildcard) : il permet la configuration automatique des profils Outlook.

6 Vérification intermédiaire

Attendre la propagation (quelques minutes à une heure), puis contrôler :

```
dig lurcat.fr MX +short           # 0
   lurcat-fr.mail.protection.outlook.com
dig lurcat.fr TXT +short          # v=spf1
   include:spf.protection.outlook.com -all
dig autodiscover.lurcat.fr +short # autodiscover.outlook.com
dig inexistant.lurcat.fr +short   # (vide : wildcard supprime)
```

Vérification

Envoyer un mail depuis une adresse personnelle externe vers un compte `@lurcat.fr`. Avant restauration, il revient en erreur ; après, il doit être distribué. Vérifier également que le domaine reste au statut « Healthy » dans le centre d'administration M365.

7 Poser DMARC en mode observation

Créer la boîte ou l'alias `dmarc-reports@lurcat.fr` dans le tenant, puis :

Nom	Type	Valeur
`_dmarc`	TXT	`v=DMARC1; p=none; rua=mailto:dmarc-reports@lurcat.fr; ruf=mailto:dmarc-forensic@lurcat.fr; adkim=r; aspf=r`

La politique `p=none` observe sans bloquer. Exploitation des rapports pendant 4 à 6 semaines, puis passage à `p=quarantine`, puis `p=reject` une fois tous les flux alignés (plan de progression de l'audit de mars).

8 Activer DKIM

1. **Dans le portail `https://security.microsoft.com` : Email & collaboration → Stratégies et règles → Stratégies de menace → DKIM → `lurcat.fr` [4].**
2. **Le portail affiche les deux CNAME à créer, de la forme `selector1-lurcat-`**

`fr._domainkey.<tenant>.onmicrosoft.com` — les copier tels quels :

Nom	Type	Valeur
`selector1._domainkey`	CNAME	valeur affichée par le portail
`selector2._domainkey`	CNAME	valeur affichée par le portail

3. Revenir sur le portail et activer la signature DKIM pour le domaine.

9 Tokens de vérification Microsoft (optionnel)

Les deux tokens `MS=ms37403205` et `MS=ms30706699` constatés en mars ne sont pas nécessaires au fonctionnement une fois le domaine vérifié. Ne les remettre que si Microsoft redemande une vérification.

Point à clarifier

La présence de deux tokens suggère l'existence de deux tenants Microsoft pour `lurcat.fr` (actif et ancien). À trancher avec la direction : quel tenant porte les comptes étudiants, et lequel peut être décommissionné ?

10 Préparer le certificat Wi-Fi public (sans action DNS manuelle)

Pour le chantier `radius.lurcat.fr` (certificat public Let's Encrypt pour le serveur RADIUS, reconnu nativement par Android et Linux) : aucun enregistrement n'est à créer à la main. La validation DNS-01 [2] se fait par un TXT `_acme-challenge.radius.lurcat.fr` créé et supprimé automatiquement

via l'API EuroDNS.

Préparer seulement :

1. **activer l'accès API sur le compte EuroDNS ;**
2. **générer une clé API dédiée et la consigner au coffre.**

L'émission et le déploiement du certificat sur le serveur NPS feront l'objet d'un mode opératoire dédié.

5 Vérifications finales

Vérification

```
dig lurcat.fr MX +short            # 0
   lurcat-fr.mail.protection.outlook.com
dig lurcat.fr TXT +short           # v=spf1
   include:spf.protection.outlook.com -all
dig autodiscover.lurcat.fr +short  # autodiscover.outlook.com
dig selector1._domainkey.lurcat.fr +short  # CNAME Microsoft
dig _dmarc.lurcat.fr TXT +short    # v=DMARC1; p=none; ...
dig inexistant.lurcat.fr +short    # (vide)
```

Puis, côté fonctionnel :

— **mail externe vers `@lurcat.fr` distribué (étape 6) ;**

— **mail sortant d'un compte `@lurcat.fr` vers un service de test (par exemple mail-tester) remontant SPF, DKIM et DMARC valides ;**

— **domaine au statut « Healthy » dans le centre d'administration M365.**

6 Retour arrière

Le risque est faible : la zone publique ne porte aucun service en production autre que le mail — déjà en panne. Si une régression survenait, l'état antérieur se restaure en recréant le wildcard `*` (CNAME vers le parking) et l'enregistrement A de l'apex vers `80.92.65.214`, puis en supprimant les enregistrements ajoutés. Compter le délai de propagation (TTL 3600) avant toute conclusion.

Références

[1] AFNIC. *WHOIS — Retrouver un nom de domaine ou un titulaire*. https://www.afnic.fr/en/domain-names-and-support/everything-there-is-to-know-about-domain-names/find-a-domain-name-or-a-holder-using-whois/. 2026. (Visité le 06/10/2026).

[2] Let's Encrypt. *Challenge Types — DNS-01 challenge*. https://letsencrypt.org/docs/challenge-types/#dns-01-challenge. 2026. (Visité le 06/10/2026).

[3] Microsoft. *Ajouter des enregistrements DNS pour connecter votre domaine*. https://learn.microsoft.com/fr-fr/microsoft-365/admin/get-help-with-domains/create-dns-records-at-any-dns-hosting-provider. 2026. (Visité le 06/10/2026).

[4] Microsoft. *Comment utiliser DKIM pour le courrier sortant envoyé depuis votre domaine personnalisé*. https://learn.microsoft.com/fr-fr/defender-office-365/email-authentication-dkim-configure. 2026. (Visité le 06/10/2026).