

# Serveur de registre UXP 1.25

**Installation et configuration de la haute disponibilité.**

UXP-IG-RSHA

# Table des matières

---

<b>1. Introduction</b>	<b>1</b>
1.1. Public cible	1
1.2. Haute disponibilité pour le Serveur de registre UXP	1
1.3. Références	1
<b>2. Points clés et limites connues pour le déploiement HA du serveur de registre UXP</b>	<b>3</b>
<b>3. Exigences et flux opérationnels pour la configuration HA</b>	<b>5</b>
3.1. Exigences	5
3.2. Flux opérationnel pour la mise en place d'une nouvelle instance UXP	5
3.3. Flux opérationnel pour la mise à jour d'un Serveur de registre UXP existant vers une configuration HA	5
3.4. Flux opérationnel pour l'ajout de nouveaux nœuds à une configuration HA existante	6
3.5. Étapes post-configuration	7
<b>4. Installation générale du support HA</b>	<b>8</b>
<b>5. Modification des adresses IP des nœuds dans une grappe HA</b>	<b>10</b>
<b>6. Surveillance de l'état HA d'un nœud</b>	<b>11</b>
<b>7. Restaurer la grappe HA</b>	<b>12</b>

# 1. Introduction

---

## 1.1. Public cible

Ce guide s'adresse aux administrateurs système chargés d'installer et de configurer la solution haute disponibilité pour le logiciel Serveur de registre UXP.

Ce document est destiné aux lecteurs ayant une bonne connaissance de la gestion des serveurs Linux, des réseaux informatiques et des principes de fonctionnement de la technologie UXP.

## 1.2. Haute disponibilité pour le Serveur de registre UXP

La solution de haute disponibilité (HA) pour le serveur de registre repose sur la réplication de la base de données entre les nœuds. La mise en grappe fonctionne comme une base de données active-active asynchrone sans partage. Cela permet à chaque nœud de fonctionner comme un serveur de registre autonome qui reçoit des mises à jour de données de tous les autres nœuds.

Les serveurs de sécurité peuvent télécharger une configuration identique à partir de n'importe quelle adresse publique publiée dans un fichier d'ancrage de configuration. Il incombe à l'administrateur système de s'assurer que les nœuds du serveur de registre ne sont pas désynchronisés en raison d'une défaillance du réseau ou d'une autre défaillance. Des scripts de surveillance sont prévus à cet effet.

La solution prend en charge jusqu'à 48 nœuds avec un minimum de 2 nœuds.

Chaque nœud de serveur de registre possède ses propres :

- clés spécifiques au nœud pour signer la configuration ;
- adresse publique spécifique au nœud qui est distribuée aux clients de configuration dans les fichiers d'ancrage de la configuration ;
- éventuellement, serveur de sécurité de gestion.

Technologie utilisée :

- PostgreSQL 9.4 ;
- Plugin BDR pour PostgreSQL.

La version minimale du serveur de registre UXP est 1.6.

## 1.3. Références

- [UXP-IG-RS] Cybernetica AS. Serveur de registre UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-RS

- [UXP-UG-RS] Cybernetica AS. Serveur de registre UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-RS

## 2. Points clés et limites connues pour le déploiement HA du serveur de registre UXP

---

### 1. Un chronométrage correct est essentiel :

Le protocole NTP est installé lors de la configuration de la grappe sur tous les nœuds. On suppose que le réglage de l'heure système à l'aide du protocole NTP est activé. L'administrateur doit veiller à ce que l'heure soit toujours synchronisée. La résolution des conflits entre les nœuds de la base de données repose sur les horodatages : la modification la plus récente l'emporte et les plus anciennes sont rejetées. La surveillance de la dérive temporelle des serveurs est généralement suggérée.

### 2. Sécurité et rapidité du réseau :

Même si toutes les connexions aux bases de données regroupées sont sécurisées et authentifiées par TLS, la sécurité du réseau (en particulier la confidentialité et la disponibilité) doit être examinée au niveau de l'infrastructure. La vitesse du réseau n'est pas très critique pour l'application elle-même car la grappe fonctionne en mode asynchrone, mais elle peut affecter le temps d'initialisation de la grappe et le temps nécessaire pour que les changements soient distribués entre les nœuds.

### 3. Mises à jour UXP impliquant des modifications de la base de données :

Tous les nœuds configurés doivent être disponibles et fonctionner au moment où la mise à jour est appliquée. Les détails seront indiqués dans le journal des modifications, le cas échéant.

### 4. Tous les nœuds doivent utiliser la même version du système d'exploitation Ubuntu, le même niveau de correctifs du logiciel UXP et la même version du logiciel de base de données.

### 5. La configuration HA avec un seul nœud n'est pas prise en charge.

### 6. La suppression d'un nœud configuré n'est pas prise en charge. Ce problème sera résolu dans les prochaines versions.

### 7. Fenêtre temporelle pour la réparation des défaillances de nœuds :

Un nœud peut fonctionner (c'est-à-dire fournir une configuration globale valide à l'instance UXP) sans contacter d'autres nœuds configurés pendant une durée illimitée tant que le nombre de nœuds actifs est égal à  $(\text{nombre de nœuds totaux})/2 + 1$ . Si moins de nœuds sont actifs, jusqu'à 1 000 enregistrements peuvent être insérés dans chaque tableau de la base de données. Pour plus de détails, consultez la documentation sur [le vote par séquence globale](#).

### 8. Les fichiers de configuration (situés dans `/etc/uxp/`) ne sont pas synchronisés entre les nœuds. Il incombe à l'administrateur du système de les modifier dans tous les nœuds si

cela est nécessaire ou indiqué dans le guide de l'utilisateur.

## 3. Exigences et flux opérationnels pour la configuration HA

---

### 3.1. Exigences

Les nœuds doivent répondre à toutes les exigences énumérées dans le guide d'installation du Serveur de registre UXP (voir [\[UXP-IG-RS\]](#)). En outre, la création d'une configuration HA nécessite les éléments suivants :

- Accès au niveau root (sudo) à tous les nœuds pour installer la clé publique SSH autorisée pour l'utilisateur root.
- Accès SSH basé sur une clé à chaque nœud pour l'utilisateur root.

Il s'agit de la configuration par défaut du serveur SSH dans Ubuntu 22.04 Support à long terme (LTS). Si les serveurs ont une configuration différente, sauvegardez la configuration du serveur SSH avant de commencer à configurer la grappe.

- Ports ouverts entre les nœuds :
  - TCP 5432 (connexions à la base de données) ;
  - TCP 22 (SSH pour la configuration de la grappe).

### 3.2. Flux opérationnel pour la mise en place d'une nouvelle instance UXP

1. Installez la prise en charge HA en suivant les étapes décrites dans la section [\[General Installation of HA Support\]](#).
2. Installez le logiciel du serveur de registre conformément au guide d'installation du Serveur de registre UXP [\[UXP-IG-RS\]](#) sur chaque nœud.

### 3.3. Flux opérationnel pour la mise à jour d'un Serveur de registre UXP existant vers une configuration HA

1. Mettez à jour le logiciel du serveur de registre existant vers la dernière version disponible, puis vérifiez l'état du système.
2. Créez une sauvegarde de la configuration du système et conservez-la en lieu sûr.
3. Poursuivez les étapes d'installation du support HA comme décrit dans la section [\[General Installation of HA Support\]](#).
4. Installez le logiciel du serveur de registre conformément au guide d'installation du Serveur de registre UXP [\[UXP-IG-RS\]](#) sur chaque nœud.
5. Après avoir installé et configuré tous les nœuds du serveur de registre, récupérez les nouveaux fichiers d'ancrage de configuration interne et externe sur l'un des nœuds et

distribuez les fichiers comme suit :

- l'ancre de configuration interne et sa valeur de hachage à tous les propriétaires de serveurs de sécurité et aux serveurs de surveillance ;
- l'ancre de configuration externe et sa valeur de hachage à tous les partenaires de la fédération, s'ils existent.

### 3.4. Flux opérationnel pour l'ajout de nouveaux nœuds à une configuration HA existante

Pour ajouter de nouveaux nœuds à l'environnement HA existant, tous les paquets UXP (à l'exception de `uxp-addon-registry-clusterhelper`) doivent être purgés de tous les autres nœuds, à l'exception du serveur sur lequel le script de création HA va être lancé. Si des paquets UXP sont détectés sur des nœuds autres que le premier, l'installation est interrompue.

1. Mettez à jour le logiciel UXP des nœuds existants vers la dernière version disponible, puis vérifiez l'état du système sur tous les nœuds.
2. Créez une configuration de sauvegarde du système des nœuds existants et conservez-la dans un endroit sûr.
3. Purguez les paquets UXP dans tous les nœuds à l'exception du serveur où la grappe va être initialisée (premier nœud) :

```
sudo apt purge uxp-addon-registry-monitor uxp-confclient uxp-jetty uxp-registry \
uxp-registry-monitor uxp-registryserver uxp-signer
```

```
sudo apt purge postgresql*
sudo rm -r /etc/uxp/
```

```
$ sudo dpkg -l | grep uxp
```

```
ii uxp-addon-registry-clusterhelper 1.25.0          all          UXP Registry
Server cluster scripts
```

4. Sur le nœud où la grappe a été initialisée :
  - a. Ajoutez les adresses IP des nouveaux nœuds à la fin du fichier `/etc/uxp/cluster/nodes`. Ne supprimez ni ne modifiez aucune ligne existante.
  - b. Réexécutez le script d'initialisation de la grappe :

```
sudo -i -u uxp /usr/share/uxp/scripts/uxp_create_cluster.sh
```

5. Installez le logiciel serveur de registre UXP comme décrit dans le Guide d'installation du Serveur de registre UXP [UXP-IG-RS] sur chacun des nouveaux nœuds.
6. Après avoir installé et configuré tous les nœuds du serveur de registre, récupérez les nouveaux fichiers d'ancrage de configuration interne et externe sur l'un des nœuds et distribuez les fichiers comme suit :



- l'ancre de configuration interne et sa valeur de hachage à tous les propriétaires de serveurs de sécurité et aux serveurs de surveillance ;
- l'ancre de configuration externe et sa valeur de hachage à tous les partenaires de la fédération, s'ils existent.

### 3.5. Étapes post-configuration

Une fois la grappe de bases de données configurée et les paquets du serveur de registre installés, il est conseillé de supprimer les clés générées lors de la configuration de la grappe.

Si l'accès SSH par clé aux nœuds par l'utilisateur root a été désactivé avant d'être activé pour la configuration de la grappe, la configuration correspondante du serveur SSH doit être rétablie.

## 4. Installation générale du support HA

1. Installez le paquet de gestion de la grappe sur un nœud (à partir du dépôt UXP configuré comme décrit dans le guide d'installation du Serveur de registre UXP [\[UXP-IG-RS\]](#)) :

```
sudo apt install uxp-addon-registry-clusterhelper
```

2. Créez/modifiez une liste d'adresses IP de nœuds HA dans `/etc/uxp/cluster/nodes`
  - une IP par ligne, pas d'espace, pas de commentaire ;
  - le nœud à mettre à niveau de non-HA→HA (le cas échéant) doit se trouver en première position dans le fichier des nœuds ;
  - Ne supprimez ni ne modifiez aucune ligne existante dans le fichier des nœuds.

Exemple de contenu du fichier des nœuds :

```
$ cat /etc/uxp/cluster/nodes
192.168.56.201
192.168.56.202
```

3. Exécutez le script de configuration de la grappe et suivez les instructions :

```
sudo -i -u uxp /usr/share/uxp/scripts/uxp_create_cluster.sh
```

Ce qui est fait pendant la configuration :

- Une clé SSH est configurée et une commande permettant de distribuer la clé SSH à tous les serveurs s'affiche. **La clé publique doit être distribuée manuellement à tous les serveurs avant de permettre au script de continuer.** L'accès SSH à tous les nœuds est ensuite vérifié.
- NTP est installé et la synchronisation immédiate du temps NTP est appelée pour garantir l'exactitude du temps sur tous les nœuds.
- Une autorité de certification auto-signée est créée et les clés TLS pour les connexions sécurisées à la base de données sont générées.
- PostgreSQL 9.4 avec le plugin BDR est installé et configuré pour établir des connexions de base de données entre les nœuds.
- Un rôle de base de données spécifique à UXP est créé avec les fonctionnalités nécessaires. Si le premier nœud contient une ancienne base de données avec le schéma de base de données UXP, l'ancien schéma de base de données sera migré vers la nouvelle base de données.



L'emplacement du fichier journal contenant des informations détaillées sur la progression de l'initialisation est affiché lorsque vous lancez le script d'initialisation de la grappe. Les journaux sont nommés `/var/log/uxp/cluster_<datetime>.log`.



Vous pouvez réexécuter le script d'initialisation de la grappe après avoir corrigé les problèmes qui ont provoqué l'arrêt du script.

4. Installez le paquet d'aide pour la grappe de serveur de registre UXP sur tous les nœuds ajoutés :

```
sudo apt install uxp-addon-registry-clusterhelper
```

En plus du script d'installation de la grappe, le paquet fournit des outils pour surveiller l'état de la grappe.

## 5. Modification des adresses IP des nœuds dans une grappe HA

---

Le script de modification des adresses IP des nœuds d'une grappe HA se comporte de la même manière que le script d'installation du support HA.

Pour modifier les adresses IP des nœuds :

1. Remplacez les adresses IP du système dans tous les nœuds de la grappe.
2. Assurez-vous que PostgreSQL fonctionne avec le support de bdr-9.4.
3. Créez un nouveau fichier de nœuds `/etc/uxp/cluster/nodes.new`, contenant `<ancienne-IP> <nouvelle-IP>` par ligne, par exemple :

```
192.168.56.40 192.168.57.45  
192.168.56.41 192.168.57.46
```

4. Exécutez le script `modify_cluster.sh` :

```
sudo -i -u uxp /usr/share/uxp/scripts/modify_cluster.sh
```

Le script va :

- remplacer les adresses IP dans le fichier `/etc/uxp/cluster/nodes` ;
- modifier le fichier de configuration PostgreSQL ;
- alterner les IP dans les tableaux Postgres-BDR.

## 6. Surveillance de l'état HA d'un nœud

Un script permettant de vérifier l'état de santé de la grappe est disponible sur chaque nœud avec le paquet `uxp-addon-registry-clusterhelper`. Pour afficher l'état de la grappe, exécutez la commande suivante :

```
/usr/share/uxp/scripts/check_ha_cluster_status.py
```

L'exemple de sortie est similaire à ce qui suit (en mettant l'accent sur les valeurs importantes) :

```
SUMMARY OF CLUSTER STATUS:
All nodes: OK
Configuration: OK

DETAILED CLUSTER STATUS INFORMATION:
{
  "all_nodes_ok": true,
  "configuration_ok": true,
  "ha_configured": true,
  "nodes": {
    "node_0": {
      "external_anchor_update_timestamp": "2017-05-03T08:40:30Z",
      "internal_anchor_update_timestamp": "2017-05-03T08:40:25Z",
      "node_status": "ready",
      "private_params_update_timestamp": "2017-05-10T10:46:02Z",
      "shared_params_update_timestamp": "2017-05-10T10:46:02Z"
    },
    "node_1": {
      "external_anchor_update_timestamp": "2017-05-03T08:40:30Z",
      "internal_anchor_update_timestamp": "2017-05-03T08:40:25Z",
      "node_status": "ready",
      "private_params_update_timestamp": "2017-05-10T10:46:01Z",
      "replication_client_address": "192.168.3.229",
      "replication_lag_bytes": "0",
      "replication_state": "streaming",
      "shared_params_update_timestamp": "2017-05-10T10:46:01Z"
    }
  }
}
```

Les horodatages des fichiers de paramètres privés et partagés générés sur différents nœuds doivent se situer dans une fenêtre temporelle raisonnable. Les horodatages des ancres internes et externes doivent être identiques.

## 7. Restaurer la grappe HA

Cette section décrit les étapes nécessaires à la restauration d'un système défaillant ayant entraîné la perte de tous les nœuds de la grappe.

1. Initialisez une grappe HA **sur au moins deux nœuds**. Voir la section [\[General Installation of HA Support\]](#). Si la grappe initiale est composée de plus de deux nœuds, des nœuds supplémentaires peuvent être ajoutés ultérieurement.
2. Installez le logiciel serveur de registre UXP conformément au guide d'installation du Serveur de registre UXP [\[UXP-IG-RS\]](#) sur le **premier nœud**.
3. Restaurez la configuration du système **sur le premier nœud (node\_0) en utilisant la sauvegarde de node\_0**. À partir de la ligne de commande, en spécifiant l'**identifiant d'instance** correct et l'**emplacement du fichier de sauvegarde** (sur une seule ligne) :

```
sudo -i -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh \
-i CC -n node_0 -f /root/rs_backup_20170303-125451.tar
```

Pour plus d'informations sur la restauration, consultez le Guide de l'utilisateur de Serveur de registre UXP [\[UXP-UG-RS\]](#).

4. Vérifiez l'interface utilisateur du serveur de registre pour vous assurer que les données sont correctes. Vérifiez spécifiquement les clés de signature de configuration, leur disponibilité et leur exactitude. Si nécessaire, modifiez l'adresse du serveur de registre.
5. Installez le logiciel serveur de registre UXP conformément au guide d'installation de Serveur de registre UXP [\[UXP-IG-RS\]](#) sur les **autres nœuds**.
6. Restaurez la configuration du système **sur le deuxième nœud (node\_1) en utilisant la sauvegarde de node\_1**. À partir de la ligne de commande, en spécifiant le **code d'instance** et l'**emplacement du fichier de sauvegarde** corrects (sur une seule ligne) :

```
sudo -i -u uxp /usr/share/uxp/scripts/restore_uxp_registry_configuration.sh \
-S -i CC -n node_1 -f /root/rs_backup_20170303-125524.tar
```



**Veillez noter le paramètre supplémentaire -S** – cela empêche la restauration de la base de données puisqu'elle a déjà été restaurée à l'étape 3. Pour plus d'informations sur la restauration, consultez le Guide de l'utilisateur de Serveur de registre [\[UXP-UG-RS\]](#).

7. Vérifiez l'interface utilisateur du serveur de registre pour vous assurer que les données sont correctes. Vérifiez spécifiquement les clés de signature de configuration, leur disponibilité et leur exactitude. Si nécessaire, modifiez l'adresse du serveur de registre.
8. Pour les autres nœuds, répétez les étapes 6 et 7 en modifiant l'identifiant du nœud de la grappe.
9. Si les clés de configuration ou les adresses du système de registre ont été modifiées pendant la restauration, de nouveaux fichiers d'ancrage de configuration interne et externe

doivent être distribués aux membres, comme suit :

- l'ancre de configuration interne et sa valeur de hachage à tous les propriétaires de serveurs de sécurité et aux serveurs de surveillance ;
- l'ancre de configuration externe et sa valeur de hachage à tous les partenaires de la fédération, s'ils existent.