

Serveur de sécurité UXP 1.25

Configuration de la haute disponibilité et de l'équilibrage de la charge

UXP-UG-SSHA

Table des matières

1. Introduction	1
1.1. Public cible	1
1.2. Haute disponibilité et équilibrage de charge pour Serveur de sécurité UXP	1
1.3. Références	1
2. Grappe de serveurs de sécurité pour la haute disponibilité	2
2.1. Grappe de serveurs de sécurité client	2
2.2. Grappe de serveurs de sécurité fournisseur	3
2.2.1. Sélection du nœud de la grappe cible	3
2.2.2. Désactiver des nœuds de grappe défectueux	4
2.3. Informations sur l'état du serveur de sécurité	4
2.3.1. Configurer les informations sur l'état	4
2.3.2. Réponse du service d'informations sur l'état	5
2.4. proxyOff	6
2.4.1. Grappes clients	6
2.4.2. Grappes fournisseurs	7
2.5. Configurer et maintenir une grappe de serveurs de sécurité	7
2.5.1. Services d'exportation et droits d'accès	8
2.5.2. Services d'importation et droits d'accès	10
Importer un fichier	10
Gestion des différences	12
Comparer les métadonnées de fichiers	13
2.5.3. Ajouter un nœud de serveur de sécurité supplémentaire	14
2.5.4. Supprimer un nœud de serveur de sécurité de la grappe	14
2.5.5. Modifier l'adresse IP ou le nom DNS d'un nœud de serveur de sécurité	15
3. Équilibreurs de charge	16
3.1. Équilibreur de charge interne	16
3.1.1. Exemple HAProxy	17
3.2. Équilibreur de charge de service	19
4. Dépannage	20
4.1. L'importation du fichier de configuration a échoué : <path-to-configuration-file>	20
4.2. Échec de la connexion à <adresse IP> port <port> après 0 ms : Connexion refusée	20

1. Introduction

1.1. Public cible

Ce guide s'adresse aux administrateurs système responsables des solutions de haute disponibilité ou d'équilibrage de charge pour le logiciel Serveur de sécurité 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.

La plupart des actions de ce guide supposent que le lecteur a accès à l'interface de ligne de commande du serveur de sécurité.

1.2. Haute disponibilité et équilibrage de charge pour Serveur de sécurité UXP

La solution de haute disponibilité (HA) pour les serveurs de sécurité UXP repose sur le fait que plusieurs serveurs de sécurité peuvent traiter les messages UXP pour le même service UXP. En substance, cela signifie que l'HA est assurée par une grappe de serveurs de sécurité ayant chacun la même configuration de service.

Une grappe de serveurs de sécurité peut être associée à un équilibreur de charge tiers pour améliorer les performances (voir la section [Équilibreurs de charge](#)).

1.3. Références

- [Apache] Projet de serveur HTTP Apache, <https://httpd.apache.org/>
- [HAProxy] Équilibreur de charge TCP/HTTP HAProxy, <http://www.haproxy.org/>
- [JSON] Présentation de JSON, <http://json.org/>
- [Nginx] Bienvenue sur le site de F5 NGINX | F5, <https://www.f5.com/go/product/welcome-to-nginx>
- [UXP-IG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide d'installation et de configuration. Identifiant du document : UXP-IG-SS
- [UXP-UG-PMA] Cybernetica AS. Serveur de sécurité UXP : Configurer la surveillance du serveur de sécurité. Identifiant du document : UXP-UG-PMA
- [UXP-UG-SS] Cybernetica AS. Serveur de sécurité UXP : Guide de l'utilisateur. Identifiant du document : UXP-UG-SS

2. Grappe de serveurs de sécurité pour la haute disponibilité

Afin d'assurer la haute disponibilité d'un service UXP, une grappe de serveurs de sécurité peut être mise en place.

Dans le cadre UXP, une grappe est constituée de deux ou plusieurs serveurs de sécurité (appelés nœuds dans le contexte d'une grappe) capables de traiter des demandes pour le même service UXP. Cela signifie que tous les nœuds d'une grappe doivent avoir la même configuration.

Une grappe peut être mise en place du côté du client du service ou du côté du fournisseur du service. Voir les sections [grappe client](#) et [grappe fournisseur](#) pour plus de détails sur la configuration nécessaire pour l'une ou l'autre configuration.

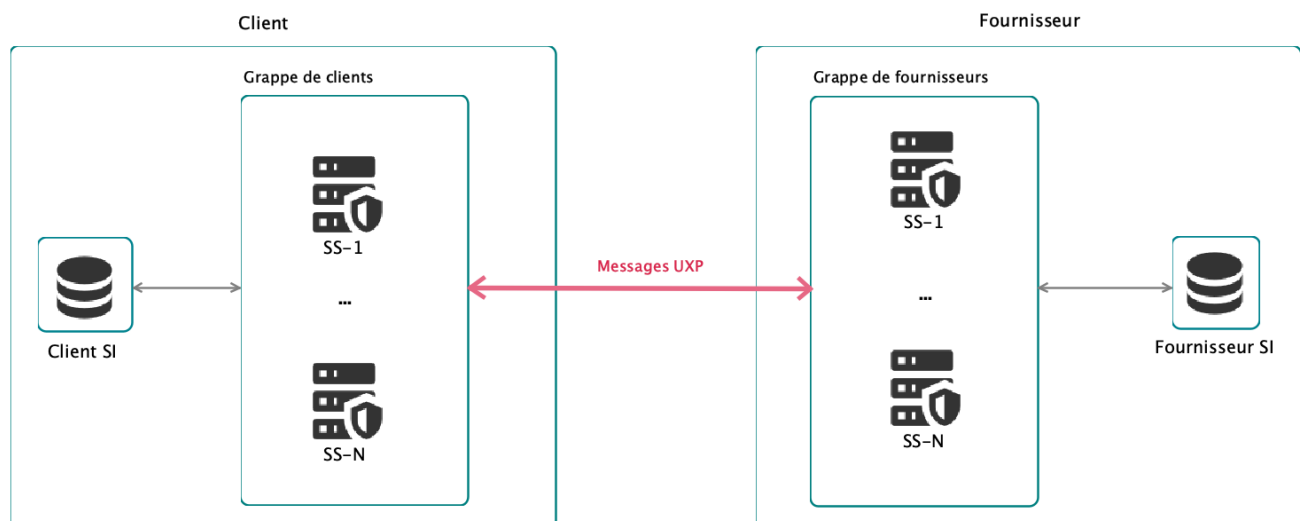


Figure 1. Exemple de configuration UXP avec des grappes de serveurs de sécurité pour les clients et les fournisseurs de services

2.1. Grappe de serveurs de sécurité client

Une grappe de serveurs de sécurité client offre une haute disponibilité pour la communication entre le système d'information (SI) du client et les serveurs de sécurité client. Dans ce scénario, une certaine logique doit être mise en œuvre du côté du SI client pour que celui-ci puisse choisir le serveur de sécurité auquel il envoie une demande donnée.

Cela signifie que chaque nœud de la grappe doit avoir :

- le(s) même(s) client(s) enregistré(s) ;
- une configuration globale valide ;
- une clé et un certificat d'authentification fonctionnels ;

- une clé de signature et un certificat fonctionnels pour chaque client ;
- si une connexion HTTPS est utilisée entre le serveur de sécurité et le système d'information, une clé et un certificat TLS internes fonctionnels pour le serveur de sécurité et une clé et un certificat TLS internes fonctionnels pour chaque système d'information.

Pour plus de détails sur chacun de ces éléments, voir le Guide de l'utilisateur du Serveur de sécurité UXP [\[UXP-UG-SS\]](#).

La grappe de serveurs de sécurité client est compatible avec des équilibreur de charge tiers (voir la section [Équilibreur de charge interne](#)).

2.2. Grappe de serveurs de sécurité fournisseur

Une grappe de serveurs de sécurité fournisseur assure la haute disponibilité de la communication entre le serveur de sécurité client et les serveurs de sécurité fournisseur.

Cela signifie que chaque nœud de la grappe doit avoir :

- le(s) même(s) client(s) enregistré(s) ;
- les mêmes services enregistrés (avec le même membre, le même sous-système et le même code de service) ;
- les mêmes droits d'accès aux services ;
- une configuration globale valide ;
- une clé et un certificat d'authentification fonctionnels ;
- une clé de signature et un certificat fonctionnels pour chaque client ;
- si une connexion HTTPS est utilisée, une clé et un certificat TLS internes fonctionnels pour le serveur de sécurité et une clé et un certificat TLS internes fonctionnels pour chaque système d'information.

Pour plus de détails sur chacun de ces éléments, voir le Guide de l'utilisateur du Serveur de sécurité UXP [\[UXP-UG-SS\]](#).



La grappe de serveurs de sécurité ne prend pas en charge les limites de débit des services parce que les limites contrôlent la consommation de service sur chaque nœud séparément, mais pas uniformément sur l'ensemble de la grappe.



Un nœud doit fonctionner pour être inclus dans la grappe – il n'existe pas de mécanisme intégré permettant d'activer de nouveaux nœuds pour remplacer les nœuds défectueux.

2.2.1. Sélection du nœud de la grappe cible

À partir de la version 1.20, les serveurs de sécurité utilisent par défaut la stratégie `round-robin` pour transférer les requêtes vers une grappe de fournisseurs de services, contrairement à la stratégie `fastest-connected` utilisée précédemment.

Avec la stratégie `round-robin`, un serveur de sécurité client distribue cycliquement les demandes entre les nœuds de la grappe du fournisseur de services qui répondent à la demande d'établissement de connexion du protocole de contrôle de transmission (TCP). La stratégie `round-robin` équilibre la charge entre différents nœuds et ne privilégie pas un seul nœud comme la stratégie `fastest-connected`.

Avec la stratégie `fastest-connected`, un serveur de sécurité client transmet la demande au nœud en grappe du fournisseur qui répond le plus rapidement à une demande d'établissement de connexion TCP. La rapidité de la réponse peut être affectée par la topologie du réseau ou l'ordre dans lequel les nœuds ont été contactés. La stratégie `fastest-connected` ne permet pas d'équilibrer la charge.

Pour que les stratégies `round-robin` et `fastest-connected` soient efficaces, il faut que chaque nœud puisse jouer le rôle de fournisseur de services, c'est-à-dire que chaque nœud dispose d'une [configuration opérationnelle et à jour](#).

2.2.2. Désactiver des nœuds de grappe défectueux

Les propriétaires de grappe peuvent éventuellement configurer un service qui désactive un nœud lorsqu'il répond négativement à une requête [informations d'état](#) (voir la section [proxyOff](#)). Cela permet d'éviter que les messages UXP soient envoyés aux nœuds de la grappe qui ne sont pas en mesure de traiter ceux-ci.

2.3. Informations sur l'état du serveur de sécurité

Chaque serveur de sécurité fournit un service d'information sur l'état qui indique si ce serveur de sécurité remplit actuellement les principales conditions pour traiter les messages UXP.



Il existe certaines conditions que le service d'information sur l'état ne peut pas vérifier, mais qui entraînent tout de même l'échec du traitement des messages UXP par un serveur de sécurité (par exemple, des problèmes du côté du service d'horodatage). Pour obtenir la liste des conditions vérifiées par les informations d'état, consultez la section [Réponse du service d'informations d'état](#).

La fonctionnalité [proxyOff](#) et certains [équilibres de charge](#) peuvent utiliser ces informations pour s'assurer que les demandes ne sont transmises qu'aux serveurs de sécurité capables de traiter les messages UXP, en fonction des informations sur l'état du serveur de sécurité. Pour plus d'informations sur l'intégration des informations d'état avec les équilibreurs de charge, consultez la section [Équilibreurs de charge](#).

2.3.1. Configurer les informations sur l'état

Pour configurer le service d'information sur l'état d'un serveur de sécurité, la section `[status-service]` doit être ajoutée au fichier de configuration `/etc/uxp/conf.d/local.ini` de ce serveur de sécurité :

```
[status-service]

; The status service listen address.
listen-address=127.0.0.1

; The status service listen HTTP port.
listen-port=2082

; The comma-separated list of host IP-addresses and/or CIDR notations that
; determine allowed addresses to request status information.
allowed-hosts=127.0.0.1
```

L'adresse d'écoute du service d'état (`listen-address`) est `localhost` par défaut. Si le service d'état doit être accessible par un service externe (par exemple, un équilibreur de charge), l'adresse d'écoute doit être remplacée par l'adresse IP du serveur de sécurité ou par une adresse IP générique (`0.0.0.0` pour IPv4 / `[::]` pour IPv6).

Le port d'écoute par défaut (`listen-port`) est 2082.

Le seul hôte autorisé par défaut (`allowed-hosts`) est `localhost`. La liste des hôtes autorisés doit être modifiée pour contenir les adresses à partir desquelles les demandes d'informations sur l'état sont effectuées (par exemple, les équilibreurs de charge).

Une fois les modifications apportées, redémarrez le service de surveillance sur le serveur de sécurité :

```
sudo systemctl restart uxp-monitor
```

Tous les hôtes autorisés (adresses écrites dans une liste séparée par des virgules) peuvent demander les informations d'état, par exemple en faisant la demande suivante :

```
curl -v http://<security-server-address>:<status-request-listen-port>/status
```

à l'aide de l'outil en ligne de commande `curl`.

Ce service doit être appelé à l'aide de la méthode GET.

2.3.2. Réponse du service d'informations sur l'état

Le point de terminaison des informations d'état renvoie le code d'état HTTP 200 (signifiant que l'état est UP) pour un serveur de sécurité donné si et seulement si toutes les conditions suivantes sont remplies :

- le processus proxy du serveur de sécurité est en cours d'exécution ;
- la configuration globale est valide ;
- la clé d'authentification est active, valide (sur la base de la date figurant dans le certificat) et l'état de la réponse OCSP est bon ;
- le jeton stockant la clé d'authentification (jeton logiciel) est connecté.

Si au moins l'une des conditions ci-dessus n'est pas remplie, le point de terminaison renvoie le code d'état HTTP 503 (ce qui signifie que l'état est DOWN).

Si la demande provient d'une adresse IP non autorisée, le point de terminaison renvoie le code d'erreur HTTP 403.

En cas d'autres erreurs, le point de terminaison renvoie le code d'erreur HTTP approprié.

2.4. proxyOff

Vous pouvez configurer les nœuds de votre grappe pour qu'ils cessent d'accepter des connexions si leur [statut](#) est DOWN. Cette fonction, appelée proxyOff, permet d'accroître la fiabilité des grappes de serveurs de sécurité et des équilibreurs de charge qui ne peuvent pas intégrer directement le service d'information sur l'état. Pour plus d'informations sur l'association de proxyOff avec des équilibreurs de charge, consultez la section [Équilibreurs de charge](#).

La fonction proxyOff permet d'éviter l'envoi de messages UXP aux nœuds de la grappe qui répondent à une requête TCP tout en étant incapables de traiter les messages UXP.



Il n'est pas nécessaire de configurer le service d'[information sur l'état](#) pour configurer la fonction proxyOff. En effet, proxyOff demande les informations d'état en interne sans avoir besoin d'utiliser le service d'information d'état.

Pour configurer la fonction proxyOff sur un nœud d'une grappe, ajoutez la section [proxy-status-check] au fichier de configuration /etc/uxp/conf.d/local.ini de ce nœud :

```
[proxy-status-check]

; Whether to stop listening for HTTP(S) connections from client applications
; in case the proxy status is down.
clientproxy-listening-switch-enabled=true

; Whether to stop listening for HTTPS connections from the service client's
; security server(s) in case the proxy status is down.
serverproxy-listening-switch-enabled=true

; Proxy status check interval in seconds (minimum value is 10).
interval-seconds=15
```

Le paramètre interval-seconds détermine la fréquence à laquelle la fonction proxyOff vérifie l'état du serveur de sécurité.

2.4.1. Grappes clients

Si l'option clientproxy-listening-switch-enabled est définie sur true sur un serveur de sécurité et que ce serveur de sécurité répond à une [demande d'information sur l'état](#) avec l'état DOWN, le serveur de sécurité cesse d'accepter les connexions sur le port qui écoute les

connexions des systèmes d'information des clients du service (applications). Les ports par défaut sont 80 et 443.

Lorsque la réponse de l'état du serveur de sécurité devient à nouveau UP, le port recommence à accepter des connexions.

2.4.2. Grappes fournisseurs

Si l'option `serverproxy-listening-switch-enabled` est définie sur `true` sur un serveur de sécurité et que ce serveur de sécurité répond à une [demande d'informations sur l'état](#) avec l'état DOWN, le serveur de sécurité cesse d'accepter des connexions sur le port qui écoute les connexions des serveurs de sécurité clients du service. Le port par défaut est 5500.

Lorsque la réponse de l'état du serveur de sécurité devient à nouveau UP, le port recommence à accepter des connexions.

2.5. Configurer et maintenir une grappe de serveurs de sécurité

Pour réaliser une grappe de serveurs de sécurité, vous devez configurer plusieurs serveurs de sécurité avec des sous-systèmes et des services identiques.

Si la configuration d'une grappe de serveurs de sécurité change, vous devez propager manuellement les modifications à tous les nœuds de la grappe.

Les objets qui doivent être propagés à tous les nœuds de la grappe sont les suivants :

- clients du serveur de sécurité ;
- services ;
 - droits d'accès aux services ;
 - tous les points de terminaison de tous les services REST ;
 - tous les groupes locaux utilisés pour les droits d'accès ;
- type de connexion (pour la communication avec les systèmes d'information) ;
- certificats TLS internes du système d'information.

Au lieu de mettre à jour manuellement tous les clients et services un par un sur chaque nœud de la grappe, il est possible d'exporter et d'importer la configuration des services d'un serveur de sécurité à l'autre. La procédure est la suivante :

1. Installez et configurez plusieurs serveurs de sécurité si vous ne l'avez pas encore fait. Assurez-vous que les serveurs de sécurité ont le même propriétaire mais des codes serveur différents.
2. Choisissez un serveur de sécurité sur lequel vous appliquerez les changements de configuration (serveur de sécurité source).

3. Mettez à jour la configuration des services sur le serveur de sécurité source.
4. Exportez le fichier de configuration des nœuds de la grappe à partir de ce serveur de sécurité source.
5. Importez ce fichier de configuration du nœud de la grappe vers chaque autre nœud de la grappe (serveur de sécurité cible).

Vous pouvez utiliser l'importation et l'exportation de la configuration pour configurer la grappe en important la configuration sur des serveurs de sécurité correctement installés et utiliser également ce processus pour mettre à jour la configuration sur des nœuds de la grappe déjà fonctionnels.



Les clés et les certificats de signature ou d'authentification doivent être gérés manuellement car ils ne sont *pas* contenus dans le fichier de configuration du nœud de la grappe.

2.5.1. Services d'exportation et droits d'accès



Si la version du serveur de sécurité cible est différente de la version du serveur de sécurité où le fichier de configuration du nœud de la grappe a été créé, l'importation peut échouer. Il est recommandé de mettre à jour tous les serveurs de sécurité avant de créer le fichier de configuration du nœud de la grappe et de l'importer.

Pour exporter tous les clients du serveur de sécurité avec leurs services et leurs droits d'accès dans un fichier, procédez comme suit :

1. Utilisez l'utilitaire d'exportation :

```
serverconf-export [-d <dir> | -p <absolute-path-to-exported-file>]
```

Par exemple, pour exporter la configuration vers le dossier `/var/tmp`, exécutez la commande suivante :

```
sudo su - uxp -c "serverconf-export -d /var/tmp"
```

L'utilitaire enregistre la configuration dans un fichier JSON `uxp-serverconf-<hostname>-<timestamp>-<version>.json` dans le répertoire `/var/tmp/`.



L'utilitaire enregistre le résultat de l'exportation (succès ou échec) directement sur la console. Vous pouvez modifier la configuration de la journalisation dans le fichier `/etc/uxp/conf.d/serverconf-cli-logback.xml`.

Si vous souhaitez donner un nom différent à votre fichier de configuration, vous pouvez utiliser le paramètre `-p` pour fournir le chemin d'accès complet et le nom du fichier. Par exemple :

```
sudo su - uxp -c "serverconf-export -p /var/tmp/ssl-conf.json"
```

Un exemple de configuration exportée :



Vous pouvez remonter un fichier de configuration jusqu'au serveur de sécurité sur lequel il a été créé, car le fichier contient l'adresse IP et le nom d'hôte du serveur de sécurité à partir duquel le fichier a été exporté.

```
{
  "metadata": {
    "version": 2,
    "timestamp": 1719411206511,
    "securityServerId": {
      "xRoadInstance": "INSTANCE",
      "memberClass": "GOV",
      "memberCode": "00000000",
      "serverCode": "CODE"
    },
    "securityServerInternalIp": "192.168.12.34",
    "hostname": "server-hostname"
  },
  "configuration": {
    "clients": [
      {
        "clientId": {
          "xRoadInstance": "INSTANCE",
          "memberClass": "GOV",
          "memberCode": "00000000",
          "subsystemCode": "Subsystem"
        },
        "connectionType": "SSLAUTH",
        "restApis": [
          {
            "appliedRateLimits": [],
            "endpoints": [
              {
                "path": "*",
                "generated": true,
                "addedDate": 1661768036942
              }
            ],
            "headers": [],
            "disabled": false,
            "disabledNotice": "Out of order",
            "serviceCode": "serviceCode",
            "serviceVersion": "serviceVersion",
            "baseUrl": "https://<url>",
            "sslAuthentication": false,
            "timeout": 60,
            "addedDate": 1661768036942
          }
        ]
      }
    ]
  }
}
```

```

    "wsdls": [],
    "localGroups": [],
    "isCerts": [],
    "acl": [],
    "rateLimits": []
  }]
}
}

```

2. Enregistrez le hachage du fichier afin de pouvoir le comparer ultérieurement au hachage du fichier de configuration du nœud de la grappe que vous allez importer pour vous assurer que le fichier est identique et n'a pas été modifié.

Vous pouvez également utiliser l'[outil serverconf-metadata](#) pour vérifier à tout moment le hachage SHA-512 du fichier de configuration d'un nœud de la grappe.

3. L'étape suivante consiste à importer le fichier sur le serveur de sécurité cible. Voir la section suivante.

2.5.2. Services d'importation et droits d'accès

Le fichier de configuration des nœuds de la grappe peut être utilisé pour importer des services et des droits d'accès vers les nœuds de la grappe du serveur de sécurité.

Importer un fichier

Vous pouvez utiliser le fichier de configuration exporté du serveur source pour importer des services et des droits d'accès vers un serveur de sécurité nouvellement installé ou pour mettre à jour un nœud de la grappe déjà en fonctionnement.

1. Copiez le fichier de configuration exporté (l'exportation est décrite dans la section [Exportation des services et des droits d'accès](#)) du serveur de sécurité source vers le serveur de sécurité cible. La commande `scp` exige que vous disposiez d'une méthode d'authentification opérationnelle entre les serveurs de sécurité source et cible. Vous pouvez également utiliser un programme comme WinSCP sur votre ordinateur pour déplacer le fichier.

Utilisation de la commande à exécuter sur le serveur de sécurité source :

```

sudo scp <full-path-to-configuration-file> \
<username>@<target-ss-address>:<full-path-to-configuration-file>

```

- `<full-path-to-configuration-file>` est le chemin d'accès complet et le nom du fichier contenant la configuration du serveur de sécurité source ;
- `<username>` est le nom d'utilisateur du compte de l'administrateur système sur le serveur de sécurité cible ;
- `<target-ss-address>` est l'adresse IP ou le nom d'hôte du serveur de sécurité cible.

Par exemple :

```
sudo scp /var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json \
john@192.168.0.1:/var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json
```

2. Vérifiez le dossier `/var/tmp/` sur le serveur de sécurité cible pour voir si le déplacement du fichier a réussi.

```
ls /var/tmp/
```

3. Modifiez les privilèges du fichier de configuration, par exemple :

```
sudo chown uxp:uxp /var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json
```

4. Importez les services et les droits d'accès du fichier de configuration vers le serveur de sécurité cible.

Utilisation de l'utilitaire d'importation :

```
serverconf-import [-m [a|i|c]] [-r [a|i]] <full-path-to-configuration-file>
```

Exemple d'utilisation pour importer la configuration, où les nouveaux clients de la configuration seront ajoutés au serveur de sécurité cible et les clients qui sont déjà dans le serveur cible seront conservés :

```
sudo su - uxp -c "serverconf-import -m c -r i \
/var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json"
```

Les paramètres `-m` (missing) et `-r` (redundant) déterminent la manière dont les conflits concernant les clients du serveur de sécurité dans le fichier de configuration et le serveur cible sont gérés (voir la section [Gestion des différences](#)).

Pour les clients qui figurent dans le fichier de configuration mais qui **sont absents** (`-m`) du serveur cible, les actions disponibles sont les suivantes : `a` (**abandonner**), `i` (**ignorer**), `c` (**ajouter un client**). Si aucune action n'est spécifiée, l'action par défaut `c` (**ajouter un client**) est utilisée.

Pour les clients qui se trouvent déjà sur le serveur cible mais pas dans le fichier de configuration (**redondants** (`-r`)), les actions disponibles sont les suivantes : `a` (**abandonner**), `i` (**ignorer**). Si aucune action n'est spécifiée, l'action par défaut `i` (**ignorer**) est utilisée.



L'utilitaire enregistre le résultat de l'importation (succès ou abandon) et liste par défaut les clients manquants et redondants directement sur la console. Notez que le résultat est `aborted` uniquement lorsque l'option `a` a été choisie pour les clients manquants (ou redondants) pour l'importation et que des clients manquants (ou redondants) ont été trouvés, entraînant donc l'interruption de l'importation. Pour les importations qui ont échoué en raison d'erreurs du système, l'échec est également consigné par défaut directement sur la console. Vous pouvez modifier la

configuration de la journalisation dans le fichier `/etc/uxp/conf.d/serverconf-cli-logback.xml`.

5. Si l'importation a réussi, vous devriez voir les sous-systèmes et leurs services dans l'interface utilisateur du serveur de sécurité. Vous pouvez supprimer les sous-systèmes devenus redondants.
6. Avant que les clients puissent commencer à utiliser les services, assurez-vous que :
 - le nouveau serveur de sécurité est enregistré dans l'instance UXP ;
 - le nouveau serveur de sécurité a choisi au moins un service d'horodatage ;
 - chaque membre dispose d'une clé de signature opérationnelle ;
 - chaque sous-système est enregistré en tant que client sur ce serveur de sécurité de l'instance UXP ;
 - les systèmes d'information qui s'authentifient mutuellement avec le serveur de sécurité disposent du certificat TLS du nouveau serveur de sécurité.

Gestion des différences

Lors de l'importation, il faut décider comment gérer les différences entre les clients présents dans le fichier de configuration du nœud de la grappe et ceux présents sur le serveur de sécurité vers lequel le fichier est importé.

Si des clients sont présents dans le fichier de configuration du nœud de la grappe mais absents du serveur cible, vous avez le choix entre les options suivantes

- Les clients manquants sont ajoutés au serveur de sécurité. Il convient de noter qu'ils doivent ensuite être enregistrés auprès de l'autorité de gouvernance. Consultez le guide d'utilisation du serveur de sécurité UXP [\[UXP-UG-SS\]](#) pour plus de détails sur l'enregistrement.
- Les clients manquants sont ignorés. Cela signifie que les clients manquants et tous leurs services ne sont pas importés sur le serveur de sécurité.
- L'importation est interrompue si un client manquant est détecté. Aucun contenu du fichier de configuration du nœud de la grappe n'est ajouté au serveur de sécurité cible si l'importation est interrompue.

Quel que soit votre choix, les clients manquants seront répertoriés lorsque l'importation sera terminée (sauf si l'importation échoue en raison d'une erreur du système). Si les clients manquants doivent être présents sur le serveur de sécurité cible, vous pouvez les ajouter et les enregistrer. Cette opération peut être effectuée par un utilisateur ayant le rôle d'administrateur serveur dans l'interface utilisateur du serveur de sécurité. Pour plus d'informations, consultez le guide de l'utilisateur du serveur de sécurité UXP [\[UXP-UG-SS\]](#).

Si des clients sont présents sur le serveur cible mais absents du fichier de configuration du nœud de la grappe, vous avez le choix entre les options suivantes

- Les clients redondants sont ignorés. Ces clients et leurs services seront laissés sur le serveur de sécurité.

- L'importation est interrompue si un client redondant est détecté. Aucun contenu du fichier de configuration du nœud de la grappe n'est ajouté au serveur de sécurité cible si l'importation est interrompue.

Dans les deux cas, les clients redondants seront répertoriés lorsque l'importation sera terminée (sauf si l'importation échoue en raison d'une erreur du système). Si les clients redondants doivent être supprimés du serveur de sécurité cible, vous pouvez les désenregistrer et les supprimer. Cette opération peut être effectuée par un utilisateur ayant le rôle d'administrateur serveur dans l'interface utilisateur du serveur de sécurité. Pour plus d'informations, consultez le guide de l'utilisateur du serveur de sécurité UXP [\[UXP-UG-SS\]](#).



Pour les services SOAP, le fichier WSDL n'est pas retéléchargé ni réparé. Pour les API REST ajoutées à partir des descriptions OpenAPI, la description OpenAPI n'est pas actualisée.

Les services SOAP et les API REST sont importés exactement dans l'état où ils se trouvaient lors de la création du fichier de configuration du nœud de la grappe.

Comparer les métadonnées de fichiers

Pour vous assurer que vous utilisez le bon fichier de configuration de nœud de la grappe, vous pouvez utiliser l'utilitaire de métadonnées de configuration du serveur pour vérifier les métadonnées du fichier.

Utilisation :

```
serverconf-metadata <full-path-to-configuration-file>
```

Par exemple, exécutez la commande :

```
sudo su - uxp -c "serverconf-metadata \  
/var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json"
```

Exemple de sortie :

Exported configuration metadata

Generation **date**: 2024-09-13 14:34:23
Security server ID: UXP_EX/COM/MEMBER1/SAMPLESUB
Security server address: uxp-example-ss1 (192.168.113.6)
File version: 1
File **hash** (SHA-512):

55:7B:26:A6:98:64:AA:7E:95:CB:34:3D:5B:34:D9:A5:
CC:EC:27:79:11:65:CF:C3:38:5E:5A:B2:C1:17:32:31:
51:A3:42:CE:44:31:0D:B9:C7:25:B1:F7:16:98:C8:D0:
D0:9F:53:28:5A:BF:E2:B1:7B:A7:84:58:52:48:55:AF

Vous pouvez vérifier cette sortie pour confirmer que le fichier de configuration du nœud de la grappe que vous utilisez est généré à l'heure prévue sur le serveur de sécurité prévu. En

outre, vous pouvez comparer le hachage du fichier de cette sortie au hachage du fichier que vous avez enregistré après avoir exporté la configuration du serveur de sécurité. Si les hachages ne correspondent pas, soit des fichiers différents ont été utilisés, soit le contenu des fichiers a été modifié manuellement à un moment donné.

2.5.3. Ajouter un nœud de serveur de sécurité supplémentaire

Pour ajouter un nœud de serveur de sécurité supplémentaire, procédez comme suit :

1. Installez et configurez un nouveau serveur de sécurité en suivant les instructions de Serveur de sécurité UXP : Guide d'installation et de configuration [\[UXP-IG-SS\]](#). Assurez-vous que le nouveau serveur de sécurité a le même propriétaire de serveur que le(s) nœud(s) existant(s) sur la grappe, mais un code serveur différent.

Chaque nœud doit gérer et utiliser de manière indépendante ses clés et certificats de signature et d'authentification, car ceux-ci ne sont pas transférables entre les nœuds. Ce principe s'applique également aux autres clés et certificats TLS utilisés au sein du serveur de sécurité, tels que le certificat TLS interne.

2. Si Zabbix et/ou Elasticsearch sont configurés pour la grappe de serveurs de sécurité, configurez-les également pour le nouveau nœud en suivant les instructions de Serveur de sécurité UXP : Configuration de la surveillance du serveur de sécurité [\[UXP-UG-PMA\]](#).
3. Exportez le fichier de configuration du nœud de la grappe à partir du nœud de serveur de sécurité existant en suivant les instructions de la section [Services d'exportation et droits d'accès](#).
4. Importez le fichier de configuration du nœud de la grappe vers le nouveau nœud en suivant les instructions de la section [Services d'importation et droits d'accès](#).
5. Assurez-vous que les systèmes d'information qui s'authentifient mutuellement avec le serveur de sécurité disposent du certificat TLS interne du nouveau serveur de sécurité. Pour exporter le certificat TLS interne, suivez les instructions de Serveur de sécurité UXP : Guide de l'utilisateur [\[UXP-UG-SS\]](#).
6. Configurez pour chaque membre importé une clé de signature et un certificat en suivant les instructions de Serveur de sécurité UXP : Guide de l'utilisateur [\[UXP-UG-SS\]](#).
7. Enregistrez chaque sous-système importé en tant que client sur ce serveur de sécurité de l'instance UXP en suivant les instructions de Serveur de sécurité UXP : Guide de l'utilisateur [\[UXP-UG-SS\]](#).
8. Si des équilibres de charge sont utilisés, mettez à jour leur configuration si nécessaire.

2.5.4. Supprimer un nœud de serveur de sécurité de la grappe

Pour supprimer un nœud de serveur de sécurité de la grappe, procédez comme suit.

1. Si le serveur de sécurité est déjà enregistré auprès de l'autorité de gouvernance (AG) de l'UXP, notifiez l'AG de sa suppression conformément aux procédures organisationnelles de votre instance UXP (par exemple, par courrier électronique ou via le portail de support). Incluez le code du serveur dans votre demande de suppression.

Une fois que l'AG a appliqué les modifications, le serveur de sécurité est supprimé de la configuration globale.

2. Supprimez le ou les certificats TLS internes du serveur de sécurité des systèmes d'information (client/serveur) connectés au serveur de sécurité afin de les nettoyer, s'ils sont configurés.
3. Supprimez l'adresse du nœud de l'équilibreur de charge s'il est configuré.

2.5.5. Modifier l'adresse IP ou le nom DNS d'un nœud de serveur de sécurité

Pour modifier l'adresse IP ou le nom DNS d'un nœud de serveur de sécurité, procédez comme suit.

1. Effectuez les étapes décrites dans la section Changer l'adresse IP ou le nom DNS du serveur de sécurité UXP : Guide de l'utilisateur [\[UXP-UG-SS\]](#).
2. Si un ou plusieurs équilibreurs de charge sont utilisés, mettez leur configuration à jour si nécessaire.

3. Équilibreurs de charge

Pour améliorer encore les performances, il faut utiliser un équilibreur de charge (LB) tiers.

Il existe deux scénarios de répartition de charge pris en charge, accompagnés d'instructions pour leur configuration :

- Équilibrage de charge interne—Équilibreur de charge entre le système d'information du client du service et la grappe de serveurs de sécurité du client du service (voir section [Équilibrage de charge interne](#)) ;
- Équilibrage de charge de service—Équilibreur de charge entre le serveur de sécurité du fournisseur et la grappe du système d'information du fournisseur de services (voir section [Équilibrage de charge des services](#)).

Les équilibreurs de charge dans d'autres scénarios ne sont pas officiellement pris en charge.

Certains LB (par exemple, [HAProxy \[HAProxy\]](#)) sont capables d'intégrer directement le [service d'information sur l'état](#) et peuvent supprimer eux-mêmes les nœuds non fonctionnels de votre grappe. Si vous utilisez un tel LB pour l'équilibrage de charge interne, il est recommandé de désactiver la [fonction proxyOff](#) (elle est désactivée par défaut).

Cependant, si votre LB interne ne peut pas intégrer le service d'information sur l'état (par exemple, [Apache \[Apache\]](#) ou [Nginx \[Nginx\]](#)), il est recommandé d'activer la fonctionnalité proxyOff.

ProxyOff cesse d'accepter les connexions aux ports d'écoute des serveurs de sécurité ayant le statut `DOWN`. Cela permet d'éviter que les messages soient envoyés aux nœuds de la grappe qui ne sont pas en mesure de traiter ceux-ci.

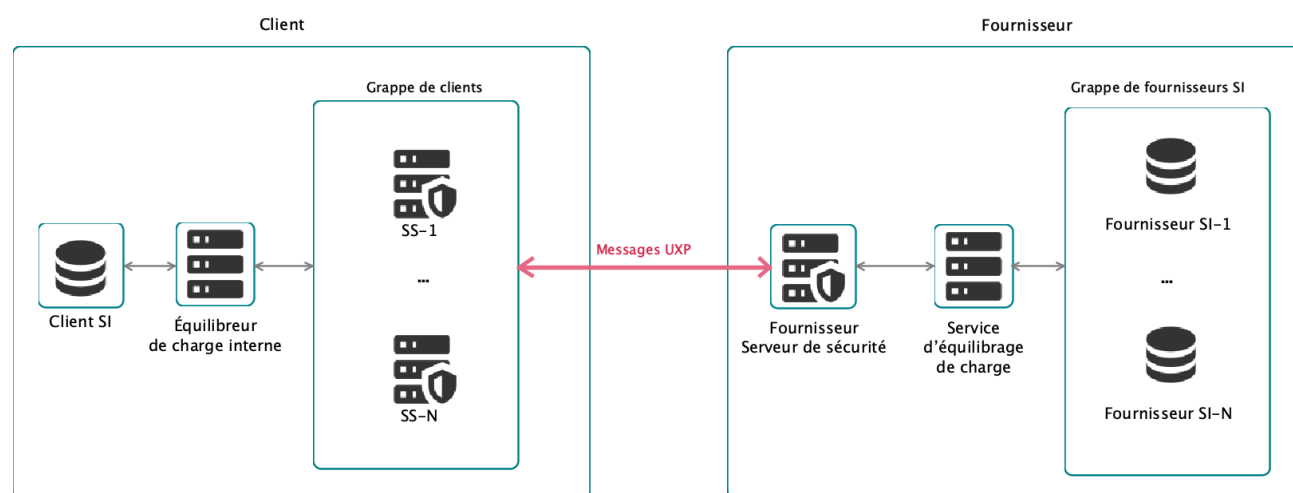


Figure 2. Exemple de configuration UXP avec un équilibreur de charge interne et un équilibreur de charge de service

3.1. Équilibreur de charge interne

Un équilibreur de charge **interne** peut être mis en place entre le système d'information du client du service et la grappe de serveurs de sécurité du client du service.

3.1.1. Exemple HAProxy

Il s'agit d'un exemple spécifique de configuration et d'utilisation de l'équilibreur de charge [HAProxy](#) [HAProxy]. Si les détails peuvent être différents pour d'autres équilibreurs de charge, l'approche principale devrait être similaire.

Pour configurer HAProxy en tant que LB interne, procédez comme suit :

1. Une grappe de serveurs de sécurité jouant le rôle de client du service, avec des nœuds SS-1, ..., SS-N.
 - a. Assurez-vous que chaque nœud peut agir en tant que client d'un service UXP en ajoutant un client sur chaque nœud et en enregistrant un certificat de signature pour le client.
2. Installez HAProxy sur un autre serveur :

```
sudo apt update
sudo apt install haproxy haproxyctl
```

3. Autorisez le serveur HAProxy à demander des informations sur l'état du serveur de sécurité :
 - a. Sur chaque nœud de la grappe de serveurs de sécurité :
 - i. ajoutez le serveur HAProxy au champ des hôtes autorisés (allowed-hosts) dans la section du fichier [status-service] du fichier /etc/uxp/conf.d/local.ini :

```
[status-service]

; The comma-separated list of host IP-addresses and/or CIDR notations that
; determine allowed addresses to request status information.
allowed-hosts=<HAProxy-server-IP>
```

- ii. si ce n'est pas déjà fait, configurez le service d'information sur l'état du serveur de sécurité, voir les instructions dans la section [Configuration de l'information sur l'état](#).
 - iii. Redémarrez le service de surveillance sur le serveur de sécurité :

```
sudo systemctl restart uxp-monitor
```

4. Sur le serveur HAProxy, ajoutez les serveurs de sécurité UXP au fichier de configuration HAProxy /etc/haproxy/haproxy.cfg :

```
listen inside-service
    bind *:80
    option httpchk GET /status
    http-check expect rstatus 200
    default-server inter 15s check port 2082
    server SS-1 <security-server-1-ip>:80
    server SS-2 <security-server-2-ip>:80
    retries 1
    option redispatch
    balance roundrobin
```

Cet exemple configure HAProxy pour qu'il écoute le port HTTP 80 et équilibre la charge des demandes entrantes entre deux serveurs de sécurité SS-1 (déployé sur <security-server-1-ip>) et SS-2 (déployé sur <security-server-2-ip>), qui écoutent tous deux les demandes sur le port HTTP 80 du serveur de sécurité du client du service par défaut. HAProxy est configuré pour utiliser le service d'état du serveur de sécurité /status sur le port 2082, qu'il interroge toutes les 15 secondes pour vérifier si le serveur de sécurité peut être utilisé (il attend une réponse avec l'état HTTP 200) — si un serveur est hors service, il est retiré de la rotation.

Comme les contrôles de santé sont effectués toutes les 15 secondes, un nœud de serveur de sécurité peut échouer entre les contrôles et rester marqué comme sain pendant un court laps de temps. Pour gérer cette situation, HAProxy est configuré avec des tentatives et l'option `redispatch`, qui lui permet d'essayer de se connecter à un autre nœud si le serveur initial ne répond pas. Le paramètre `retries` détermine le nombre de tentatives de HAProxy sur le même serveur. Lorsque `redispatch` est activé, HAProxy passe automatiquement à un nœud sain si toutes les tentatives échouent. Pour un basculement plus rapide, vous pouvez fixer le nombre de tentatives à 1.

5. Vérifiez la validité du fichier de configuration de HAProxy :

```
sudo haproxyctl configcheck
```

a. La réponse attendue est la suivante :

```
Configuration file is valid
```

6. Chargez le nouveau fichier de configuration :

```
sudo systemctl restart haproxy
```

7. Vérifiez que l'installation a réussi en utilisant le service d'information sur l'état par l'intermédiaire de HAProxy :

```
sudo haproxyctl show health
```

a. La réponse attendue énumère tous les nœuds de la grappe de serveurs de sécurité :

#	pxname	svname	status	weight
	inside-service	FRONTEND	OPEN	
	inside-service	SS-1	UP	1
	...			
	inside-service	SS-N	UP	1
	inside-service	BACKEND	UP	2

b. Notez que dans cet exemple, le poids de tous les serveurs de sécurité est égal.

Après cette mise en place, le LB transmet chaque demande du système d'information du client du service à l'un des nœuds de la grappe avec une réponse positive d'information sur l'état.

3.2. Équilibreur de charge de service

Un équilibreur de charge de **service** peut être mis en place entre le serveur de sécurité du fournisseur et la grappe du système d'information du fournisseur de services.

Dans cette configuration, il existe plusieurs instances du système d'information du fournisseur de services et un LB est utilisé pour choisir l'instance du système d'information avec laquelle le serveur de sécurité du fournisseur de services communique.

Aucune action particulière ne doit être entreprise sur le serveur de sécurité pour utiliser un LB de service.

4. Dépannage

4.1. L'importation du fichier de configuration a échoué : <path-to-configuration-file>

Exemple d'erreur :

```
Import configuration file failed: /var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json
```

Si vous obtenez le message d'erreur « import configuration file failed » lorsque vous [importez la configuration sur le serveur de sécurité cible](#), assurez-vous que le fichier dispose des privilèges corrects (uxp uxp).

Vérifiez les privilèges actuels du fichier de configuration :

```
ls -l /var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json
```

Vous verrez peut-être que le fichier appartient à l'utilisateur que vous avez utilisé pour déplacer le fichier d'un serveur à l'autre (john) :

```
-rw-r----- 1 john john 52831 Jan 14 14:01 uxp-serverconf-securityserver1-20240913-143423-2.json
```

Modifiez la propriété du fichier en uxp :

```
sudo chown uxp:uxp /var/tmp/uxp-serverconf-securityserver1-20240913-143423-2.json
```

Réessayez d'importer la configuration sur le serveur cible.

4.2. Échec de la connexion à <adresse IP> port <port> après 0 ms : Connexion refusée

Exemple d'erreur :

```
Failed to connect to 192.168.12.34 port 2082 after 0 ms: Connection refused
```

Lorsqu'une demande externe des informations sur l'état adressée au point de terminaison du serveur de sécurité aboutit à `Connection refused`, assurez-vous que vous avez remplacé la valeur par défaut de `listen-address` par l'adresse IP du serveur de sécurité ou par une adresse IP de remplacement (0.0.0.0 pour IPv4 / [:::] pour IPv6). La valeur par défaut 127.0.0.1 n'autorise que les demandes d'état provenant du même serveur.

1. Dans le fichier `/etc/uxp/conf.d/local.ini`, définissez `listen-address` comme étant l'adresse IP du serveur de sécurité.

```
[status-service]  
  
; The status service listen address.  
listen-address=<security-server-IP>
```

2. Redémarrez le service de surveillance sur le serveur de sécurité :

```
sudo systemctl restart uxp-monitor
```

3. Réessayez la demande à partir d'un serveur externe (l'IP du serveur externe doit être répertoriée dans `allowed-hosts` dans le fichier `local.ini`).