Proxy de services Web

E-Series Systems

NetApp
March 06, 2023

Table des matières

Proxy de services Web

Présentation du proxy de services Web SANtricity

SANtricity Web Services Proxy est un serveur API RESTful installé séparément sur un système hôte afin de gérer des centaines de systèmes de stockage NetApp E-Series existants et nouveaux. Le proxy inclut SANtricity Unified Manager, une interface web qui fournit des fonctions similaires.

Présentation de l'installation

L'installation et la configuration du proxy de services Web implique les étapes suivantes :

1. "Examinez les conditions d'installation et de mise à niveau".
2. "Téléchargez et installez le fichier Web Services Proxy".
3. "Connectez-vous aux API et à Unified Manager".
4. "Configurer le proxy de services Web".

Trouvez plus d'informations

- Unified Manager — l'installation proxy inclut SANtricity Unified Manager, une interface web qui permet d'accéder à une configuration plus récente des systèmes de stockage E-Series et EF-Series. Pour plus d'informations, consultez l'aide en ligne de Unified Manager, disponible depuis son interface utilisateur ou depuis "Documentation sur le logiciel SANtricity".
- Référentiel GitHub : le stockage GitHub contient un référentiel pour la collecte et l'organisation d'exemples de scripts illustrant l'utilisation de l'API des services Web NetApp SANtricity. Pour accéder au référentiel, voir "Exemples de services Web NetApp".
- Representational State Transfer (REST) — les services Web sont une API RESTful qui permet d'accéder à quasiment toutes les fonctionnalités de gestion de SANtricity. Il est donc préférable de vous familiariser avec les concepts REST. Pour plus d'informations, voir "Styles architecturaux et conception d'architectures logicielles réseau".
- JavaScript Object notation (JSON) — parce que les données des services Web sont codées via JSON, vous devez être familier des concepts de programmation JSON. Pour plus d'informations, voir "Présentation de JSON".

En savoir plus sur Web Services

Présentation des services Web et de Unified Manager

Avant d'installer et de configurer le proxy de services Web, lisez la présentation des services Web et de SANtricity Unified Manager.

Services Web

Web Services est une API (application Programming interface) qui vous permet de configurer, de gérer et de surveiller les systèmes de stockage NetApp E-Series et EF-Series. En émettant des requêtes API, vous pouvez compléter des workflows, tels que la configuration, le provisionnement et la surveillance des

performances des systèmes de stockage E-Series.

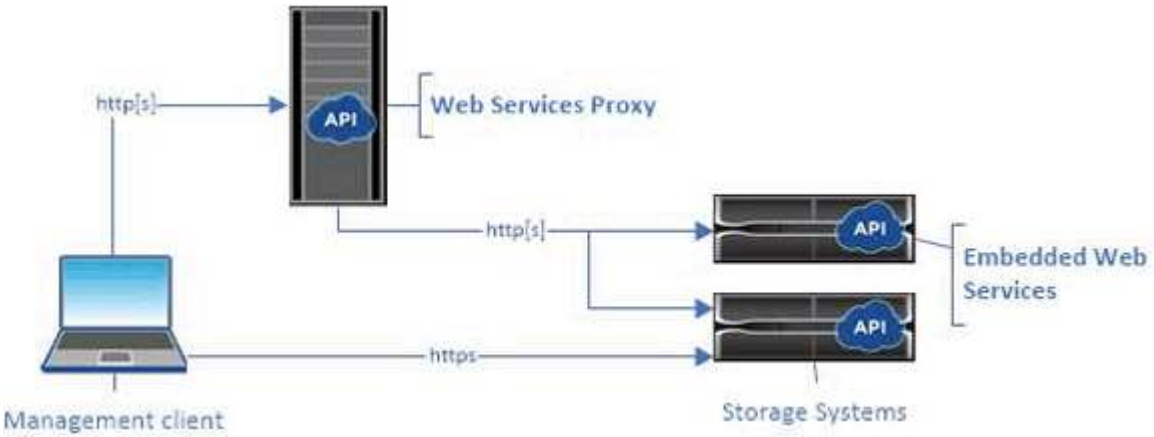
Lorsque vous utilisez l'API Web Services pour gérer les systèmes de stockage, vous devez connaître les éléments suivants :

- JavaScript Object notation (JSON) : les données des services Web étant codées via JSON, vous devez être familier des concepts de programmation JSON. Pour plus d'informations, voir "Présentation de JSON".
- Representational State Transfer (REST) : les services Web sont une API RESTful qui permet d'accéder à quasiment toutes les fonctionnalités de gestion de SANtricity. Il est donc préférable de vous familiariser avec les concepts REST. Pour plus d'informations, voir "Styles architecturaux et conception d'architectures logicielles réseau".
- Concepts de langage de programmation – Java et Python sont les langages de programmation les plus courants utilisés avec l'API des services Web, mais tout langage de programmation pouvant faire des requêtes HTTP est suffisant pour l'interaction API.

Les services Web sont disponibles dans deux implémentations :

- **Embedded** — Un serveur API RESTful est intégré sur chaque contrôleur d'un système de stockage E2800/EF280 exécutant NetApp SANtricity 11.30 ou version ultérieure, un système E5700/EF570 exécutant SANtricity 11.40 ou version ultérieure et un système EF300 ou EF600 exécutant SANtricity 11.60 ou version ultérieure. Aucune installation n'est requise.
- **Proxy** — le proxy de services Web SANtricity est un serveur API RESTful installé séparément sur un serveur Windows ou Linux. Cette application basée sur l'hôte peut gérer des centaines de systèmes de stockage NetApp E-Series existants ou nouveaux. En général, vous devez utiliser le proxy pour les réseaux comptant plus de 10 systèmes de stockage. Le proxy peut traiter de nombreuses demandes plus efficacement que l'API intégrée.

Le cœur de l'API est disponible dans les deux implémentations.



Le tableau suivant fournit une comparaison entre le proxy et la version incorporée.

Réflexion	Proxy	Intégré
Installation	Requiert un système hôte (Linux ou Windows). Le proxy est disponible en téléchargement sur le "Site de support NetApp" ou sur "DockerHub".	Aucune installation ni activation requises.

Réflexion	Proxy	Intégré
Sécurité	Paramètres de sécurité minimaux par défaut. Les paramètres de sécurité sont faibles pour permettre aux développeurs de commencer à utiliser l'API rapidement et facilement. Si vous le souhaitez, vous pouvez configurer le proxy avec le même profil de sécurité que la version intégrée.	Paramètres de sécurité élevés par défaut. Les paramètres de sécurité sont élevés car l'API s'exécute directement sur les contrôleurs. Par exemple, il n'autorise pas l'accès HTTP et désactive tous les protocoles de cryptage SSL et TLS plus anciens pour HTTPS.
Gestion centrale	Gestion de tous les systèmes de stockage à partir d'un seul serveur.	Gère uniquement le contrôleur sur lequel il est intégré.

Unified Manager

Le pack d'installation proxy comprend une interface web Unified Manager qui permet d'accéder à la configuration des systèmes de stockage E-Series et EF-Series plus récents, notamment les systèmes E2800, E5700, EF300 et EF600.

À partir d'Unified Manager, vous pouvez effectuer les opérations de traitement par lots suivantes :

- Afficher l'état de plusieurs systèmes de stockage depuis une vue centralisée
- Découvrir les nombreux systèmes de stockage de votre réseau
- Importer les paramètres d'un système de stockage vers plusieurs systèmes
- Mise à niveau du firmware pour plusieurs systèmes de stockage

Compatibilité et restrictions

La compatibilité et les restrictions suivantes s'appliquent à l'utilisation du proxy de services Web.

Réflexion	Compatibilité ou restriction
Prise en charge HTTP	Le proxy de services Web permet l'utilisation de HTTP ou HTTPS. (La version intégrée des services Web nécessite HTTPS pour des raisons de sécurité.)
Firmwares et systèmes de stockage	Le proxy de services Web peut gérer tous les systèmes de stockage E-Series, notamment des systèmes plus anciens et les tout derniers modèles E2800, EF280, E5700, EF570, EF300, Et les systèmes EF600.

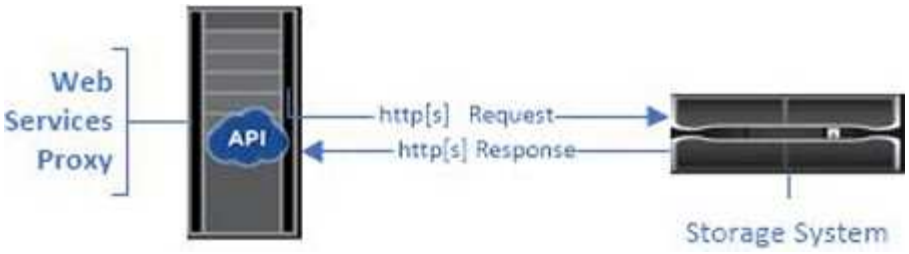
Réflexion	Compatibilité ou restriction
Prise en charge IP	Le proxy de services Web prend en charge le protocole IPv4 ou IPv6. Le protocole IPv6 peut échouer lorsque le proxy de services Web tente de détecter automatiquement l'adresse de gestion à partir de la configuration du contrôleur. Les causes possibles de cette défaillance incluent les problèmes lors du transfert d'adresse IP ou de l'activation d'IPv6 sur les systèmes de stockage, mais pas sur le serveur.
Contraintes de nom de fichier NVSRAM	Le proxy de services Web utilise les noms de fichiers NVSRAM pour identifier précisément les informations de version. Par conséquent, vous ne pouvez pas modifier les noms de fichier NVSRAM lorsqu'ils sont utilisés avec le proxy de services Web. Il se peut que le proxy des services Web ne reconnaisse pas un fichier NVSRAM renommé comme un fichier de micrologiciel valide.
Symbol Web	Symbol Web est une URL dans l'API REST. Il permet d'accéder à presque tous les appels de symboles. La fonction de symbole fait partie de l'URL suivante : `http://host:port/devmgr/storage-system/storage array ID/symbol/symbol function` Les systèmes de stockage désactivés par Symbol sont pris en charge via Web Services Proxy.

Notions de base sur les API

Dans l'API des services Web, les communications HTTP impliquent un cycle de réponse aux demandes.

Éléments URL dans les demandes

Quel que soit le langage de programmation ou l'outil utilisé, chaque appel à l'API des services Web a une structure similaire, avec une URL, un verbe HTTP et un en-tête accepter.



Toutes les demandes incluent une URL, comme dans l'exemple suivant, et contiennent les éléments décrits dans le tableau.

```
https://webservices.name.com:8443/devmgr/v2/storage-systems
```

De service	Description
Transport HTTP `https://`	Le proxy de services Web permet l'utilisation de HTTP ou HTTPS. Pour des raisons de sécurité, les services Web intégrés nécessitent HTTPS.
URL et port de base `webservices.name.com:8443`	Chaque demande doit être correctement acheminée vers une instance active de Web Services. Le FQDN (nom de domaine complet) ou l'adresse IP de l'instance est requis, avec le port d'écoute. Par défaut, les services Web communiquent via le port 8080 (pour HTTP) et le port 8443 (pour HTTPS). Pour le proxy de services Web, les deux ports peuvent être modifiés pendant l'installation du proxy ou dans le fichier wsconfig.xml. Les conflits de ports sont courants sur les hôtes du data Center qui exécutent diverses applications de gestion. Pour les services Web intégrés, le port du contrôleur ne peut pas être modifié ; il est défini par défaut sur le port 8443 pour les connexions sécurisées.

De service	Description
Chemin d'API `devmgr/v2/storage-systems`	Une demande est faite à une ressource REST ou à un noeud final spécifique dans l'API de services Web. La plupart des terminaux se présentent sous forme : `devmgr/v2/<resource>/[id]` Le chemin d'accès à l'API se compose de trois parties : • `devmgr` (Device Manager) est l'espace de noms de l'API Web Services. • `v2` Indique la version de l'API à laquelle vous accédez. Vous pouvez également utiliser `utils` pour accéder aux terminaux de connexion. • `storage-systems` est une catégorie dans la documentation.

Verbes HTTP pris en charge

Les verbes HTTP pris en charge comprennent OBTENIR, PUBLIER et SUPPRIMER :

- Les demandes GET sont utilisées pour les demandes en lecture seule.
- Les demandes POST sont utilisées pour créer et mettre à jour des objets, ainsi que pour les demandes de lecture qui peuvent avoir des implications sur la sécurité.
- Les demandes DE SUPPRESSION sont généralement utilisées pour supprimer un objet de la gestion, pour supprimer entièrement un objet ou pour réinitialiser l'état de cet objet.

> Actuellement, l'API des services Web ne prend pas en charge LES CORRECTIFS PUT ou PATCH. Au lieu de cela, vous pouvez utiliser POST pour fournir les fonctionnalités typiques de ces verbes.

Accepter les en-têtes

Lors du renvoi d'un corps de demande, Web Services renvoie les données au format JSON (sauf indication contraire). Certains clients ne font pas défaut à demander « texte/html » ou quelque chose de similaire. Dans ce cas, l'API répond par un code HTTP 406, indiquant qu'elle ne peut pas fournir de données dans ce format. Il est recommandé de définir l'en-tête Accept comme « application/json » dans tous les cas où vous vous attendez à ce que JSON soit le type de réponse. Dans d'autres cas où un corps de réponse n'est pas retourné (PAR exemple, SUPPRIMER), à condition que l'en-tête accepter ne cause aucun effet involontaire.

Réponses

Lorsqu'une demande est adressée à l'API, une réponse renvoie deux informations essentielles :

- Code d'état HTTP — indique si la demande a réussi.
- Corps de réponse facultatif — fournit généralement un corps JSON représentant l'état de la ressource ou d'un corps fournissant plus de détails sur la nature d'une défaillance.

Vous devez vérifier le code d'état et l'en-tête de type contenu pour déterminer à quoi ressemble le corps de réponse obtenu. Pour les codes d'état HTTP 200-203 et 422, Web Services renvoie un corps JSON avec la réponse. Pour les autres codes d'état HTTP, les services Web ne renvoient généralement pas un corps JSON supplémentaire, soit parce que la spécification ne l'autorise pas (204), soit parce que l'état est explicite. Le tableau répertorie les codes d'état et les définitions HTTP les plus courants. Elle indique également si les informations associées à chaque code HTTP sont renvoyées dans un corps JSON.

Code d'état HTTP	Description	Corps JSON
200 OK	Indique une réponse réussie.	Oui.
201 créé	Indique qu'un objet a été créé. Ce code est utilisé dans quelques rares cas au lieu d'un état 200.	Oui.
202 accepté	Indique que la demande est acceptée pour le traitement en tant que demande asynchrone, mais vous devez faire une demande ultérieure pour obtenir le résultat réel.	Oui.
203 renseignements non officiels	Similaire à une réponse 200, mais les services Web ne peuvent pas garantir que les données sont à jour (par exemple, seules les données mises en cache sont disponibles pour le moment).	Oui.
204 aucun contenu	Indique une opération réussie, mais il n'y a pas de corps de réponse.	Non
400 demande erronée	Indique que le corps JSON fourni dans la demande n'est pas valide.	Non
401 non autorisé	Indique qu'une erreur d'authentification s'est produite. Aucune information d'identification n'a été fournie ou le nom d'utilisateur ou le mot de passe n'était pas valide.	Non
403 interdit	Échec de l'autorisation, qui indique que l'utilisateur authentifié n'est pas autorisé à accéder au noeud final demandé.	Non

Code d'état HTTP	Description	Corps JSON
404 introuvable	Indique que la ressource demandée n'a pas pu être localisée. Ce code est valide pour les API inexistantes ou les ressources non existantes demandées par l'identificateur.	Non
422 entité impossible à traiter	Indique que la demande est généralement bien formée, mais que les paramètres d'entrée ne sont pas valides ou que l'état du système de stockage ne permet pas aux services Web de satisfaire la demande.	Oui.
424 échec de la dépendance	Utilisé dans le proxy de services Web pour indiquer que le système de stockage demandé est actuellement inaccessible. Par conséquent, les services Web ne peuvent pas satisfaire la demande.	Non
429 trop de demandes	Indique qu'une limite de demande a été dépassée et qu'elle doit être relancée ultérieurement.	Non

Exemples de scripts

GitHub contient un référentiel pour la collecte et l'organisation d'exemples de scripts illustrant l'utilisation de l'API des services Web NetApp SANtricity. Pour accéder au référentiel, voir "Exemples de services Web NetApp".

Termes et concepts

Les termes suivants s'appliquent au proxy de services Web.

Durée	Définition
API	Une interface de programmation d'applications (API) est un ensemble de protocoles et de méthodes qui permet aux développeurs de communiquer avec les périphériques. L'API de services Web permet de communiquer avec les systèmes de stockage E-Series.

Durée	Définition
ASUP	La fonctionnalité AutoSupport (ASUP) collecte les données dans un bundle de support client et envoie automatiquement le fichier des messages au support technique pour le dépannage et l'analyse des problèmes à distance.
Point final	Les terminaux sont des fonctions disponibles via l'API. Un noeud final inclut un verbe HTTP, plus le chemin URI. Dans les services Web, les terminaux peuvent exécuter des tâches telles que la découverte des systèmes de stockage et la création de volumes.
Verb. HTTP	Un verbe HTTP est une action correspondante pour un noeud final, comme la récupération et la création de données. Dans les services Web, les verbes HTTP incluent POST, GET et DELETE.
JSON	JavaScript Object notation (JSON) est un format de données structuré semblable à XML, qui utilise un format lisible minimal. Les données contenues dans les services Web sont codées au moyen d'un fichier JSON.
REST/RESTful	Representational State Transfer (REST) est une spécification non standard qui définit un style architectural pour une API. La plupart des API REST n'étant pas entièrement conformes aux spécifications, elles sont décrites comme « C'est-à-dire « C'est » ou « c'est-à-dire ». En règle générale, une API « RETESTABLE » est indépendante des langages de programmation et présente les caractéristiques suivantes : • Basé sur HTTP, qui suit la sémantique générale du protocole • Producteur et consommateur de données structurées (JSON, XML, etc.) • Orienté objet (par opposition à une opération orientée) Web Services est une API RESTful qui permet d'accéder à quasiment toutes les fonctions de gestion de SANtricity.
adieu les migrations de données onéreuses	Un système de stockage est une baie E-Series qui comprend des tiroirs, des contrôleurs, des disques, des logiciels, et des firmwares.

Durée	Définition
API de symbole	Symbol est une API héritée destinée à gérer les systèmes de stockage E-Series. L'implémentation sous-jacente de l'API Web Services utilise le symbole.
Services Web	Web Services est une API NetApp conçue pour les développeurs de gérer les systèmes de stockage E-Series. Il existe deux implémentations de services Web : intégrées sur le contrôleur et un proxy distinct qui peut être installé sur Linux ou Windows.

Installation et configuration

Examinez les conditions d'installation et de mise à niveau

Avant d'installer Web Services Proxy, vérifiez les conditions requises pour l'installation et la mise à niveau.

Conditions requises pour l'installation

Vous pouvez installer et configurer le proxy de services Web sur un système hôte Windows ou Linux.

L'installation du proxy comprend les conditions suivantes.

Conditions requises	Description
Limites du nom d'hôte	Assurez-vous que le nom d'hôte du serveur où vous avez l'intention d'installer le proxy de services Web contient uniquement des lettres ASCII, des chiffres numériques et des tirets (-). Cette exigence est due à une limitation de Java Keytool, qui est utilisée pour générer un certificat auto-signé pour le serveur. Si le nom d'hôte de votre serveur contient d'autres caractères, tels qu'un trait de soulignement (_), le serveur Web ne démarrera pas après l'installation.
Systèmes d'exploitation	Vous pouvez installer le proxy sur les systèmes d'exploitation suivants : • Linux • Répertoires de base Pour obtenir la liste complète des systèmes d'exploitation et de la compatibilité du micrologiciel, reportez-vous au "Matrice d'interopérabilité NetApp".

Conditions requises	Description
Linux : autres considérations	Les bibliothèques Linux Standard base (fonctions init) sont requises pour que le Webserver fonctionne correctement. Vous devez installer les packages lsb/insserv pour votre système d'exploitation. Pour plus d'informations, reportez-vous à la section « modules supplémentaires requis » du fichier Readme.
Instances multiples	Vous ne pouvez installer qu'une seule instance de proxy de services Web sur un serveur, mais vous pouvez installer ce proxy sur plusieurs serveurs de votre réseau.
La planification de la capacité	Web Services Proxy requiert un espace suffisant pour la connexion. Assurez-vous que votre système répond aux exigences suivantes en matière d'espace disque : • Espace d'installation requis — 275 Mo • Espace d'enregistrement minimum — 200 Mo • Mémoire système — 2 Go ; l'espace de tas est de 1 Go par défaut Vous pouvez utiliser un outil de surveillance de l'espace disque pour vérifier l'espace disque disponible pour le stockage permanent et la journalisation.
Licence	Le proxy de services Web est un produit autonome gratuit qui ne nécessite pas de clé de licence. Toutefois, les droits d'auteur et les conditions de service applicables s'appliquent. Si vous installez le proxy en mode graphique ou Console, vous devez accepter le contrat de licence utilisateur final (CLUF).

Mise à niveau

Si vous effectuez une mise à niveau à partir d'une version précédente, sachez que certains éléments sont conservés ou supprimés.

- Pour le proxy de services Web, les paramètres de configuration précédents sont conservés. Ces paramètres incluent les mots de passe utilisateur, tous les systèmes de stockage découverts, les certificats de serveur, les certificats approuvés et la configuration d'exécution du serveur.
- Pour Unified Manager, tous les fichiers SANtricity OS précédemment chargés dans le référentiel sont supprimés lors de la mise à niveau.

Installez ou mettez à niveau le fichier Web Services Proxy

L'installation implique le téléchargement du fichier, puis l'installation du package proxy sur

un serveur Linux ou Windows. Vous pouvez également mettre à niveau le proxy à l'aide de ces instructions.

Téléchargez les fichiers proxy de services Web

Vous pouvez télécharger le fichier d'installation et le fichier readme depuis la page de téléchargement des logiciels du site de support NetApp.

Le package de téléchargement inclut le proxy de services Web et l'interface Unified Manager.

Étapes

1. Accédez à "Support NetApp - Téléchargements".
2. Sélectionnez **E-Series SANtricity Web Services Proxy**.
3. Suivez les instructions pour télécharger le fichier. Assurez-vous de sélectionner le progiciel de téléchargement approprié pour votre serveur (par exemple, EXE pour Windows ; BIN ou RPM pour Linux).
4. Téléchargez le fichier d'installation sur le serveur où vous souhaitez installer le proxy et Unified Manager.

Installez sous Windows ou Linux Server

Vous pouvez installer Web Services Proxy et Unified Manager à l'aide de l'un des trois modes (graphique, Console ou silencieux) ou en utilisant un fichier RPM (Linux uniquement).

Avant de commencer

- "Vérifiez les conditions requises pour l'installation".
- Assurez-vous d'avoir téléchargé le fichier d'installation correct (EXE pour Windows ; BIN pour Linux) sur le serveur sur lequel vous souhaitez installer le proxy et Unified Manager.

Installation du mode graphique

Vous pouvez exécuter l'installation en mode graphique pour Windows ou Linux. En mode graphique, les invites s'affichent dans une interface de type Windows.

Étapes

1. Accédez au dossier dans lequel vous avez téléchargé le fichier d'installation.
2. Lancez l'installation pour Windows ou Linux, comme suit :
   - Windows — Double-cliquez sur le fichier d'installation :

     `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`

   - Linux — exécutez la commande suivante : `santricity_webservices-linux_x64-nn.nn.nn.nnnn.bin`

     Dans les noms de fichier ci-dessus, `nn.nn.nn.nnnn` représente le numéro de version.

   Le processus d'installation démarre et l'écran de démarrage de NetApp SANtricity Web Services Proxy + Unified Manager s'affiche.
3. Suivez les invites à l'écran.

   Au cours de l'installation, vous êtes invité à activer plusieurs fonctionnalités et à saisir certains paramètres

de configuration. Si nécessaire, vous pouvez modifier l'une de ces sélections ultérieurement dans les fichiers de configuration.

> Lors d'une mise à niveau, vous n'êtes pas invité à entrer les paramètres de configuration.

4. Lorsque le message serveur Web démarré apparaît, cliquez sur **OK** pour terminer l'installation.

   La boîte de dialogue installation terminée s'affiche.

5. Cochez les cases si vous souhaitez lancer Unified Manager ou la documentation interactive de l'API, puis cliquez sur **Done**.

Installation du mode console

Vous pouvez exécuter l'installation en mode Console pour Windows ou Linux. En mode Console, les invites s'affichent dans la fenêtre du terminal.

Étapes

1. Exécutez la commande suivante : `<install filename> -i console`

   Dans la commande ci-dessus, `<install filename>` représente le nom du fichier d'installation du proxy que vous avez téléchargé (par exemple : `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

   > Pour annuler l'installation à tout moment pendant le processus d'installation, tapez `QUIT` à l'invite de commande.

   Le processus d'installation démarre et le message lancer le programme d'installation — Introduction s'affiche.

2. Suivez les invites à l'écran.

   Au cours de l'installation, vous êtes invité à activer plusieurs fonctionnalités et à saisir certains paramètres de configuration. Si nécessaire, vous pouvez modifier l'une de ces sélections ultérieurement dans les fichiers de configuration.

   > Lors d'une mise à niveau, vous n'êtes pas invité à entrer les paramètres de configuration.

3. Une fois l'installation terminée, appuyez sur **entrée** pour quitter le programme d'installation.

Installation du mode silencieux

Vous pouvez exécuter l'installation en mode silencieux pour Windows ou Linux. En mode silencieux, aucun message ou script de retour n'apparaît dans la fenêtre du terminal.

Étapes

1. Exécutez la commande suivante : `<install filename> -i silent`

   Dans la commande ci-dessus, `<install filename>` représente le nom du fichier d'installation du proxy que vous avez téléchargé (par exemple : `santricity_webservices-windows_x64-nn.nn.nn.nnnn.exe`).

2. Appuyez sur **entrée**.

   La procédure d'installation peut prendre plusieurs minutes. Une fois l'installation terminée, une invite de commande s'affiche dans la fenêtre du terminal.

Installation de la commande RPM (Linux uniquement)

Pour les systèmes Linux compatibles avec le système de gestion des packages RPM, vous pouvez installer Web Services Proxy à l'aide d'un fichier RPM facultatif.

Étapes

1. Téléchargez le fichier RPM sur le serveur où vous souhaitez installer le proxy et Unified Manager.
2. Ouvrez une fenêtre de terminal.
3. Saisissez la commande suivante :

   ```
   rpm -u santricity_webservices-nn.nn.nn.nnnn-n.x86_64.rpm
   ```

   Dans la commande ci-dessus, `nn.nn.nn.nnnn` représente le numéro de version.

   La procédure d'installation peut prendre plusieurs minutes. Une fois l'installation terminée, une invite de commande s'affiche dans la fenêtre du terminal.

Connectez-vous aux API et à Unified Manager

Web Services inclut une documentation API qui vous permet d'interagir directement avec l'API REST. Elle comprend également Unified Manager, une interface web pour gérer plusieurs baies de stockage E-Series.

Connectez-vous à l'API des services Web

Après avoir installé le proxy de services Web, vous pouvez accéder à la documentation interactive de l'API dans un navigateur.

La documentation relative aux API est exécutée avec chaque instance des services Web. Elle est également disponible au format PDF statique depuis le site de support NetApp. Pour accéder à la version interactive, ouvrez un navigateur et entrez l'URL pointant vers l'emplacement où réside les services Web (contrôleur de la version intégrée ou serveur du proxy).

L'API Web Services implémente la spécification OpenAPI (appelée à l'origine la spécification swagger).

Pour la connexion initiale, utilisez les identifiants « admin ». « Admin » est considéré comme un super administrateur avec accès à toutes les fonctions et tous les rôles.

Étapes

1. Ouvrez un navigateur.
2. Saisissez l'URL de l'implémentation incorporée ou du proxy :

   - Embarqué : `https://<controller>:<port>/devmgr/docs/`

Dans cette URL, `<controller>` Est l'adresse IP ou le FQDN du contrôleur, et `<port>` est le numéro du port de gestion du contrôleur (par défaut, 8443).

- Proxy : `http[s]://<server>:<port>/devmgr/docs/`

  Dans cette URL, `<server>` Est l'adresse IP ou le FQDN du serveur où le proxy est installé, et `<port>` Est le numéro du port d'écoute (par défaut : 8080 pour HTTP ou 8443 pour HTTPS).

  > Si le port d'écoute est déjà utilisé, le proxy détecte le conflit et vous invite à choisir un autre port d'écoute.

La documentation API s'ouvre dans le navigateur.

3. Lorsque la documentation interactive de l'API s'ouvre, accédez au menu déroulant en haut à droite de la page et sélectionnez **utils**.
4. Cliquez sur la catégorie **connexion** pour afficher les noeuds finaux disponibles.
5. Cliquez sur le noeud final **POST: /Login**, puis sur **essayez-le**.
6. Pour la première connexion, entrez admin pour le nom d'utilisateur et le mot de passe.
7. Cliquez sur **Exécuter**.
8. Pour accéder aux noeuds finaux pour la gestion du stockage, allez dans le menu déroulant en haut à droite et sélectionnez **v2**.

   Les catégories de haut niveau pour les terminaux sont affichées. Vous pouvez naviguer dans la documentation de l'API comme décrit dans le tableau.

De service	Description
Menu déroulant	Dans le coin supérieur droit de la page, un menu déroulant propose des options permettant de basculer entre la version 2 de la documentation API (V2), l'interface de symboles (symbole V2) et les utilitaires API (utilitaires) pour la connexion. La version 1 de la documentation de l'API étant une version préliminaire et n'étant généralement pas disponible, V1 n'est pas inclus dans le menu déroulant.
Catégories	La documentation API est organisée par catégories générales (par exemple : administration, configuration). Cliquez sur une catégorie pour afficher les noeuds finaux associés.
Terminaux	Sélectionnez un noeud final pour voir ses chemins d'URL, ses paramètres requis, ses corps de réponse et ses codes d'état que les URL sont susceptibles de renvoyer.

De service	Description
Essayez-le	Interagissez directement avec le noeud final en cliquant sur **essayez-le**. Ce bouton est fourni dans chacune des vues développées pour les noeuds finaux. Lorsque vous cliquez sur le bouton, des champs s'affichent pour saisir les paramètres (le cas échéant). Vous pouvez ensuite entrer des valeurs et cliquer sur **Exécuter**. La documentation interactive utilise JavaScript pour faire la demande directement à l'API; ce n'est pas une demande de test.

Connectez-vous à Unified Manager

Après avoir installé Web Services Proxy, vous pouvez accéder à Unified Manager pour gérer plusieurs systèmes de stockage dans une interface Web.

Pour accéder à Unified Manager, vous ouvrez un navigateur et entrez l'URL pointant vers l'emplacement d'installation du proxy. Les navigateurs et versions suivants sont pris en charge.

Navigateur	Version minimale
Google Chrome	79
Microsoft Internet Explorer	11
Microsoft Edge	79
Mozilla Firefox	70
Safari	12

Étapes

1. Ouvrez un navigateur et saisissez l'URL suivante :

   `http[s]://<server>:<port>/um`

   Dans cette URL, `<server>` Représente l'adresse IP ou le FQDN du serveur où le proxy de services Web est installé, et `<port>` Représente le numéro du port d'écoute (par défaut : 8080 pour HTTP ou 8443 pour HTTPS).

   La page de connexion à Unified Manager s'ouvre.

2. Pour la première connexion, entrez `admin` pour le nom d'utilisateur, puis définissez et confirmez un mot de passe pour l'utilisateur admin.

Le mot de passe peut comporter jusqu'à 30 caractères. Pour plus d'informations sur les utilisateurs et les mots de passe, reportez-vous à la section gestion des accès de l'aide en ligne de Unified Manager.

Configurer le proxy de services Web

Vous pouvez modifier les paramètres Web Services Proxy pour répondre aux exigences uniques de fonctionnement et de performances de votre environnement.

Arrêtez ou redémarrez le serveur Web

Le service Webserver est démarré lors de l'installation et s'exécute en arrière-plan. Au cours de certaines tâches de configuration, vous devrez peut-être arrêter ou redémarrer le service Webserver.

Étapes

1. Effectuez l'une des opérations suivantes :

   - Pour Windows, accédez au menu **Démarrer**, sélectionnez **Outils d'administration › Services**, recherchez **Services Web SANtricity** et sélectionnez **Arrêter** ou **redémarrer**.
   - Pour Linux, choisissez la méthode d'arrêt et de redémarrage du serveur Web pour la version de votre système d'exploitation. Au cours de l'installation, une boîte de dialogue contextuelle indique le démarrage du démon. Par exemple :

     ```
     web_services_proxy webserver installed and started. You can interact with it
     using systemctl start|stop|restart|status web_services_proxy.service
     ```

   La méthode la plus courante pour interagir avec le service est d'utiliser `systemctl` commandes.

Résoudre les conflits de ports

Si Web Services Proxy s'exécute alors qu'une autre application est disponible à l'adresse ou au port défini, vous pouvez résoudre le conflit de port dans le fichier wsconfig.xml.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez la ligne suivante au fichier wsconfig.xml, dans lequel *n* est le numéro de port :

   ```
   <sslport clientauth="request">*n*</sslport>
   <port>n</port>
   ```

   Le tableau suivant présente les attributs de contrôle des ports HTTP et HTTPS.

Nom	Description	Nœud parent	Attributs	Obligatoire
gstn de la	Nœud racine de la configuration	Nul	Version - la version du schéma de configuration est actuellement 1.0.	Oui.
sslport	Port TCP pour écouter les requêtes SSL. La valeur par défaut est 8443.	gstn de la	Clientauth	Non
port	Port TCP pour écouter la requête HTTP, valeur par défaut : 8080.	gstn de la	-	Non

3. Enregistrez et fermez le fichier.
4. Redémarrez le service Webserver pour que la modification prenne effet.

Configurez l'équilibrage de charge et/ou la haute disponibilité

Pour utiliser le proxy de services Web dans une configuration haute disponibilité (HA), vous pouvez configurer l'équilibrage de charge. Dans une configuration haute disponibilité, un nœud unique reçoit toutes les demandes, tandis que les autres sont en attente, ou les demandes sont équilibrées sur l'ensemble des nœuds.

Le proxy de services Web peut exister dans un environnement haute disponibilité (HA), avec la plupart des API fonctionnant correctement, quel que soit le destinataire de la demande. Les balises et les dossiers de métadonnées sont deux exceptions, car les balises et les dossiers sont stockés dans une base de données locale et ne sont pas partagés entre les instances Web Services Proxy.

Toutefois, certains problèmes de synchronisation connus se produisent dans un petit pourcentage de demandes. Plus précisément, une instance du proxy peut avoir des données plus récentes qu'une seconde instance pour une petite fenêtre. Le proxy de services Web inclut une configuration spéciale qui supprime ce problème de synchronisation. Cette option n'est pas activée par défaut, car elle augmente la durée de service des demandes (pour la cohérence des données). Pour activer cette option, vous devez ajouter une propriété à un fichier .INI (pour Windows) ou à un fichier .SH (pour Linux).

Étapes

1. Effectuez l'une des opérations suivantes :
   - Windows : ouvrez le fichier appserver64.ini, puis ajoutez le `Dload-balance.enabled=true` propriété.

     Par exemple : `vmarg.7=-Dload-balance.enabled=true`
   - Linux : ouvrez le fichier webserver.sh, puis ajoutez le `Dload-balance.enabled=true` propriété.

     Par exemple : `DEBUG_START_OPTIONS="-Dload-balance.enabled=true"`
2. Enregistrez les modifications.

3. Redémarrez le service Webserver pour que la modification prenne effet.

Désactivez le symbole HTTPS

Vous pouvez désactiver les commandes de symbole (paramètre par défaut) et envoyer des commandes via un appel de procédure distante (RPC). Ce paramètre peut être modifié dans le fichier wsconfig.xml.

Par défaut, le proxy de services Web envoie des commandes Symbol sur HTTPS pour tous les systèmes de stockage des gammes E2800 et E5700 exécutant SANtricity OS version 08.40 ou ultérieure. Les commandes Symbol envoyées via HTTPS sont authentifiées sur le système de stockage. Si nécessaire, vous pouvez désactiver la prise en charge des symboles HTTPS et envoyer des commandes via RPC. Chaque fois que le symbole sur RPC est configuré, toutes les commandes passives du système de stockage sont activées sans authentification.

Lorsque le symbole sur RPC est utilisé, le proxy de services Web ne peut pas se connecter aux systèmes dont le port de gestion des symboles est désactivé.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Dans le `devicemgt.symbolclientstrategy` entrée, remplacer le `httpsPreferred` valeur avec `rpcOnly`.

   Par exemple :

   ```
   <env key="devicemgt.symbolclientstrategy">rpcOnly</env>
   ```

3. Enregistrez le fichier.

Configurer le partage de ressources d'origine croisée

Vous pouvez configurer le partage de ressources entre les origines (CORS), qui est un mécanisme qui utilise des en-têtes HTTP supplémentaires pour fournir une application Web exécutée à une origine pour avoir la permission d'accéder aux ressources sélectionnées à partir d'un serveur à une autre origine.

CORS est géré par le fichier cors.cfg situé dans le répertoire de travail. La configuration CORS est ouverte par défaut, de sorte que l'accès inter-domaine n'est pas restreint.

Si aucun fichier de configuration n'est présent, CORS est ouvert. Mais si le fichier cors.cfg est présent, il est utilisé. Si le fichier cors.cfg est vide, vous ne pouvez pas effectuer de demande CORS.

Étapes

1. Ouvrez le fichier cors.cfg situé dans le répertoire de travail.
2. Ajoutez les lignes souhaitées au fichier.

   Chaque ligne du fichier de configuration CORS est un modèle d'expression régulier à associer. L'en-tête d'origine doit correspondre à une ligne du fichier cors.cfg. Si un motif de ligne correspond à l'en-tête d'origine, la demande est autorisée. L'origine complète est comparée, pas uniquement l'élément hôte.

3. Enregistrez le fichier.

Les requêtes sont associées sur l'hôte et selon le protocole, par exemple :

- Correspondance avec localhost avec n'importe quel protocole — `*localhost*`
- Correspondance localhost pour HTTPS uniquement — `https://localhost*`

Désinstallez Web Services Proxy

Pour supprimer Web Services Proxy et Unified Manager, vous pouvez utiliser n'importe quel mode (fichier graphique, Console, silencieux ou RPM), quelle que soit la méthode utilisée pour installer le proxy.

Désinstallation en mode graphique

Vous pouvez exécuter la désinstallation en mode graphique pour Windows ou Linux. En mode graphique, les invites s'affichent dans une interface de type Windows.

Étapes

1. Lancez la désinstallation pour Windows ou Linux, comme suit :
   - Windows — accédez au répertoire contenant le fichier de désinstallation de uninstall_web_services_proxy. Le répertoire par défaut est à l'emplacement suivant : C:/Program Files/NetApp/SANtricity Web Services Proxy/. Double-cliquez sur `uninstall_web_services_proxy.exe`.

     Vous pouvez également accéder au menu :panneau de configuration[programmes > Désinstaller un programme], puis sélectionner « NetApp SANtricity Web Services Proxy ».

   - Linux — accédez au répertoire contenant le fichier de désinstallation de Web Services Proxy. Le répertoire par défaut se trouve à l'emplacement suivant : `/opt/netapp/santricity_web_services_proxy/uninstall_web_services_proxy`
2. Exécutez la commande suivante :

   ```
   uninstall_web_services_proxy -i gui
   ```

   L'écran de démarrage du proxy de services Web SANtricity s'affiche.
3. Dans la boîte de dialogue Désinstaller, cliquez sur **Désinstaller**.

   La barre de progression du programme de désinstallation s'affiche et indique la progression.
4. Lorsque le message Désinstaller terminé s'affiche, cliquez sur **terminé**.

Désinstallation du mode console

Vous pouvez exécuter la désinstallation en mode Console pour Windows ou Linux. En mode Console, les invites s'affichent dans la fenêtre du terminal.

Étapes

1. Accédez au répertoire uninstall_web_services_proxy.
2. Exécutez la commande suivante :

```
uninstall_web_services_proxy -i console
```

Le processus de désinstallation démarre.

3. Une fois la désinstallation terminée, appuyez sur **entrée** pour quitter le programme d'installation.

Désinstallation en mode silencieux

Vous pouvez exécuter la désinstallation en mode silencieux pour Windows ou Linux. En mode silencieux, aucun message ou script de retour n'apparaît dans la fenêtre du terminal.

Étapes

1. Accédez au répertoire uninstall_web_services_proxy.
2. Exécutez la commande suivante :

```
uninstall_web_services_proxy -i silent
```

Le processus de désinstallation s'exécute, mais aucun message ou script de retour n'apparaît dans la fenêtre du terminal. Une fois Web Services Proxy désinstallé, une invite de commande apparaît dans la fenêtre du terminal.

COMMANDE RPM désinstaller (Linux uniquement)

Vous pouvez utiliser une commande RPM pour désinstaller Web Services Proxy d'un système Linux.

Étapes

1. Ouvrez une fenêtre de terminal.
2. Saisissez la ligne de commande suivante :

```
rpm -e santricity_webservices
```

> Le processus de désinstallation peut laisser des fichiers qui ne faisaient pas partie de l'installation d'origine. Supprimez manuellement ces fichiers pour supprimer complètement Web Services Proxy.

Gérer l'accès des utilisateurs dans Web Services Proxy

Vous pouvez gérer l'accès des utilisateurs à l'API Web Services et à Unified Manager pour des raisons de sécurité.

Présentation de la gestion des accès

La gestion des accès comprend les connexions basées sur des rôles, le chiffrement par mot de passe, l'authentification de base et l'intégration LDAP.

Accès basé sur des rôles

Le contrôle d'accès basé sur des rôles (RBAC) associe des utilisateurs prédéfinis à des rôles. Chaque rôle accorde des autorisations à un niveau de fonctionnalité spécifique.

Le tableau suivant décrit chaque rôle.

Rôle	Description
security.admin	SSL et gestion des certificats.
storage.admin	Accès complet en lecture/écriture à la configuration du système de stockage.
storage.monitor	Accès en lecture seule pour afficher les données du système de stockage.
support.admin	Accès à toutes les ressources matérielles sur les systèmes de stockage et aux opérations de prise en charge telles que la récupération AutoSupport (ASUP).

Les comptes utilisateur par défaut sont définis dans le fichier users.properties. Vous pouvez modifier les comptes utilisateur en modifiant directement le fichier users.properties ou en utilisant les fonctions de gestion des accès d'Unified Manager.

Le tableau suivant répertorie les connexions utilisateur disponibles pour le proxy de services Web.

Connexion utilisateur prédéfinie	Description
admin	Super administrateur qui a accès à toutes les fonctions et inclut tous les rôles. Pour Unified Manager, vous devez définir le mot de passe lors de la première connexion.
stockage	L'administrateur responsable du provisionnement du stockage. Cet utilisateur comprend les rôles suivants : Storage.admin, support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
sécurité	L'utilisateur responsable de la configuration de la sécurité. Cet utilisateur comprend les rôles suivants : Security.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
assistance	L'utilisateur est responsable des ressources matérielles, des données de défaillance et des mises à niveau du micrologiciel. Cet utilisateur comprend les rôles suivants : support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.

Connexion utilisateur prédéfinie	Description
superviser	Un utilisateur avec un accès au système en lecture seule. Cet utilisateur inclut uniquement le rôle Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
rw (ancienne génération pour les baies plus anciennes)	L'utilisateur rw (read/write) comprend les rôles suivants : Storage.admin, support.admin et Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.
ro (ancienne génération de baies)	L'utilisateur ro (lecture seule) inclut uniquement le rôle Storage.Monitor. Ce compte est désactivé jusqu'à ce qu'un mot de passe soit défini.

Chiffrement par mot de passe

Pour chaque mot de passe, vous pouvez appliquer un processus de chiffrement supplémentaire à l'aide de l'encodage de mot de passe SHA256 existant. Ce processus de chiffrement supplémentaire applique un ensemble aléatoire d'octets à chaque mot de passe (Salt) pour chaque chiffrement SHA256. Le chiffrement saled SHA256 est appliqué à tous les mots de passe nouvellement créés.

Avant la version 3.0 de Web Services Proxy, les mots de passe étaient chiffrés uniquement par hachage SHA256. Tous les mots de passe chiffrés SHA256 uniquement à hachage conservent ce codage et sont toujours valides sous le fichier users.properties. Toutefois, les mots de passe chiffrés uniquement au hachage SHA256 ne sont pas aussi sécurisés que les mots de passe avec chiffrement SAH256 salé.

Authentification de base

Par défaut, l'authentification de base est activée, ce qui signifie que le serveur renvoie un défi d'authentification de base. Ce paramètre peut être modifié dans le fichier wsconfig.xml.

LDAP

Le protocole LDAP (Lightweight Directory Access Protocol), un protocole d'application permettant d'accéder aux services d'informations d'annuaire distribués et de les gérer, est activé pour le proxy de services Web. L'intégration LDAP permet l'authentification des utilisateurs et le mappage des rôles aux groupes.

Pour plus d'informations sur la configuration de la fonctionnalité LDAP, reportez-vous aux options de configuration dans l'interface Unified Manager ou dans la section LDAP de la documentation interactive de l'API.

Configurez l'accès utilisateur

Vous pouvez gérer l'accès des utilisateurs en appliquant un cryptage supplémentaire aux mots de passe, en définissant une authentification de base et en définissant un accès basé sur les rôles.

Appliquer un chiffrement supplémentaire aux mots de passe

Pour un niveau de sécurité maximal, vous pouvez appliquer un chiffrement supplémentaire aux mots de passe à l'aide du codage de mot de passe SHA256 existant.

Ce processus de chiffrement supplémentaire applique un ensemble aléatoire d'octets à chaque mot de passe (Salt) pour chaque chiffrement SHA256. Le chiffrement saled SHA256 est appliqué à tous les mots de passe nouvellement créés.

Étapes

1. Ouvrez le fichier users.properties, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_services_proxy/données/config
2. Saisissez à nouveau le mot de passe chiffré en texte brut.
3. Exécutez le `securepasswds` Utilitaire de ligne de commande pour crypter à nouveau le mot de passe ou simplement redémarrer Web Services Proxy. Cet utilitaire est installé dans le répertoire d'installation racine du proxy de services Web.

> Vous pouvez également Salt et hacher les mots de passe des utilisateurs locaux dès que des modifications du mot de passe sont effectuées via Unified Manager.

Configurer l'authentification de base

Par défaut, l'authentification de base est activée, ce qui signifie que le serveur renvoie un défi d'authentification de base. Si vous le souhaitez, vous pouvez modifier ce paramètre dans le fichier wsconfig.xml.

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Modifiez la ligne suivante dans le fichier en spécifiant FALSE (non activé) ou true (activé).

   Par exemple : `<env key="enable-basic-auth">true</env>`
3. Enregistrez le fichier.
4. Redémarrez le service Webserver pour que la modification prenne effet.

Configurer l'accès basé sur les rôles

Pour limiter l'accès des utilisateurs à des fonctions spécifiques, vous pouvez modifier les rôles spécifiés pour chaque compte utilisateur.

Le proxy de services Web comprend un contrôle d'accès basé sur des rôles (RBAC), dans lequel les rôles sont associés à des utilisateurs prédéfinis. Chaque rôle accorde des autorisations à un niveau de fonctionnalité spécifique. Vous pouvez modifier les rôles affectés aux comptes d'utilisateur en modifiant directement le fichier users.properties.

> Vous pouvez également modifier des comptes d'utilisateur à l'aide de Access Management dans Unified Manager. Pour plus d'informations, consultez l'aide en ligne disponible avec Unified Manager.

Étapes

1. Ouvrez le fichier users.properties, situé dans :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy\data\config
   - (Linux) — /opt/netapp/santricity_web_services_proxy/données/config
2. Recherchez la ligne du compte utilisateur que vous souhaitez modifier (stockage, sécurité, moniteur, prise en charge, rw, ou ro).

   Ne modifiez pas l'utilisateur admin. Il s'agit d'un super utilisateur avec accès à toutes les fonctions.

3. Ajoutez ou supprimez les rôles spécifiés, le cas échéant.

   Les rôles incluent :

   - Security.admin — SSL et gestion des certificats.
   - Storage.admin — accès en lecture/écriture complet à la configuration du système de stockage.
   - Storage.Monitor — accès en lecture seule pour afficher les données du système de stockage.
   - Support.admin — accès à toutes les ressources matérielles sur les systèmes de stockage et aux opérations de support telles que la récupération AutoSupport (ASUP).

     Le rôle Storage.Monitor est obligatoire pour tous les utilisateurs, y compris l'administrateur.

4. Enregistrez le fichier.

Gérer la sécurité et les certificats dans Web Services Proxy

Pour des raisons de sécurité dans Web Services Proxy, vous pouvez spécifier une désignation de port SSL et gérer les certificats. Les certificats identifient les propriétaires de sites Web pour des connexions sécurisées entre les clients et les serveurs.

Activez SSL

Le proxy de services Web utilise SSL (Secure Sockets Layer) pour la sécurité, qui est activé pendant l'installation. Vous pouvez modifier la désignation du port SSL dans le fichier wsconfig.xml.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez ou modifiez le numéro de port SSL, comme dans l'exemple suivant :

```
<sslport clientauth="request">8443</sslport>
```

Résultat

Lorsque le serveur démarre avec SSL configuré, le serveur recherche les fichiers du magasin de clés et du magasin de certificats.

- Si le serveur ne trouve pas de magasin de clés, le serveur utilise l'adresse IP de la première adresse IPv4 non-bouclage détectée pour générer un magasin de clés, puis ajoute un certificat auto-signé au magasin de clés.
- Si le serveur ne trouve pas de truststore ou si le truststore n'est pas spécifié, le serveur utilise le magasin de stockage en tant que truststore.

Validation de certificat de dérivation

Pour prendre en charge les connexions sécurisées, le proxy de services Web valide les certificats des systèmes de stockage par rapport à ses propres certificats de confiance. Si nécessaire, vous pouvez spécifier que le proxy contourne cette validation avant de se connecter aux systèmes de stockage.

Avant de commencer

- Toutes les connexions du système de stockage doivent être sécurisées.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Entrez `true` dans le `trust.all.arrays` comme indiqué dans l'exemple :

```
<env key="trust.all.arrays">true</env>
```

3. Enregistrez le fichier.

Générer et importer un certificat de gestion d'hôte

Les certificats identifient les propriétaires de sites Web pour des connexions sécurisées entre les clients et les serveurs. Pour générer et importer des certificats d'autorité de certification (CA) pour le système hôte sur lequel le proxy de services Web est installé, vous pouvez utiliser des noeuds finaux API.

Pour gérer les certificats du système hôte, vous devez effectuer les tâches suivantes à l'aide de l'API :

- Créez une requête de signature de certificat (RSC) pour le système hôte.
- Envoyez le fichier CSR à une autorité de certification, puis attendez qu'ils vous envoient les fichiers de certificat.
- Importez les certificats signés sur le système hôte.

> Vous pouvez également gérer les certificats dans l'interface Unified Manager. Pour plus d'informations, consultez l'aide en ligne disponible dans Unified Manager.

Étapes

1. Connectez-vous au "Documentation interactive sur les API".
2. Accédez au menu déroulant en haut à droite, puis sélectionnez **v2**.

3. Développez le lien **Administration** et faites défiler vers le bas jusqu'aux noeuds finaux **/certificats**.
4. Générer le fichier CSR :
   a. Sélectionnez **POST:/certificats**, puis **essayez-le**.

      Le serveur Web régénère un certificat auto-signé. Vous pouvez ensuite saisir des informations dans les champs pour définir le nom commun, l'organisation, l'unité organisationnelle, l'ID de remplacement et d'autres informations utilisées pour générer la RSC.

   b. Ajoutez les informations requises dans le volet **exemples de valeurs** pour générer un certificat d'autorité de certification valide, puis exécutez les commandes.

      > ⓘ N'appelez pas **POST:/certificats** ou **POST:/certificats/reset** à nouveau, ou vous devez régénérer la RSC. Lorsque vous appelez **POST:/certificats** ou **POST:/certificats/reset**, vous générez un nouveau certificat auto-signé avec une nouvelle clé privée. Si vous envoyez une RSC générée avant la dernière réinitialisation de la clé privée sur le serveur, le nouveau certificat de sécurité ne fonctionne pas. Vous devez générer une nouvelle RSC et demander un nouveau certificat CA.

   c. Exécutez le noeud final **GET:/certificates/Server** pour confirmer que l'état actuel du certificat est le certificat auto-signé avec les informations ajoutées à partir de la commande **POST:/certificates**.

      Le certificat du serveur (désigné par l'alias `jetty`) est toujours auto-signé à ce stade.

   d. Développez le noeud final **POST:/certificats/export**, sélectionnez **essayez-le**, entrez un nom de fichier pour le fichier CSR, puis cliquez sur **Exécuter**.
5. Copiez et collez le `fileUrl` Dans un nouvel onglet de navigateur pour télécharger le fichier CSR, puis envoyer le fichier CSR à une autorité de certification valide pour demander une nouvelle chaîne de certificats de serveur Web.
6. Lorsque l'autorité de certification émet une nouvelle chaîne de certificats, utilisez un outil de gestionnaire de certificats pour séparer les certificats de serveur racine, intermédiaire et Web, puis importez-les sur le serveur proxy de services Web :
   a. Développez le noeud final **POST:/sslconfig/Server** et sélectionnez **essayez-le**.
   b. Entrez un nom pour le certificat racine de l'autorité de certification dans le champ **alias**.
   c. Sélectionnez **FALSE** dans le champ **replaceMainServerCertificate**.
   d. Recherchez et sélectionnez le nouveau certificat racine de l'autorité de certification.
   e. Cliquez sur **Exécuter**.
   f. Vérifiez que le téléchargement du certificat a réussi.
   g. Répétez la procédure de téléchargement du certificat CA pour le certificat intermédiaire CA.
   h. Répétez la procédure de téléchargement de certificat pour le nouveau fichier de certificat de sécurité du serveur Web, sauf dans cette étape, sélectionnez **true** dans la liste déroulante **replaceMainServerCertificate**.
   i. Vérifiez que l'importation du certificat de sécurité du serveur Web a réussi.
   j. Pour confirmer que les nouveaux certificats de serveur racine, intermédiaire et Web sont disponibles dans le magasin de clés, exécutez **GET:/certificats/serveur**.
7. Sélectionnez et développez le noeud final **POST:/Certificates/reload**, puis sélectionnez **essayez-le out**. Lorsque vous y êtes invité, que vous souhaitiez redémarrer les deux contrôleurs ou non, sélectionnez **FALSE**. (« vrai » s'applique uniquement dans le cas de contrôleurs à double baie.) Cliquez sur **Exécuter**.

Le noeud final **/certificats/rechargement** renvoie généralement une réponse http 202 réussie. Cependant, le rechargement des certificats de stockage fiable du serveur Web et du magasin de clés crée une condition de race entre le processus API et le processus de rechargement des certificats du serveur Web. Dans de rares cas, le rechargement du certificat du serveur Web peut battre le traitement de l'API. Dans ce cas, le rechargement semble échouer même s'il a réussi. Si cela se produit, passez à l'étape suivante. Si le rechargement a effectivement échoué, l'étape suivante échoue également.

8. Fermez la session de navigateur actuelle sur le proxy de services Web, ouvrez une nouvelle session de navigateur et confirmez qu'une nouvelle connexion de navigateur sécurisée au proxy de services Web peut être établie.

   En utilisant une session de navigation privée ou incognito, vous pouvez ouvrir une connexion au serveur sans utiliser les données enregistrées des sessions de navigation précédentes.

Gérer les systèmes de stockage à l'aide du proxy de services Web

Pour gérer les systèmes de stockage sur le réseau, vous devez d'abord les découvrir, puis les ajouter à la liste de gestion.

Découvrir les systèmes de stockage

Vous pouvez configurer la détection automatique ou découvrir manuellement les systèmes de stockage.

Détecter automatiquement les systèmes de stockage

Vous pouvez spécifier que les systèmes de stockage sont automatiquement détectés sur le réseau en modifiant les paramètres du fichier wsconfig.xml. Par défaut, la détection automatique IPv6 est désactivée et IPv4 est activé.

Pour ajouter un système de stockage, il vous suffit de fournir une adresse IP ou DNS de gestion. Le serveur détecte automatiquement tous les chemins de gestion lorsque les chemins ne sont pas configurés ou que les chemins sont configurés et pivotables.

> Si vous tentez d'utiliser un protocole IPv6 pour détecter automatiquement les systèmes de stockage de la configuration du contrôleur après la connexion initiale, le processus risque d'échouer. Les causes possibles de la panne incluent les problèmes lors du transfert d'adresse IP ou de l'activation d'IPv6 sur les systèmes de stockage, mais pas d'activation sur le serveur.

Avant de commencer

Avant d'activer les paramètres de découverte IPv6, vérifiez que votre infrastructure prend en charge la connectivité IPv6 avec les systèmes de stockage pour limiter les problèmes de connexion.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Dans les chaînes de découverte automatique, modifiez les paramètres de `true` à `false`, selon le besoin. Voir l'exemple suivant.

```
<env key="autodiscover.ipv6.enable">true</env>
```

Lorsque les chemins sont configurés, mais pas configurés pour que le serveur puisse acheminer vers les adresses, des erreurs de connexion intermittentes se produisent. Si vous ne pouvez pas définir les adresses IP comme routables à partir de l'hôte, désactivez la détection automatique (définissez les paramètres sur `false`).

3. Enregistrez le fichier.

Découvrez et ajoutez des systèmes de stockage à l'aide de terminaux API

Vous pouvez utiliser des terminaux API pour détecter et ajouter des systèmes de stockage à la liste gérée. Cette procédure crée une connexion de gestion entre le système de stockage et l'API.

Cette tâche décrit comment détecter et ajouter des systèmes de stockage à l'aide de l'API REST, pour que vous puissiez gérer ces systèmes dans la documentation interactive de l'API. Cependant, il peut être préférable de gérer les systèmes de stockage dans Unified Manager, ce qui constitue une interface simple d'utilisation. Pour plus d'informations, consultez l'aide en ligne disponible avec Unified Manager.

Avant de commencer

Pour les systèmes de stockage avec SANtricity versions 11.30 et ultérieures, l'interface de gestion héritée pour le symbole doit être activée dans l'interface SANtricity System Manager. Dans le cas contraire, les noeuds finaux de découverte échouent. Pour trouver ce paramètre, ouvrez System Manager, puis accédez au menu :Paramètres[System > Paramètres supplémentaires > interface de gestion des changements].

Étapes

1. Connectez-vous au "Documentation interactive sur les API".
2. Identifier les systèmes de stockage :

   a. Dans la documentation API, assurez-vous que **V2** est sélectionné dans la liste déroulante, puis développez la catégorie **Storage-Systems**.

   b. Cliquez sur le noeud final **POST: /Discovery**, puis sur **essayez-le**.

   c. Entrez les paramètres comme indiqué dans le tableau.

StartIP IP	
Remplacez la chaîne par la plage d'adresses IP de début et de fin pour un ou plusieurs systèmes de stockage du réseau.	
UseAgents	

Définissez cette valeur sur : • True = utiliser des agents intrabande pour l'analyse réseau. • FALSE = ne pas utiliser d'agents intrabande pour l'analyse réseau.
Délai de connexion
Saisissez les secondes autorisées pour l'acquisition avant que la connexion ne soit interrompue.
MaxPortsToUtilisez
Entrez un nombre maximum de ports utilisés pour l'analyse réseau.

d. Cliquez sur **Exécuter**.

Les actions d'API s'exécutent sans les invites de l'utilisateur.

Le processus de détection s'exécute en arrière-plan.

a. Assurez-vous que le code renvoie un 202.

b. Sous **corps de réponse**, localisez la valeur renvoyée pour la requête. Vous avez besoin de l'ID de la demande pour afficher les résultats à l'étape suivante.

3. Afficher les résultats de la découverte, comme suit :

a. Cliquez sur le noeud final **GET: /Discovery**, puis sur **essayez-le**.

b. Saisissez l'ID de la demande à partir de l'étape précédente. Si vous laissez le champ **Request ID** vide, le noeud final est défini par défaut sur le dernier ID de demande exécuté.

c. Cliquez sur **Exécuter**.

d. S'assurer que le code renvoie 200.

e. Dans le corps de réponse, localisez votre ID de requête et les chaînes pour systèmes de stockage. Les chaînes ressemblent à l'exemple suivant :

```
"storageSystems": [
    {
      "serialNumber": "123456789",
      "wwn": "000A011000AF0000000000001A0C000E",
      "label": "EF570_Array",
      "firmware": "08.41.10.01",
      "nvsram": "N5700-841834-001",
      "ipAddresses": [
        "10.xxx.xx.213",
        "10.xxx.xx.214"
      ],
```

f. Notez les valeurs wwn, label et IPadresses. Vous en avez besoin pour l'étape suivante.

4. Ajout de systèmes de stockage de la manière suivante :
   a. Cliquez sur le noeud final **POST: /Storage-system**, puis sur **essayez-le**.
   b. Entrez les paramètres comme indiqué dans le tableau.

id
Entrez un nom unique pour ce système de stockage. Vous pouvez saisir le libellé (affiché dans la réponse de GET: /Discovery), mais le nom peut être n'importe quelle chaîne que vous choisissez. Si vous ne fournissez pas de valeur pour ce champ, Web Services attribue automatiquement un identifiant unique.
Adresses des contrôleurs
Entrez les adresses IP affichées dans la réponse pour OBTENIR : /Discovery. Pour les doubles contrôleurs, séparez les adresses IP par une virgule. Par exemple : `"IP address 1","IP address 2"`
validation
Entrez `true`, Afin de recevoir une confirmation que les services Web peuvent se connecter au système de stockage.
mot de passe
Entrez le mot de passe d'administration du système de stockage.
wwn
Entrez le WWN du système de stockage (affiché dans la réponse de GET: /Discovery).

   c. Supprimez toutes les chaînes après `"enableTrace": true`, de sorte que l'ensemble de la chaîne soit similaire à l'exemple suivant :

```
{
  "id": "EF570_Array",
  "controllerAddresses": [
    "Controller-A-Mgmt-IP","Controller-B-Mgmt_IP"
  ],
  "validate":true,
  "password": "array-admin-password",
  "wwn": "000A011000AF0000000000001A0C000E",
  "enableTrace": true
}
```

d. Cliquez sur **Exécuter**.

e. Assurez-vous que le code de réponse est 201, ce qui indique que le noeud final a été exécuté avec succès.

   Le noeud final **Post: /Storage-Systems** est mis en file d'attente. Vous pouvez afficher les résultats à l'aide du noeud final **GET: /Storage-Systems** à l'étape suivante.

5. Confirmez l'ajout de la liste comme suit :

   a. Cliquez sur le noeud final **GET: /Storage-system**.

      Aucun paramètre n'est requis.

   b. Cliquez sur **Exécuter**.

   c. Assurez-vous que la réponse du code est 200, ce qui indique que le noeud final a été exécuté avec succès.

   d. Dans le corps de réponse, recherchez les détails relatifs au système de stockage. Les valeurs renvoyées indiquent qu'elles ont été correctement ajoutées à la liste des matrices gérées, comme dans l'exemple suivant :


```
[
  {
    "id": "EF570_Array",
    "name": "EF570_Array",
    "wwn": "000A011000AF0000000000001A0C000E",
    "passwordStatus": "valid",
    "passwordSet": true,
    "status": "optimal",
    "ip1": "10.xxx.xx.213",
    "ip2": "10.xxx.xx.214",
    "managementPaths": [
      "10.xxx.xx.213",
      "10.xxx.xx.214"
  ]
  }
]
```


Évolutivité verticale du nombre de systèmes de stockage gérés

Par défaut, l'API peut gérer jusqu'à 100 systèmes de stockage. Si vous devez gérer davantage de mémoire, vous devez augmenter les exigences de mémoire du serveur.

Le serveur est configuré pour utiliser 512 Mo de mémoire. Pour chaque 100 systèmes de stockage supplémentaires de votre réseau, ajoutez 250 Mo à ce nombre. N'ajoutez pas plus de mémoire que ce que vous avez physiquement. Prévoyez suffisamment d'espace supplémentaire pour votre système d'exploitation et d'autres applications.

La taille par défaut du cache est de 8,192 événements. L'utilisation approximative des données pour le cache d'événements MEL est de 1 Mo pour chaque 8,192 événements. Par conséquent, en conservant les valeurs par défaut, l'utilisation du cache doit être d'environ 1 Mo pour un système de stockage.

Outre la mémoire, le proxy utilise des ports réseau pour chaque système de stockage. Linux et Windows considèrent les ports réseau comme des descripteurs de fichiers. Par mesure de sécurité, la plupart des systèmes d'exploitation limitent le nombre de descripteurs de fichier ouverts qu'un processus ou un utilisateur peut ouvrir à la fois. En particulier dans les environnements Linux, où les connexions TCP ouvertes sont considérées comme des descripteurs de fichier, le proxy de services Web peut facilement dépasser cette limite. Comme le correctif dépend du système, vous devez vous reporter à la documentation de votre système d'exploitation pour savoir comment augmenter cette valeur.

Étapes

1. Effectuez l'une des opérations suivantes :
   - Sous Windows, accédez au fichier appserver64.init. Localiser la ligne, `vmarg.3=-Xmx512M`
   - Sous Linux, accédez au fichier webserver.sh. Localiser la ligne, `JAVA_OPTIONS="-Xmx512M"`
2. Pour augmenter la mémoire, remplacez `512` Avec la mémoire souhaitée en Mo.
3. Enregistrez le fichier.

Gérer l'interrogation automatique des statistiques Web Services Proxy

Vous pouvez configurer l'interrogation automatique pour toutes les statistiques de disque et de volume sur les systèmes de stockage découverts.

Aperçu des statistiques

Ces statistiques fournissent des informations sur les taux de collecte des données et les performances des systèmes de stockage.

Le proxy de services Web permet d'accéder aux types de statistiques suivants :

- Statistiques brutes — compteurs totaux pour les points de données au moment de la collecte des données. Les statistiques brutes peuvent être utilisées pour les opérations de lecture totales ou pour les opérations d'écriture totales.
- Statistiques analysées — informations calculées pour un intervalle. Les statistiques analysées sont des exemples d'opérations de lecture/sortie par seconde ou de débit d'écriture.

Les statistiques brutes sont linéaires et requièrent en général au moins deux points de données collectés pour en extraire des données exploitables. Les statistiques analysées sont une dérivation des statistiques brutes, qui fournissent des mesures importantes. De nombreuses valeurs qui peuvent être dérivées des statistiques brutes sont affichées dans un format de point dans le temps utilisable dans les statistiques analysées pour votre commodité.

Vous pouvez récupérer des statistiques brutes, que l'interrogation automatique soit activée ou non. Vous pouvez ajouter le `usecache=true` Requête chaîne à la fin de l'URL pour récupérer les statistiques mises en cache à partir du dernier sondage. Les résultats en cache augmentent considérablement les performances de

la récupération des statistiques. Toutefois, plusieurs appels à un taux égal ou inférieur à la mémoire cache d'intervalle d'interrogation configurée récupère les mêmes données.

Fonctionnalité Statistiques

Le proxy de services Web fournit des points de terminaison API qui permettent de récupérer les statistiques brutes et analysées du contrôleur et de l'interface à partir de modèles matériels et de versions logicielles pris en charge.

API de statistiques brutes

- `/storage-systems/{system-id}/controller-statistics`
- `/storage-systems/{system-id}/drive-statistics/{optional list of disk ids}`
- `/storage-systems/{system-id}/interface-statistics/{optional list of interface ids}`
- `/storage-systems/{system-id}/volume-statistics/{optional list of volume ids}`

API de statistiques analysées

- `/storage-systems/{id}/analysed-controller-statistics/`
- `/storage-systems/{id}/analysed-drive-statistics/{optional list of disk ids}`
- `/storage-systems/{id}/analysed-interface-statistics/{optional list of interface ids}`
- `/storage-systems/{id}/analysed-volume-statistics/{optional list of volume ids}`

Ces URL extraient les statistiques analysées du dernier sondage et ne sont disponibles que lorsque l'interrogation est activée. Ces URL incluent les données d'entrée-sortie suivantes :

- Opérations par seconde
- Débit en mégaoctets par seconde
- Temps de réponse en millisecondes

Les calculs sont basés sur les différences entre les itérations de polling statistiques, qui sont les mesures les plus courantes en matière de performances du stockage. Ces statistiques sont préférables aux statistiques non analysées.

> Lorsque le système démarre, aucune collecte de statistiques précédente n'est utilisée pour calculer les différentes mesures. Les statistiques analysées nécessitent donc au moins un cycle d'interrogation après le démarrage pour renvoyer les données. En outre, si les compteurs cumulatifs sont réinitialisés, le cycle d'interrogation suivant aura des nombres imprévisibles pour les données.

Configurer les intervalles d'interrogation

Pour configurer les intervalles d'interrogation, modifiez le fichier wsconfig.xml pour spécifier un intervalle d'interrogation en secondes.

Les statistiques étant mises en cache en mémoire, il est possible que la mémoire soit plus importante de 1.5 Mo pour chaque système de stockage.

Avant de commencer

- Les systèmes de stockage doivent être découverts par le proxy.

Étapes

1. Ouvrez le fichier wsconfig.xml, à l'adresse suivante :
   - (Windows) — C:\Program Files\NetApp\SANtricity Web Services Proxy
   - (Linux) — /opt/netapp/santricity_web_services_proxy
2. Ajoutez la ligne suivante à l'intérieur du `<env-entries>` balise, dans laquelle `n` est le nombre de secondes de l'intervalle entre les demandes d'interrogation :

   ```
   <env key="stats.poll.interval">n</env>
   ```

   Par exemple, si 60 est saisi, l'interrogation commence à des intervalles de 60 secondes. C'est-à-dire que le système demande que l'interrogation commence 60 secondes après la fin de la période précédente (quelle que soit la durée de la période de scrutin précédente). Toutes les statistiques sont horodatées avec l'heure exacte de récupération. Le système utilise l'horodatage ou la différence de temps sur laquelle baser le calcul de 60 secondes.

3. Enregistrez le fichier.

Gérer AutoSupport à l'aide du proxy de services Web

Vous pouvez configurer AutoSupport (ASUP), qui collecte les données, puis les envoie automatiquement au support technique pour le dépannage et l'analyse des problèmes à distance.

Présentation d'AutoSupport (ASUP)

La fonctionnalité AutoSupport (ASUP) transmet automatiquement des messages à NetApp selon des critères manuels et basés sur la planification.

Chaque message AutoSupport est un ensemble de fichiers journaux, de données de configuration, de données d'état et de mesures de performances. Par défaut, AutoSupport transmet les fichiers répertoriés dans le tableau suivant à l'équipe de support NetApp une fois par semaine.

Nom du fichier	Description
x-headers-data.txt	Fichier .txt contenant les informations d'en-tête X.
manifest.xml	Fichier .xml détaillant le contenu du message.
arraydata.xml	Un fichier .xml contenant la liste des données client a persisté.

Nom du fichier	Description
appserver-config.txt	Fichier .txt contenant les données de configuration du serveur d'applications.
wsconfig.txt	Fichier .txt contenant les données de configuration du service Web.
host-info.txt	Fichier .txt contenant des informations sur l'environnement hôte.
journaux-serveur.7z	Un fichier .7z contenant chaque fichier journal de serveur Web disponible.
client-info.txt	Fichier .txt avec paires clé/valeur arbitraires pour les compteurs spécifiques à l'application, tels que les accès aux méthodes et aux pages Web.
profil-webservices.json	Ces fichiers contiennent des données de profil Webservices et des données statistiques de surveillance de Jersey. Par défaut, les statistiques de surveillance Jersey sont activées. Vous pouvez les activer et les désactiver dans le fichier wsconfig.xml, comme suit : • Activer : `<env key="enable.jersey.statistics">true</env>` • Désactiver : `<env key="enable.jersey.statistics">false</env>`

Configurez AutoSupport

AutoSupport est activé par défaut lors de l'installation. Cependant, vous pouvez modifier ce paramètre ou les types de distribution.

Activez ou désactivez le protocole AutoSupport

La fonction AutoSupport est activée ou désactivée lors de l'installation initiale du proxy de services Web, mais vous pouvez modifier ce paramètre dans le fichier de configuration de l'utilitaire.

Vous pouvez activer ou désactiver AutoSupport à l'aide du fichier ASUPConfig.xml, comme décrit dans les étapes ci-dessous. Vous pouvez également activer ou désactiver cette fonctionnalité via l'API en utilisant **Configuration** et **POST/asup**, puis en saisissant "true" ou "false".

1. Ouvrez le fichier ASUPConfig.xml dans le répertoire de travail.
2. Localiser les lignes pour <asupdata enable="Boolean_value" timestamp="timestamp">
3. Entrez `true` (activer) ou `false` (désactiver). Par exemple :

```
<asupdata enabled="false" timestamp="0">
```

L'entrée d'horodatage est superflue.

4. Enregistrez le fichier.

Configurer la méthode de livraison AutoSupport

Vous pouvez configurer la fonction AutoSupport pour qu'elle utilise les méthodes de distribution HTTPS, HTTP ou SMTP. HTTPS est la méthode de livraison par défaut.

1. Accédez au fichier ASUPConfig.xml dans le répertoire de travail.
2. Dans la chaîne, `<delivery type="n">`, entrez 1, 2 ou 3 comme décrit dans le tableau :

Valeur	Description
1	**HTTPS** (par défaut) <type de livraison=« 1 »>
2	**HTTP** <type de livraison="2">

3	**SMTP** — pour configurer correctement le type de distribution AutoSupport sur SMTP, vous devez inclure l'adresse du serveur de messagerie SMTP, ainsi que les e-mails de l'expéditeur et du destinataire, comme dans l'exemple suivant :
	
	`<delivery type="3">`
	`<smtp>`
	`<mailserver>smtp.example.com</mailserver>`
	`<sender>user@example.com</sender>`
	`<replyto>user@example.com</replyto>`
	`</smtp>`
	`</delivery>`