Flux de production communs pour la gestion du stockage

Active IQ Unified Manager 9.10

NetApp
October 16, 2025

This PDF was generated from https://docs.netapp.com/fr-fr/active-iq-unified-manager-910/api-automation/concept_workflow_space_issue.html on October 16, 2025. Always check docs.netapp.com for the latest.

Sommaire

Flux de production communs pour la gestion du stockage 1
Présentation des appels API utilisés dans les workflows 1
Détermination des problèmes d'espace dans les agrégats 1
Détermination des problèmes dans les objets de stockage à l'aide d'événements 3
Dépannage des volumes ONTAP à l'aide d'API de passerelle 4
Flux de travail pour la gestion des charges de travail 8
Vérification des SVM sur les clusters 8
Provisionnement des partages de fichiers CIFS et NFS 10
Provisionner les LUN 21
Modification des charges de travail du stockage 26

Flux de production communs pour la gestion du stockage

Les workflows courants fournissent aux développeurs d'applications client des exemples de la façon dont une application client peut appeler les API Active IQ Unified Manager pour exécuter des fonctions courantes de gestion du stockage. Cette section contient certains de ces exemples de flux de travail.

Les flux de travail décrivent les quelques cas d'utilisation courants de gestion du stockage ainsi que des exemples de codes à utiliser. Chacune des tâches est décrite à l'aide d'un processus de workflow composé d'un ou de plusieurs appels API.

Présentation des appels API utilisés dans les workflows

Vous pouvez consulter la page de documentation en ligne de votre instance Unified Manager qui comprend les détails de chaque appel d'API REST. Ce document ne répète pas les détails de la documentation en ligne. Chaque appel API utilisé dans les exemples de flux de travail de ce document comprend uniquement les informations dont vous avez besoin pour localiser l'appel sur la page de documentation. Après avoir localisé un appel API spécifique, vous pouvez vérifier les détails complets de l'appel, y compris les paramètres d'entrée, les formats de sortie, les codes d'état HTTP et le type de traitement de la demande.

Les informations suivantes sont incluses pour chaque appel d'API au sein d'un flux de travail afin de localiser l'appel sur la page de documentation :

- Catégorie : les appels API sont organisés sur la page de documentation en zones ou catégories liées aux fonctions. Pour localiser un appel API spécifique, faites défiler la page jusqu'en bas et cliquez sur la catégorie API applicable.
- Verbe HTTP (appeler) : le verbe HTTP identifie l'action effectuée sur une ressource. Chaque appel d'API est exécuté via un seul verbe HTTP.
- Chemin : le chemin détermine la ressource spécifique à laquelle l'action s'applique dans le cadre d'un appel. La chaîne de chemin d'accès est ajoutée à l'URL principale pour former l'URL complète identifiant la ressource.

Détermination des problèmes d'espace dans les agrégats

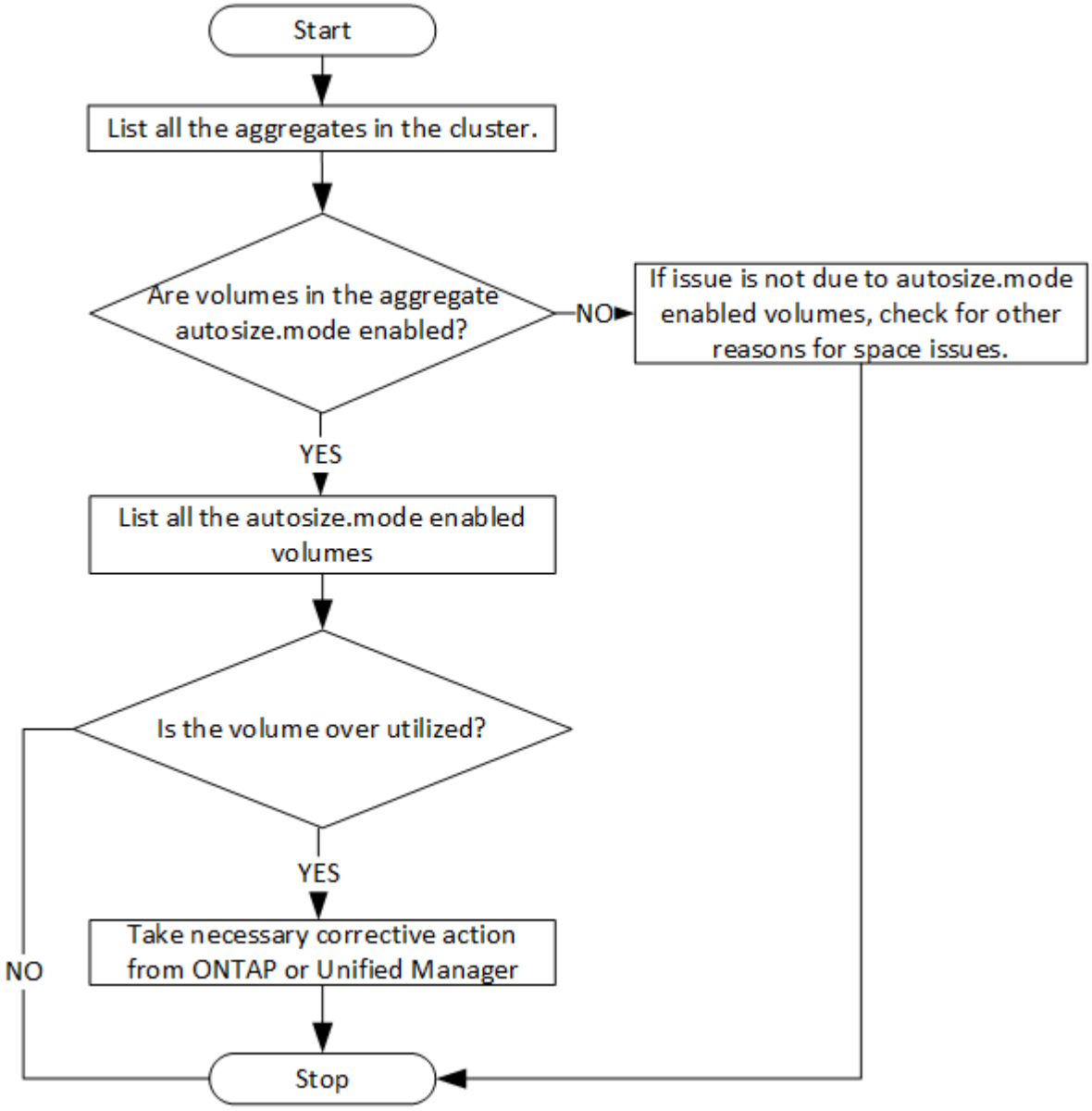
Vous pouvez utiliser les API de data Center de Active IQ Unified Manager pour surveiller la disponibilité et l'utilisation de l'espace dans vos volumes. Vous pouvez identifier les problèmes d'espace de votre volume et les ressources de stockage sur-exploitées ou sous-utilisées,

Les API de data Center pour les agrégats récupère les informations pertinentes sur l'espace disponible et utilisé, et les paramètres d'efficacité pour le gain d'espace. Vous pouvez également filtrer les informations récupérées en fonction des attributs spécifiés.

L'une des méthodes permettant de déterminer le manque d'espace de vos agrégats consiste à vérifier si il existe des volumes dans votre environnement où le mode de taille automatique est activé. Vous devez ensuite identifier les volumes sur-utilisés et effectuer les actions correctives nécessaires.

L'organigramme suivant illustre le processus de récupération des informations sur les volumes dont le mode

autotaille est activé :



Ce flux suppose que les clusters ont déjà été créés dans ONTAP et ajoutés à Unified Manager.

1. Obtenir la clé de cluster, sauf si vous en connaissez la valeur :

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/cluster/clusters`

2. En utilisant la clé de cluster comme paramètre de filtre, interrogez les agrégats sur ce cluster.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/aggregates`

3. Depuis le délai de réponse, analysez l'utilisation de l'espace par les agrégats et déterminez quels agrégats ont des problèmes d'espace. Pour chaque agrégat ayant un problème d'espace, procurez-vous la clé d'agrégat à partir de la même sortie JSON.
4. À l'aide de chaque clé d'agrégat, filtrez tous les volumes qui ont la valeur du paramètre autosize.mode comme `grow`.

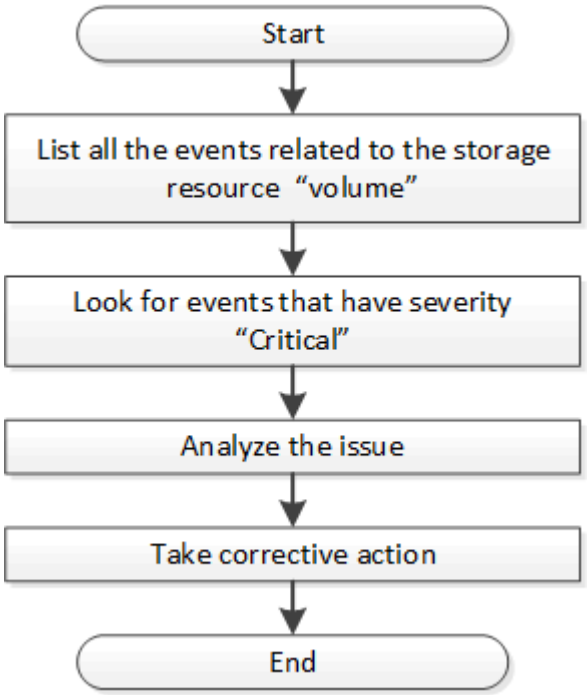
Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/volumes`

5. Analysez les volumes sur-utilisés.
6. Effectuez les actions correctives nécessaires, telles que le déplacement du volume dans les agrégats, pour résoudre les problèmes d'espace de votre volume. Vous pouvez effectuer ces actions à partir de l'interface Web de ONTAP ou de Unified Manager.

Détermination des problèmes dans les objets de stockage à l'aide d'événements

Lorsqu'un objet de stockage de votre data Center franchit un seuil, vous obtenez une notification à propos de cet événement. Grâce à cette notification, vous pouvez analyser le problème et prendre des mesures correctives en utilisant le `events` Via les API.

Ce flux de travail utilise l'exemple d'un volume en tant qu'objet de ressource. Vous pouvez utiliser le `events` API pour récupérer la liste d'événements liés à un volume, analyser les problèmes critiques pour ce volume, puis prendre des mesures correctives pour résoudre le problème.



Procédez comme suit afin de déterminer les problèmes rencontrés sur votre volume avant de prendre les mesures correctives qui s'imposent.

Étapes

1. Analysez les notifications d'événements Active IQ Unified Manager critiques pour les volumes de votre data Center.
2. Interroger tous les événements des volumes à l'aide des paramètres suivants dans l'API /management-Server/Events : `"resource_type": "volume" "severity": "critical"`

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	/serveur-gestion/événements

3. Affichez la sortie et analysez les problèmes des volumes spécifiques.
4. Effectuez les actions nécessaires en utilisant l'API REST ou l'interface utilisateur Web de Unified Manager pour résoudre les problèmes.

Dépannage des volumes ONTAP à l'aide d'API de passerelle

Les API de passerelle servent de passerelle pour appeler les API ONTAP pour interroger les informations sur vos objets de stockage ONTAP et prendre les mesures correctives nécessaires pour résoudre les problèmes signalés.

Ce flux de travail prend un exemple d'utilisation dans lequel un événement est déclenché lorsqu'un volume ONTAP atteint presque sa capacité. Ce workflow explique également comment résoudre ce problème en invoquant une combinaison d'API REST Active IQ Unified Manager et ONTAP.

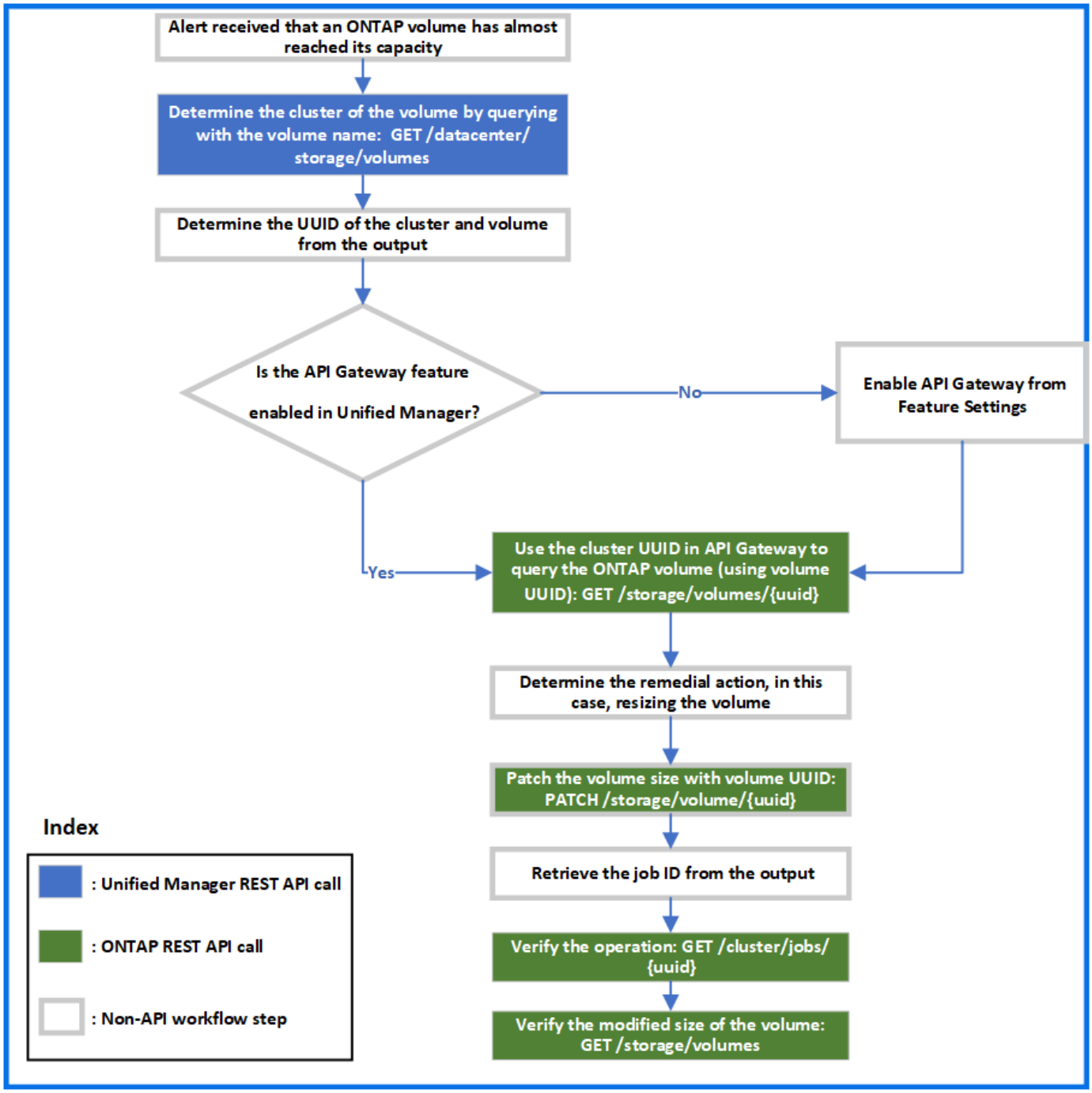
Avant d'exécuter les étapes du workflow, assurez-vous que :

- Vous connaissez les API de passerelle et leur utilisation. Pour plus d'informations, reportez-vous à la section « API de passerelle ».

  "Accès aux API ONTAP via un accès proxy"

- Vous connaissez l'utilisation des API REST de ONTAP. Pour plus d'informations sur l'utilisation des API REST de ONTAP, reportez-vous à la sectionhttps://docs.netapp.com/us-en/ontap-automation/index.html["Documentation sur l'automatisation ONTAP"].
- Vous êtes administrateur d'applications.
- Le cluster sur lequel vous souhaitez exécuter les opérations d'API REST est pris en charge par ONTAP 9.5 ou version ultérieure et le cluster est ajouté à Unified Manager via HTTPS.

Le schéma suivant illustre chaque étape du workflow pour le dépannage des problèmes liés à l'utilisation de la capacité des volumes ONTAP.



Ce workflow couvre les points d'invocation des API REST Unified Manager et ONTAP.

1. Noter le nom du volume provenant de l'événement afin de prévenir l'utilisation de la capacité du volume.
2. En utilisant le nom du volume comme valeur dans le paramètre name, interrogez le volume en exécutant l'API Unified Manager suivante.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/storage/volumes`

3. Récupère l'UUID et l'UUID de volume du cluster à partir du résultat.

4. Dans l'interface utilisateur Web d'Unified Manager, accédez à **général** > **Paramètres de fonctionnalité** > **passerelle API** pour vérifier si la fonctionnalité passerelle API est activée. Sauf si elle est activée, les API de la catégorie passerelle ne sont pas disponibles pour que vous puissiez appeler. Activez la fonction si elle est désactivée.
5. Utilisez l'UUID de cluster pour exécuter l'API ONTAP `/storage/volumes/{uuid}` Via la passerelle API. La requête renvoie les détails du volume lorsque l'UUID du volume est transmis en tant que paramètre API.

   Pour exécuter les API ONTAP via la passerelle d'API, les identifiants Unified Manager sont transférés en interne à des fins d'authentification, et vous n'avez pas besoin d'exécuter une étape d'authentification supplémentaire pour l'accès individuel au cluster.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	OBTENEZ	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

   Dans /gateways/{UUID}/{path}, la valeur de {UUID} doit être remplacée par l'UUID de cluster sur lequel l'opération DE REPOS doit être effectuée. {path} doit être remplacé par l'URL REST ONTAP /stockage/volumes/{UUID}.

   L'URL ajoutée est : `/gateways/{cluster_uuid}/storage/volumes/{volume_uuid}`

   Lors de l'exécution de L'opération GET, l'URL générée est : `GEThttps://<hostname\>/api/gateways/<cluster_UUID\>/storage/volumes/{volume_uuid}`

   Commande Curl exemple

```
curl -X GET "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7"
-H "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>"
```

6. À partir des résultats, déterminez la taille, l'utilisation et la mesure corrective à prendre. Dans ce flux de travail, la mesure corrective prise consiste à redimensionner le volume.
7. Utilisez l'UUID de cluster et exécutez l'API ONTAP suivante via la passerelle d'API pour redimensionner le volume. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	CORRECTIF	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

> En plus de l'UUID et de l'UUID de volume du cluster, vous devez saisir une valeur pour le paramètre size permettant le redimensionnement du volume. Assurez-vous de saisir la valeur *dans octets*. Par exemple, pour augmenter la taille d'un volume de 100 Go à 120 Go, entrez la valeur du paramètre size à la fin de la requête : `-d {\"size\": 128849018880}"`

Commande Curl exemple

```
curl -X PATCH "https://<hostname>/api/gateways/1cd8a442-86d1-11e0-ae1c-
9876567890123/storage/volumes/028baa66-41bd-11e9-81d5-00a0986138f7" -H
    "accept: application/hal+json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
    {\"size\": 128849018880}"
```

La sortie JSON renvoie un UUID de tâche.

8. Vérifiez si le travail a bien été exécuté à l'aide de l'UUID du travail. Utilisez l'UUID et l'UUID de cluster pour exécuter l'API ONTAP suivante via la passerelle d'API. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : cluster	OBTENEZ	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/cluster/jobs/{uuid}`

Les codes HTTP renvoyés sont les mêmes que les codes d'état HTTP de l'API REST ONTAP.

9. Exécutez l'API ONTAP suivante pour interroger les détails du volume redimensionné. Pour plus d'informations sur les paramètres d'entrée de la passerelle et des API ONTAP, reportez-vous à l'étape 5.

Catégorie	Verbe HTTP	Chemin
Unified Manager : passerelle ONTAP : stockage	OBTENEZ	API de passerelle : `/gateways/{uuid}/{path}` API ONTAP : `/storage/volumes/{uuid}`

La sortie affiche une taille de volume accrue de 120 Go.

Flux de travail pour la gestion des charges de travail

Active IQ Unified Manager permet de provisionner et de modifier les charges de travail de stockage (LUN, partages de fichiers NFS et partages CIFS). Le provisionnement s'effectue en plusieurs étapes, de la création des SVM (Storage Virtual machine) à l'application des règles de niveau de service en matière de performances et d'efficacité du stockage aux charges de travail du stockage. La modification des charges de travail consiste en des étapes de modification de paramètres spécifiques et d'activation de fonctionnalités supplémentaires.

Les flux de production suivants sont décrits :

- Flux de production pour le provisionnement des SVM (Storage Virtual machines) sur Unified Manager.

  Ce flux de travail est requis avant de provisionner des LUN ou des partages de fichiers sur Unified Manager.

- Provisionnement des partages de fichiers.
- Provisionner les LUN.
- Modification des LUN et des partages de fichiers (à l'aide de l'exemple de mise à jour du paramètre Performance Service Level pour les charges de travail du stockage).
- Modification d'un partage de fichiers NFS pour prendre en charge le protocole CIFS
- Modification des charges de travail pour mettre à niveau QoS vers AQoS

Pour chaque workflow de provisionnement (partages de LUN et de fichiers), veillez à avoir terminé le workflow de vérification des SVM sur les clusters.

Vous devez également lire les recommandations et limites avant d'utiliser chaque API dans les workflows. Les détails pertinents des API sont disponibles dans leurs différentes sections répertoriées dans les concepts et références associés.

Vérification des SVM sur les clusters

Avant de provisionner des partages de fichiers ou des LUN, vous devez vérifier si les clusters disposent de SVM (Storage Virtual machines) créés.

Le flux de travail suppose que des clusters ONTAP doivent avoir été ajoutés à Unified Manager et que la clé de cluster a été obtenue. Les clusters doivent disposer des licences requises pour provisionner les LUN et les partages de fichiers sur eux.

1. Vérifier si le cluster a un SVM créé ou non.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/svm/svms` `/datacenter/svm/svms/{key}`

CURL d'échantillon

```
curl -X GET "https://<hostname>/api/datacenter/svm/svms" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si la clé SVM n'est pas renvoyée, créer la SVM. Pour la création des SVM, il faut la clé de cluster sur laquelle vous provisionnez la SVM. Vous devez également spécifier le nom du SVM. Effectuez la procédure suivante.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/cluster/clusters` `/datacenter/cluster/clusters/{key}`

Obtenir la clé de cluster.

CURL d'échantillon

```
curl -X GET "https://<hostname>/api/datacenter/cluster/clusters" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

3. Depuis le résultat, obtenir la clé du cluster, puis l'utiliser comme entrée pour la création de la SVM.

> Lors de la création du SVM, s'assurer qu'il prend en charge tous les protocoles requis pour le provisionnement des LUN et des partages de fichiers sur eux, par exemple, CIFS, NFS, FCP, Et iSCSI. Les workflows de provisionnement peuvent échouer si le SVM ne prend pas en charge les services requis. Il est recommandé que les services pour les types de charges de travail respectifs soient également activés sur le SVM.

Catégorie	Verbe HTTP	Chemin
data center	POST	`/datacenter/svm/svms`

CURL d'échantillon

Entrer les détails de l'objet SVM en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/datacenter/svm/svms" -H "accept:
application/json" -H "Content-Type: application/json" -H "Authorization:
Basic <Base64EncodedCredentials>" "{ \"aggregates\": [ { \"_links\": {},
\"key\": \"1cd8a442-86d1,type=objecttype,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\",
\"name\": \"cluster2\", \"uuid\": \"02c9e252-41be-11e9-81d5-
00a0986138f7\" } ],
\"cifs\": { \"ad_domain\": { \"fqdn\": \"string\", \"password\":
\"string\",
\"user\": \"string\" }, \"enabled\": true, \"name\": \"CIFS1\" },
\"cluster\": { \"key\": \"1cd8a442-86d1-11e0-ae1c-
123478563412,type=object type,uuid=1cd8a442-86d1-11e0-ae1c-
9876567890123\" },
\"dns\": { \"domains\": [ \"example.com\", \"example2.example3.com\" ],
\"servers\": [ \"10.224.65.20\", \"2001:db08:a0b:12f0::1\" ] },
\"fcp\": { \"enabled\": true }, \"ip_interface\": [ { \"enabled\": true,
\"ip\": { \"address\": \"10.10.10.7\", \"netmask\": \"24\" },
\"location\": { \"home_node\": { \"name\": \"node1\" } }, \"name\":
\"dataLif1\" } ], \"ipspace\": { \"name\": \"exchange\" },
\"iscsi\": { \"enabled\": true }, \"language\": \"c.utf_8\",
\"ldap\": { \"ad_domain\": \"string\", \"base_dn\": \"string\",
\"bind_dn\": \"string\", \"enabled\": true, \"servers\": [ \"string\" ]
},
\"name\": \"svm1\", \"nfs\": { \"enabled\": true },
\"nis\": { \"domain\": \"string\", \"enabled\": true,
\"servers\": [ \"string\" ] }, \"nvme\": { \"enabled\": true },
\"routes\": [ { \"destination\": { \"address\": \"10.10.10.7\",
\"netmask\": \"24\" }, \"gateway\": \"string\" } ],
\"snapshot_policy\": { \"name\": \"default\" },
\"state\": \"running\", \"subtype\": \"default\"}"
```

La sortie JSON affiche une clé d'objet Job que vous pouvez utiliser pour vérifier la SVM que vous avez créée.

4. Vérifier la création du SVM à l'aide de la clé d'objet de travail pour la requête. Si la SVM est correctement créée, la clé de SVM est renvoyée dans la réponse.

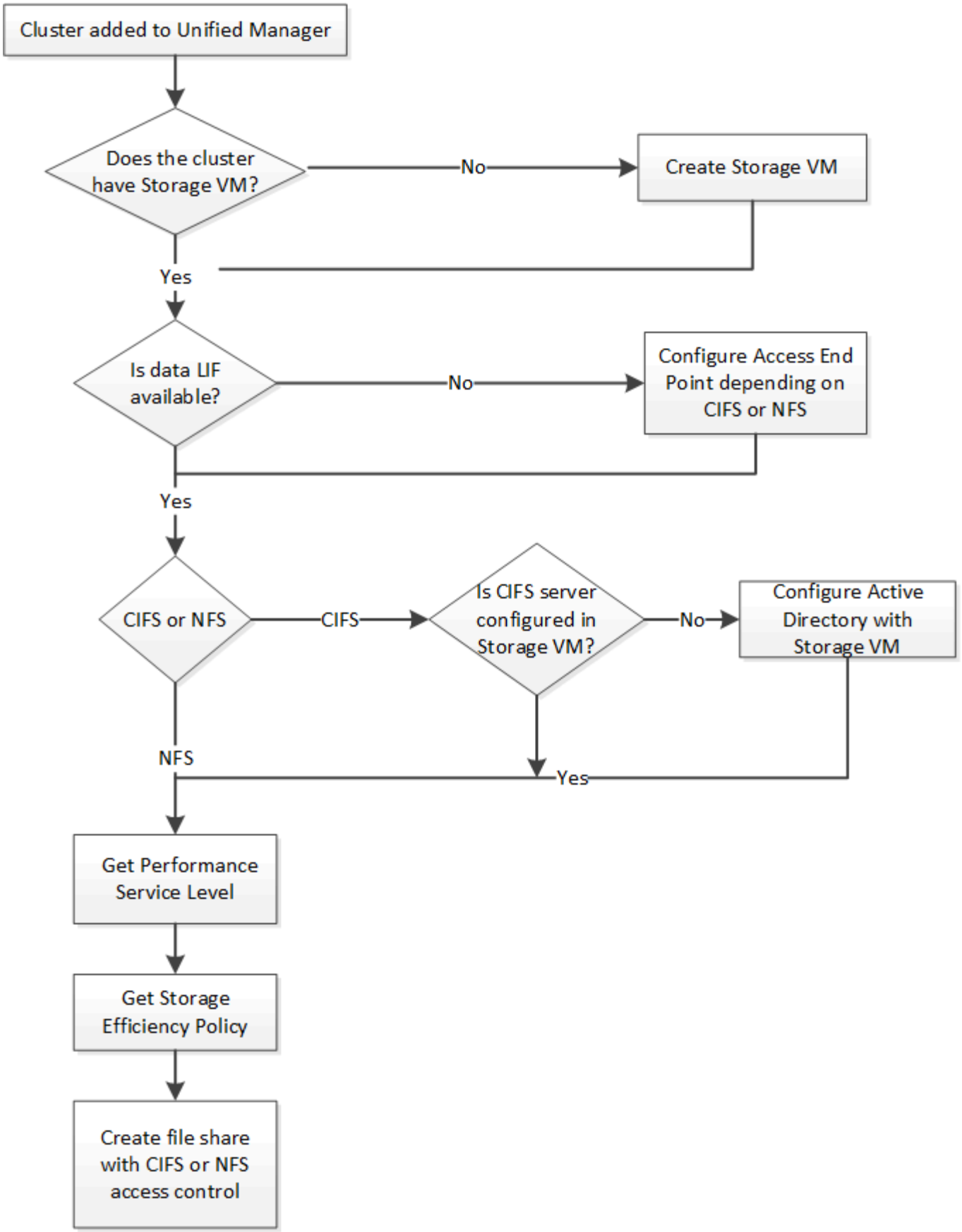
Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

Provisionnement des partages de fichiers CIFS et NFS

Vous pouvez provisionner les partages CIFS et les partages de fichiers NFS sur vos SVM

(Storage Virtual machines) en utilisant les API de provisionnement fournies dans Active IQ Unified Manager. Ce workflow de provisionnement détaille les étapes à suivre pour récupérer les clés des SVM, Performance Service Levels et Storage Efficiency Policies avant de créer les partages de fichiers.

Le schéma suivant illustre chaque étape d'un workflow de provisionnement de partage de fichiers. Il inclut le provisionnement des partages CIFS et des partages de fichiers NFS.


Cluster added to Unified Manager
Does the cluster have Storage VM?
No
Create Storage VM
Yes
Is data LIF available?
No
Configure Access End Point depending on CIFS or NFS
Yes
CIFS or NFS
CIFS
Is CIFS server configured in Storage VM?
No
Configure Active Directory with Storage VM
NFS
Yes
Get Performance Service Level
Get Storage Efficiency Policy
Create file share with CIFS or NFS access control

Vérifiez les points suivants :

- Les clusters ONTAP ont été ajoutés à Unified Manager et la clé de cluster a été obtenue.
- Les SVM ont été créés sur les clusters.
- Les SVM prennent en charge les services CIFS et NFS. Le provisionnement des partages de fichiers peut échouer si les SVM ne prennent pas en charge les services requis.
- Le port FCP est en ligne pour le provisionnement des ports.

1. Déterminez si les LIF de données ou les terminaux d'accès sont disponibles sur le SVM sur lequel vous souhaitez créer le partage CIFS. Obtenez la liste des terminaux d'accès disponibles sur le SVM :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/access-endpoints /storage-provider/access-endpoints/{key}`

CURL d'échantillon

```
curl -X GET "https://<hostname>/api/storage-provider/access-endpoints?resource.key=7d5a59b3-953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
```

2. Si votre point de terminaison d'accès est disponible dans la liste, procurez-vous la clé du point de terminaison d'accès, sinon créez le point de terminaison d'accès.

Veillez à créer des points de terminaison d'accès sur lesquels le protocole CIFS est activé. Le provisionnement des partages CIFS échoue, sauf si vous avez créé un terminal d'accès avec le protocole CIFS activé sur celui-ci.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

CURL d'échantillon

Vous devez entrer les détails du point final d'accès que vous souhaitez créer, en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/storage-provider/access-endpoints"
-H "accept: application/json" -H "Content-Type: application/json" -H
"Authorization: Basic <Base64EncodedCredentials>"
{ \"data_protocols\": \"nfs\",
\"fileshare\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=volume,uuid=f3063d27-2c71-44e5-9a69-a3927c19c8fc\" },
\"gateway\": \"10.132.72.12\",
\"ip\": { \"address\": \"10.162.83.26\",
\"ha_address\": \"10.142.83.26\",
\"netmask\": \"255.255.0.0\" },
\"lun\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a098d39e12:type=lun,uuid=d208cc7d-80a3-4755-93d4-5db2c38f55a6\" },
\"mtu\": 15000, \"name\": \"aep1\",
\"svm\": { \"key\": \"cbd1757b-0580-11e8-bd9d-
00a178d39e12:type=vserver,uuid=1d1c3198-fc57-11e8-99ca-00a098d38e12\" },
\"vlan\": 10}"
```

La sortie JSON affiche une clé d'objet travail que vous pouvez utiliser pour vérifier le noeud final d'accès que vous avez créé.

3. Vérifiez le point d'accès :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

4. Déterminez si vous devez créer un partage CIFS ou NFS. Pour créer des partages CIFS, suivez ces sous-étapes :

   a. Déterminer si le serveur CIFS est configuré sur votre SVM, il s'agit de déterminer si un mappage Active Directory est créé sur le SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/active-directories-mappings`

   b. Si le mappage Active Directory est créé, prendre la clé, sinon créer le mappage Active Directory sur la SVM.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/active-directories-mappings`

CURL d'échantillon

Vous devez entrer les détails de création du mappage Active Directory, en tant que paramètres d'entrée.

```
curl -X POST "https://<hostname>/api/storage-provider/active-
directories-mappings" -H "accept: application/json" -H "Content-Type:
application/json" -H "Authorization: Basic <Base64EncodedCredentials>"
{ \"_links\": {},
\"dns\": \"10.000.000.000\",
\"domain\": \"example.com\",
\"password\": \"string\",
\"svm\": { \"key\": \"9f4ddea-e395-11e9-b660-
005056a71be9:type=vserver,uuid=191a554a-f0ce-11e9-b660-005056a71be9\" },
\"username\": \"string\"}"
```

+ Il s'agit d'un appel synchrone et vous pouvez vérifier la création du mappage Active Directory dans la sortie. En cas d'erreur, le message d'erreur s'affiche pour vous permettre de dépanner et de relancer la demande.

5. Obtenir la clé SVM pour le SVM sur lequel vous souhaitez créer le partage CIFS ou le partage de fichiers NFS, comme décrit dans la rubrique *vérification des SVM sur clusters* workflow.
6. Obtenir la clé pour le niveau de service des performances en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/performance-service-levels`

Pour récupérer les détails des niveaux de service de performances définis par le système, définissez le paramètre `system_defined` saisissez le paramètre à `true`. À partir de la sortie, procurez-vous la clé du niveau de service de performances que vous souhaitez appliquer sur le partage de fichiers.

7. Si vous le souhaitez, vous pouvez également obtenir la clé de stratégie d'efficacité du stockage pour la stratégie d'efficacité du stockage que vous souhaitez appliquer au partage de fichiers en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/storage-efficiency-policies`

8. Créez le partage de fichiers. Vous pouvez créer un partage de fichiers prenant en charge CIFS et NFS en spécifiant la liste de contrôle d'accès et les règles d'exportation. Les sous-étapes suivantes fournissent des

informations si vous souhaitez créer un partage de fichiers pour la prise en charge d'un seul des protocoles sur le volume. Vous pouvez également mettre à jour un partage de fichiers NFS pour inclure la liste de contrôle d'accès après avoir créé le partage NFS. Pour plus d'informations, reportez-vous à la rubrique *modification des charges de travail du stockage*.

a. Pour la création uniquement d'un partage CIFS, collectez les informations de la liste de contrôle d'accès (ACL). Pour créer le partage CIFS, indiquez des valeurs valides pour les paramètres d'entrée suivants. Pour chaque groupe d'utilisateurs que vous attribuez, une liste de contrôle d'accès est créée lorsqu'un partage CIFS/SMB est provisionné. En fonction des valeurs que vous saisissez pour le mappage ACL et Active Directory, le contrôle d'accès et le mappage sont déterminés pour le partage CIFS lors de sa création.

   Une commande curl avec des valeurs d'échantillon

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    },
```

b. Pour la création uniquement d'un partage de fichiers NFS, collectez les informations de l'export policy. Pour créer le partage de fichiers NFS, indiquez des valeurs valides pour les paramètres d'entrée suivants. En fonction de vos valeurs, l'export policy est jointe au partage de fichiers NFS lors de sa création.

   Lors du provisionnement du partage NFS, vous pouvez créer une export policy en fournissant toutes les valeurs requises ou fournir la clé export policy et réutiliser une export policy existante. Si vous souhaitez réutiliser une export policy pour la machine virtuelle de stockage, vous devez ajouter la clé export policy. À moins que vous ne sachiez la clé, vous pouvez récupérer la clé d'export-policy à l'aide de l'`/datacenter/protocols/nfs/export-policies` API. Pour créer une nouvelle règle, vous devez entrer les règles comme indiqué dans l'exemple suivant. Pour les règles saisies, l'API tente de rechercher une export policy existante en faisant correspondre l'hôte, la VM de stockage et les règles. S'il existe une export policy existante, elle est utilisée. Dans le cas contraire, une nouvelle export-policy est créée.

   Une commande curl avec des valeurs d'échantillon

```
"export_policy": {
      "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
      "name_tag": "ExportPolicyNameTag",
      "rules": [
        {
          "clients": [
            {
              "match": "0.0.0.0/0"
            }
```

Après avoir configuré la liste de contrôle d'accès et la stratégie d'exportation, fournissez les valeurs valides des paramètres d'entrée obligatoires pour les partages de fichiers CIFS et NFS :

Storage Efficiency Policy est un paramètre facultatif pour la création de partages de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/file-shares`

La sortie JSON affiche une clé d'objet travail que vous pouvez utiliser pour vérifier le partage de fichiers que vous avez créé. . Vérifiez la création du partage de fichiers à l'aide de la clé objet travail renvoyée dans l'interrogation du travail :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

À la fin de la réponse, vous voyez la clé du partage de fichiers créé.

```
    ],
    "job_results": [
        {
            "name": "fileshareKey",
            "value": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6"
        }
    ],
    "_links": {
        "self": {
            "href": "/api/management-server/jobs/06a6148bf9e862df:-
2611856e:16e8d47e722:-7f87"
        }
    }
}
```

1. Vérifiez la création du partage de fichiers en exécutant l'API suivante avec la clé renvoyée :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares/{key}`

Sortie JSON échantillon

Vous pouvez voir que la méthode POST de `/storage-provider/file-shares` Appelle en interne toutes les API requises pour chacune des fonctions et crée l'objet. Par exemple, il invoque le `/storage-provider/performance-service-levels/` API permettant d'attribuer le niveau de service de performances au partage de fichiers.

```
{
    "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-00a098dcc6b6",
    "name": "FileShare_377",
    "cluster": {
        "uuid": "7d5a59b3-953a-11e8-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-00a098dcc959",
        "name": "AFFA300-206-68-70-72-74",
        "_links": {
            "self": {
                "href": "/api/datacenter/cluster/clusters/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=cluster,uuid=7d5a59b3-953a-11e8-8857-
00a098dcc959"
            }
```

```
        }
    },
    "svm": {
        "uuid": "b106d7b1-51e9-11e9-8857-00a098dcc959",
        "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-00a098dcc959",
        "name": "RRT_ritu_vs1",
        "_links": {
            "self": {
                "href": "/api/datacenter/svm/svms/7d5a59b3-953a-11e8-
8857-00a098dcc959:type=vserver,uuid=b106d7b1-51e9-11e9-8857-
00a098dcc959"
            }
        }
    },
    "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
    },
    "recommended_performance_service_level": {
        "key": null,
        "name": "Idle",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
    },
    "space": {
        "size": 104857600
    },
    "assigned_storage_efficiency_policy": {
        "key": null,
        "name": "Unassigned",
        "_links": {}
    },
    "access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
```

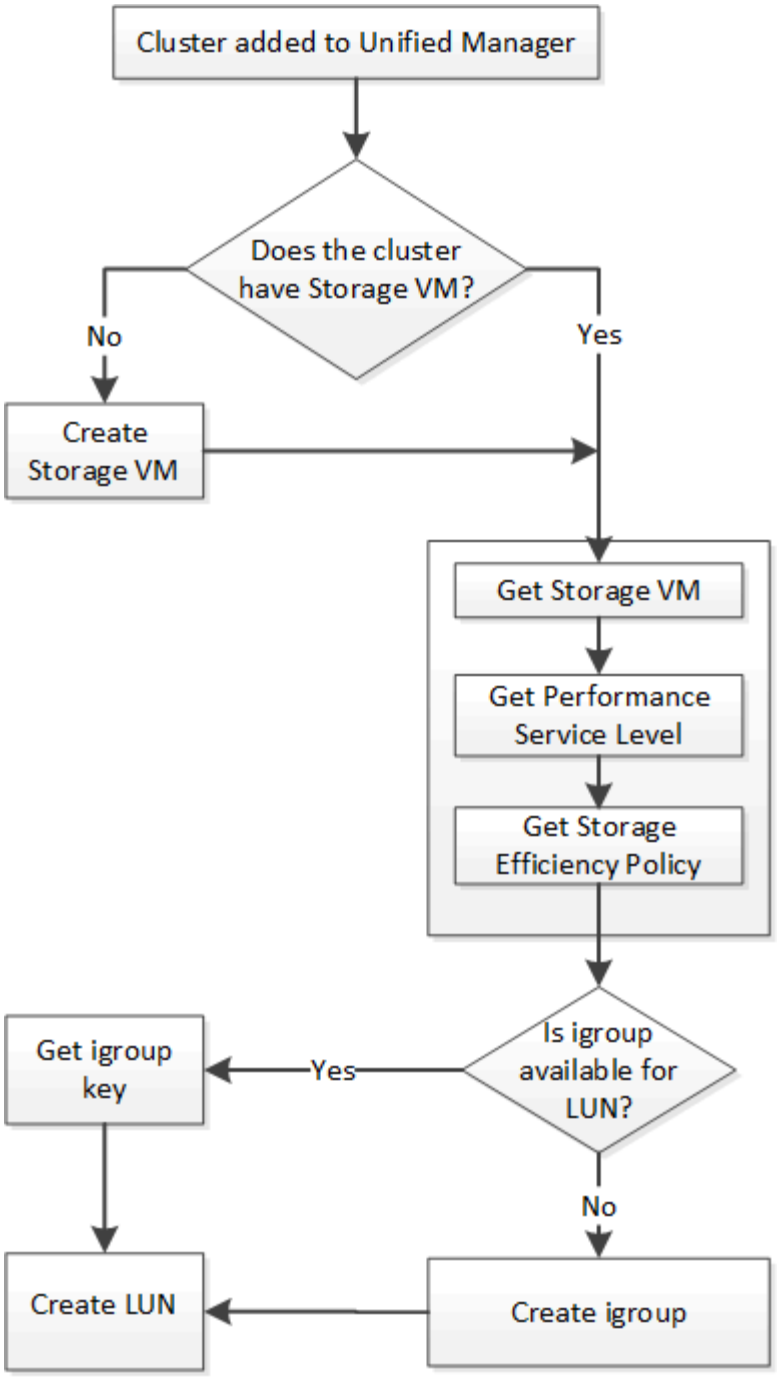
```
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
```

```
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
}
```

Provisionner les LUN

Vous pouvez provisionner des LUN sur vos SVM (Storage Virtual machines) en utilisant les API de provisionnement fournies par Active IQ Unified Manager. Ce workflow de provisionnement détaille les étapes à suivre pour récupérer les clés des SVM, les niveaux de service performances et les règles d'efficacité du stockage avant de créer la LUN.

Le schéma suivant illustre les étapes d'un workflow de provisionnement de LUN.



Ce flux de travail suppose que les clusters ONTAP ont été ajoutés à Unified Manager et que la clé de cluster a été obtenue. Le workflow suppose également que les SVM ont déjà été créés sur les clusters.

1. Obtenir la clé SVM pour le SVM sur lequel vous souhaitez créer la LUN, comme décrit dans la rubrique *Vérification des SVM sur les clusters* workflow.
2. Obtenir la clé pour le niveau de service des performances en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/performance-service-levels`

Pour récupérer les détails des niveaux de service de performances définis par le système, définissez le paramètre `system_defined` saisissez le paramètre à `true`. Dans le résultat de cette commande, vous devez obtenir la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

3. Si vous le souhaitez, vous pouvez également obtenir la clé de la politique d'efficacité du stockage que vous souhaitez appliquer sur la LUN en exécutant l'API suivante et en récupérant la clé de la réponse.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/storage-efficiency-policies`

4. Déterminez si des groupes initiateurs (igroups) ont été créés pour autoriser l'accès à la cible de LUN que vous souhaitez créer.

Catégorie	Verbe HTTP	Chemin
data center	OBTENEZ	`/datacenter/protocols/san/igroups` `/datacenter/protocols/san/igroups/{key}`

Vous devez saisir la valeur de paramètre pour indiquer la SVM pour laquelle le groupe initiateur a autorisé l'accès. En outre, pour effectuer une requête sur un groupe initiateur spécifique, entrez le nom de ce groupe initiateur (clé) comme paramètre d'entrée.

5. Dans le résultat de cette commande, si vous trouvez le groupe initiateur auquel vous souhaitez accorder l'accès, obtenez la clé. Sinon, créez le groupe initiateur.

Catégorie	Verbe HTTP	Chemin
data center	POST	`/datacenter/protocols/san/igroups`

Vous devez entrer les détails du groupe initiateur que vous souhaitez créer en tant que paramètres d'entrée. Il s'agit d'un appel synchrone pour vérifier la création du groupe initiateur dans la sortie. En cas d'erreur, un message s'affiche pour vous permettre de dépanner et de relancer l'API.

6. Créer la LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/luns`

Pour créer la LUN, assurez-vous d'avoir ajouté les valeurs récupérées en tant que paramètres d'entrée obligatoires.

La stratégie d'efficacité du stockage est un paramètre facultatif pour la création des LUN.

CURL d'échantillon

Vous devez entrer tous les détails de la LUN que vous souhaitez créer en tant que paramètres d'entrée.

Wombat : extrait n° 1

La sortie JSON affiche une clé d'objet travail que vous pouvez utiliser pour vérifier la LUN que vous avez créée.

7. Vérifiez la création de la LUN à l'aide de la clé de l'objet travail renvoyée dans l'interrogation du travail :

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

À la fin de la réponse, vous voyez la clé de la LUN créée.

Wombat: Extrait # 2

8. Vérifiez la création de la LUN en exécutant l'API suivante avec la clé renvoyée :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Sortie JSON échantillon

Vous pouvez voir que la méthode POST de `/storage-provider/luns` Appelle en interne toutes les API requises pour chacune des fonctions et crée l'objet. Par exemple, il invoque le `/storage-provider/performance-service-levels/` API permettant d'attribuer un niveau de service de performances à la LUN.

Wombat: Extrait # 3

Procédure de dépannage en cas de échec de la création ou du mappage de LUN

À l'issue de ce workflow, il se peut que la création de LUN ait échoué. Même si la LUN est correctement créée, le mappage de LUN avec le groupe initiateur peut échouer en raison d'une indisponibilité d'une LIF SAN ou d'un point de terminaison d'accès sur le nœud sur lequel vous créez la LUN. En cas de défaillance, le message suivant s'affiche :

```
The nodes <node_name> and <partner_node_name> have no LIFs configured with
the iSCSI or FCP protocol for Vserver <server_name>. Use the access-
endpoints API to create a LIF for the LUN.
```

Suivez ces étapes de dépannage pour contourner ce problème.

1. Créer un point d'accès prenant en charge le protocole ISCSI/FCP sur le SVM sur lequel vous avez essayé de créer la LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	POST	`/storage-provider/access-endpoints`

CURL d'échantillon

Vous devez entrer les détails du point final d'accès que vous souhaitez créer, en tant que paramètres d'entrée.

> Assurez-vous que dans le paramètre d'entrée vous avez ajouté l'adresse pour indiquer le nœud d'origine de la LUN et l'adresse ha pour indiquer le nœud partenaire du nœud de départ. Lorsque vous exécutez cette opération, des terminaux d'accès sont créés sur le nœud de rattachement et le nœud partenaire.

Wombat: Extrait # 4

2. Interroger le travail avec la clé objet Job renvoyée dans la sortie JSON pour vérifier qu'elle s'exécute correctement pour ajouter les terminaux d'accès sur la SVM et que les services iSCSI/FCP ont été activés sur la SVM.

Catégorie	Verbe HTTP	Chemin
serveur-gestion	OBTENEZ	`/management-server/jobs/{key}`

Sortie JSON échantillon

À la fin de la sortie, vous pouvez voir la clé des points d'extrémité d'accès créés. Dans le résultat suivant, la valeur "nom": "AccessEndpointKey" indique le noeud final d'accès créé sur le noeud d'origine du LUN, pour lequel la clé est 9c964258-14ef-11ea-95e2-00a098e32c28. La valeur "name": "AccessEndpointHADKey" indique le noeud final d'accès créé sur le noeud partenaire du noeud d'origine, pour lequel la clé est 9d347006-14ef-11ea-8760-00a098e3215f.

Wombat: Extrait # 5

3. Modifiez la LUN pour mettre à jour le mappage de groupe initiateur. Pour plus d'informations sur la modification des flux de travail, reportez-vous à la section « Modifier les charges de travail de stockage ».

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans le champ d'entrée, spécifiez la clé igroup avec laquelle vous souhaitez mettre à jour le mappage de LUN, ainsi que la clé de LUN.

CURL d'échantillon

Wombat: Extrait # 6

La sortie JSON affiche une clé d'objet travail que vous pouvez utiliser pour vérifier si le mappage a réussi.

4. Vérifiez le mappage de LUN en interrogeant la clé de LUN.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Sortie JSON échantillon

Dans le résultat, vous voyez que la LUN a été correctement mappée avec le groupe initiateur (clé d19ec2fa-fec7-11e8-b23d-00a098e32c28) avec lequel elle a été initialement mise en service.

Wombat: Extrait # 7

Modification des charges de travail du stockage

La modification des charges de travail de stockage consiste à mettre à jour les LUN ou les partages de fichiers dont les paramètres sont manquants ou à modifier les paramètres existants.

Ce flux de travail utilise un exemple de mise à jour des niveaux de service de performance pour les LUN et les partages de fichiers.

Le flux de travail suppose que le partage de fichiers ou de LUN a été provisionné avec des niveaux de service de performance.

Modification des partages de fichiers

Lors de la modification d'un partage de fichiers, vous pouvez mettre à jour les paramètres suivants :

- Capacité ou taille.
- Paramètre en ligne ou hors ligne.
- Règles d'efficacité du stockage.
- Niveau de service de performances.
- Les paramètres de la liste de contrôle d'accès (ACL).

- Paramètres des export-policy. Vous pouvez également supprimer des paramètres d'export policy et rétablir les règles d'export policy par défaut (vides) sur le partage de fichiers.

Lors d'une exécution d'API unique, vous ne pouvez mettre à jour qu'un paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performances à un partage de fichiers. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété de partage de fichiers.

1. Procurez-vous la clé de partage de fichiers CIFS ou NFS du partage de fichiers à mettre à jour. Elle interroge tous les partages de fichiers sur votre data Center. Ignorez cette étape si vous connaissez déjà la clé de partage de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares`

2. Affichez les détails du partage de fichiers en exécutant l'API suivante avec la clé de partage de fichiers obtenue.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares/{key}`

   Affichez les détails du partage de fichiers dans la sortie.

```
"assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Obtenez la clé du niveau de service de performances que vous souhaitez attribuer à ce partage de fichiers. Aucune stratégie n'est actuellement attribuée à cette règle.

Catégorie	Verbe HTTP	Chemin
Niveaux de services de performances	OBTENEZ	`/storage-provider/performance-service-levels`

Pour récupérer les détails des niveaux de service de performances définis par le système, définissez le paramètre `system_defined` saisissez le paramètre à `true`. À partir de la sortie, procurez-vous la clé du niveau de service de performances que vous souhaitez appliquer au partage de fichiers.

4. Appliquez le niveau de service Performance sur le partage de fichiers.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares/{key}`

Dans l'entrée, vous devez spécifier uniquement le paramètre que vous souhaitez mettre à jour, avec la clé de partage de fichiers. Dans ce cas, c'est la clé du niveau de service de performance.

CURL d'échantillon

```
curl -X POST "https://<hostname>/api/storage-provider/file-shares"`-H
"accept: application/json" -H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{
\"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" },
}"
```

La sortie JSON affiche un objet Job que vous pouvez utiliser pour vérifier si les terminaux d'accès des nœuds home et Partner ont été créés correctement.

5. Vérifiez si le niveau de service de performances a été ajouté au partage de fichiers à l'aide de la clé d'objet travail affichée dans votre sortie.

Catégorie	Verbe HTTP	Chemin
Serveur de gestion	OBTENEZ	`/management-server/jobs/{key}`

Si vous effectuez une requête en fonction de l'ID de l'objet travail, vous voyez si le partage de fichiers a été mis à jour avec succès. En cas de défaillance, dépannez la panne et exécutez de nouveau l'API. Lors de la création réussie, interroger le partage de fichiers pour voir l'objet modifié :

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares/{key}`

Affichez les détails du partage de fichiers dans la sortie.

```
"assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
        }
```

Mise à jour des LUN

Lors de la mise à jour d'une LUN, vous pouvez modifier les paramètres suivants :

- Capacité ou taille
- Paramètre en ligne ou hors ligne
- Règles d'efficacité du stockage
- Niveau de service de performances
- Mappage de LUN

Lors d'une exécution d'API unique, vous ne pouvez mettre à jour qu'un paramètre.

Cette procédure décrit l'ajout d'un niveau de service de performances à une LUN. Vous pouvez utiliser la même procédure pour mettre à jour toute autre propriété de LUN.

1. Procurez-vous la clé LUN du LUN que vous souhaitez mettre à jour. Cette API renvoie les détails de toutes LES LUN de votre data Center. Ignorez cette étape si vous connaissez déjà la clé LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns`

2. Afficher les détails de la LUN en exécutant l'API suivante avec la clé de LUN obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Pour afficher les détails de la LUN dans le résultat de la commande. Vous pouvez voir qu'aucun niveau de service de performances n'est attribué à cette LUN.

Sortie JSON échantillon

```
  "assigned_performance_service_level": {
        "key": null,
        "name": "Unassigned",
        "peak_iops": null,
        "expected_iops": null,
        "_links": {}
      },
```

3. Obtenez la clé du niveau de service de performances que vous souhaitez attribuer à la LUN.

Catégorie	Verbe HTTP	Chemin
Niveaux de services de performances	OBTENEZ	`/storage-provider/performance-service-levels`

> Pour récupérer les détails des niveaux de service de performances définis par le système, définissez le paramètre `system_defined` saisissez le paramètre à `true`. Dans le résultat de cette commande, vous devez obtenir la clé du niveau de service de performances que vous souhaitez appliquer sur le LUN.

4. Appliquez le niveau de service de performances sur la LUN.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	CORRECTIF	`/storage-provider/lun/{key}`

Dans l'entrée, vous devez spécifier uniquement le paramètre à mettre à jour et la clé LUN. Dans ce cas, c'est la clé du niveau de service de performances.

CURL d'échantillon

```
curl -X PATCH "https://<hostname>/api/storage-provider/luns/7d5a59b3-
953a-11e8-8857-00a098dcc959" -H "accept: application/json" -H "Content-
Type: application/json" H "Authorization: Basic
<Base64EncodedCredentials>" -d
"{ \"performance_service_level\": { \"key\": \"1251e51b-069f-11ea-980d-
fa163e82bbf2\" }"
```

La sortie JSON affiche une clé d'objet tâche que vous pouvez utiliser pour vérifier la LUN que vous avez mise à jour.

5. Afficher les détails de la LUN en exécutant l'API suivante avec la clé de LUN obtenue.

Catégorie	Verbe HTTP	Chemin
Fournisseur de stockage	OBTENEZ	`/storage-provider/luns/{key}`

Pour afficher les détails de la LUN dans le résultat de la commande. Vous pouvez voir que le niveau de service performances est attribué à cette LUN.

Sortie JSON échantillon

```
     "assigned_performance_service_level": {
        "key": "1251e51b-069f-11ea-980d-fa163e82bbf2",
        "name": "Value",
        "peak_iops": 75,
        "expected_iops": 75,
        "_links": {
            "self": {
                "href": "/api/storage-provider/performance-service-
levels/1251e51b-069f-11ea-980d-fa163e82bbf2"
            }
```

Modification d'un partage de fichiers NFS pour prendre en charge CIFS

Vous pouvez modifier un partage de fichiers NFS pour prendre en charge le protocole CIFS. Lors de la création de partages de fichiers, il est possible de spécifier à la fois les paramètres de listes de contrôle d'accès (ACL) et les règles d'export policy pour le même partage de fichiers. Toutefois, si vous souhaitez activer CIFS sur le même volume que celui sur lequel vous avez créé un partage de fichiers NFS, vous pouvez mettre à jour les paramètres ACL sur ce partage de fichiers pour prendre en charge CIFS.

Ce dont vous aurez besoin

1. Un partage de fichiers NFS doit avoir été créé avec uniquement les détails de la export policy. Pour plus d'informations, reportez-vous aux sections *gestion des partages de fichiers* et *modification des charges de travail du stockage*.
2. Vous devez disposer de la clé de partage de fichiers pour exécuter cette opération. Pour plus d'informations sur l'affichage des détails du partage de fichiers et la récupération de la clé de partage de fichiers à l'aide de l'ID de tâche, voir *Provisioning des partages de fichiers CIFS et NFS*.

Cette fonctionnalité s'applique à un partage de fichiers NFS que vous avez créé en ajoutant uniquement des règles d'export policy et non des paramètres ACL. Vous modifiez le partage de fichiers NFS pour inclure les paramètres ACL.

Étapes

1. Sur le partage de fichiers NFS, exécutez une `PATCH` Fonctionnement avec les détails de la liste de contrôle d'accès pour autoriser l'accès CIFS.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	CORRECTIF	`/storage-provider/file-shares`

CURL d'échantillon

En fonction des privilèges d'accès que vous attribuez au groupe d'utilisateurs, comme indiqué dans l'exemple suivant, une liste de contrôle d'accès est créée et attribuée au partage de fichiers.

```
{
  "access_control": {
    "acl": [
      {
        "permission": "read",
        "user_or_group": "everyone"
      }
    ],
    "active_directory_mapping": {
      "key": "3b648c1b-d965-03b7-20da-61b791a6263c"
    }
```

Sortie JSON échantillon

L'opération renvoie l'ID du travail qui exécute la mise à jour.

2. Vérifiez si les paramètres ont été correctement ajoutés en interrogeant les détails du partage de fichiers pour le même partage de fichiers.

Catégorie	Verbe HTTP	Chemin
fournisseur de stockage	OBTENEZ	`/storage-provider/file-shares/{key}`

Sortie JSON échantillon

```
"access_control": {
        "acl": [
            {
                "user_or_group": "everyone",
                "permission": "read"
            }
        ],
        "export_policy": {
            "id": 1460288880641,
            "key": "7d5a59b3-953a-11e8-8857-
```

```
00a098dcc959:type=export_policy,uuid=1460288880641",
            "name": "default",
            "rules": [
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 1,
                    "protocols": [
                        "nfs3",
                        "nfs4"
                    ],
                    "ro_rule": [
                        "sys"
                    ],
                    "rw_rule": [
                        "sys"
                    ],
                    "superuser": [
                        "none"
                    ]
                },
                {
                    "anonymous_user": "65534",
                    "clients": [
                        {
                            "match": "0.0.0.0/0"
                        }
                    ],
                    "index": 2,
                    "protocols": [
                        "cifs"
                    ],
                    "ro_rule": [
                        "ntlm"
                    ],
                    "rw_rule": [
                        "ntlm"
                    ],
                    "superuser": [
                        "none"
                    ]
                }
```

```
            ],
            "_links": {
                "self": {
                    "href": "/api/datacenter/protocols/nfs/export-
policies/7d5a59b3-953a-11e8-8857-
00a098dcc959:type=export_policy,uuid=1460288880641"
                }
            }
        }
    },
    "_links": {
        "self": {
            "href": "/api/storage-provider/file-shares/7d5a59b3-953a-
11e8-8857-00a098dcc959:type=volume,uuid=e581c23a-1037-11ea-ac5a-
00a098dcc6b6"
        }
    }
```

Vous pouvez voir la liste de contrôle d’accès attribuée ainsi que l’export policy vers le même partage de fichiers.

Informations sur le copyright

Copyright © 2025 NetApp, Inc. Tous droits réservés. Imprimé aux États-Unis. Aucune partie de ce document protégé par copyright ne peut être reproduite sous quelque forme que ce soit ou selon quelque méthode que ce soit (graphique, électronique ou mécanique, notamment par photocopie, enregistrement ou stockage dans un système de récupération électronique) sans l'autorisation écrite préalable du détenteur du droit de copyright.

Les logiciels dérivés des éléments NetApp protégés par copyright sont soumis à la licence et à l'avis de non-responsabilité suivants :

CE LOGICIEL EST FOURNI PAR NETAPP « EN L'ÉTAT » ET SANS GARANTIES EXPRESSES OU TACITES, Y COMPRIS LES GARANTIES TACITES DE QUALITÉ MARCHANDE ET D'ADÉQUATION À UN USAGE PARTICULIER, QUI SONT EXCLUES PAR LES PRÉSENTES. EN AUCUN CAS NETAPP NE SERA TENU POUR RESPONSABLE DE DOMMAGES DIRECTS, INDIRECTS, ACCESSOIRES, PARTICULIERS OU EXEMPLAIRES (Y COMPRIS L'ACHAT DE BIENS ET DE SERVICES DE SUBSTITUTION, LA PERTE DE JOUISSANCE, DE DONNÉES OU DE PROFITS, OU L'INTERRUPTION D'ACTIVITÉ), QUELLES QU'EN SOIENT LA CAUSE ET LA DOCTRINE DE RESPONSABILITÉ, QU'IL S'AGISSE DE RESPONSABILITÉ CONTRACTUELLE, STRICTE OU DÉLICTUELLE (Y COMPRIS LA NÉGLIGENCE OU AUTRE) DÉCOULANT DE L'UTILISATION DE CE LOGICIEL, MÊME SI LA SOCIÉTÉ A ÉTÉ INFORMÉE DE LA POSSIBILITÉ DE TELS DOMMAGES.

NetApp se réserve le droit de modifier les produits décrits dans le présent document à tout moment et sans préavis. NetApp décline toute responsabilité découlant de l'utilisation des produits décrits dans le présent document, sauf accord explicite écrit de NetApp. L'utilisation ou l'achat de ce produit ne concède pas de licence dans le cadre de droits de brevet, de droits de marque commerciale ou de tout autre droit de propriété intellectuelle de NetApp.

Le produit décrit dans ce manuel peut être protégé par un ou plusieurs brevets américains, étrangers ou par une demande en attente.

LÉGENDE DE RESTRICTION DES DROITS : L'utilisation, la duplication ou la divulgation par le gouvernement sont sujettes aux restrictions énoncées dans le sous-paragraphe (b)(3) de la clause Rights in Technical Data-Noncommercial Items du DFARS 252.227-7013 (février 2014) et du FAR 52.227-19 (décembre 2007).

Les données contenues dans les présentes se rapportent à un produit et/ou service commercial (tel que défini par la clause FAR 2.101). Il s'agit de données propriétaires de NetApp, Inc. Toutes les données techniques et tous les logiciels fournis par NetApp en vertu du présent Accord sont à caractère commercial et ont été exclusivement développés à l'aide de fonds privés. Le gouvernement des États-Unis dispose d'une licence limitée irrévocable, non exclusive, non cessible, non transférable et mondiale. Cette licence lui permet d'utiliser uniquement les données relatives au contrat du gouvernement des États-Unis d'après lequel les données lui ont été fournies ou celles qui sont nécessaires à son exécution. Sauf dispositions contraires énoncées dans les présentes, l'utilisation, la divulgation, la reproduction, la modification, l'exécution, l'affichage des données sont interdits sans avoir obtenu le consentement écrit préalable de NetApp, Inc. Les droits de licences du Département de la Défense du gouvernement des États-Unis se limitent aux droits identifiés par la clause 252.227-7015(b) du DFARS (février 2014).

Informations sur les marques commerciales

NETAPP, le logo NETAPP et les marques citées sur le site http://www.netapp.com/TM sont des marques déposées ou des marques commerciales de NetApp, Inc. Les autres noms de marques et de produits sont des marques commerciales de leurs propriétaires respectifs.