Guide de référence de Veritas NetBackup™ WebSocket Service (NBWSS)

Version 8.0

VERITAS™

Guide de référence de Veritas NetBackup™ WebSocket Service (NBWSS)

Mentions légales

Veritas Technologies LLC
500 E Middlefield Road
Mountain View, CA 94043

http://www.veritas.com

.

Support technique

Le support technique entretient globalement les centres de support. Tous les services de support sont fournis conformément à votre contrat de support et à les politiques de support technique en vigueur dans l'entreprise à ce moment. Pour plus d'informations sur les offres de support et comment contacter le support technique, rendez-vous sur notre site web :

https://www.veritas.com/support

Vous pouvez gérer les informations de votre compte Veritas à l'adresse URL suivante :

https://my.veritas.com

Si vous avez des questions concernant un contrat de support existant, envoyez un message électronique à l'équipe d'administration du contrat de support de votre région :

Dans le monde entier (sauf le Japon)	CustomerCare@veritas.com
Japon	CustomerCare_Japan@veritas.com

Documentation

Assurez-vous que vous utilisez la version actuelle de la documentation. Chaque document affiche la date de la dernière mise à jour sur la page 2. La documentation la plus récente est disponible sur le site web de Veritas :

https://sort.veritas.com/documents

Commentaires sur la documentation

Vos commentaires sont importants pour nous. Suggérez des améliorations ou rapportez des erreurs ou omissions dans la documentation. Indiquez le titre et la version du document, le titre du chapitre et le titre de la section du texte que vous souhaitez commenter. Envoyez le commentaire à :

NB.docs@veritas.com

Vous pouvez également voir des informations sur la documentation ou poser une question sur le site de la communauté Veritas :

http://www.veritas.com/community/

Services and Operations Readiness Tools (SORT) de Veritas

Les Services and Operations Readiness Tools (SORT) de Veritas est un site web qui fournit de l'information et des outils pour automatiser et simplifier certaines tâches administratives

qui prennent du temps. Selon le produit, SORT vous aide à préparer les installations et les mises à jour, à identifier les risques dans votre datacenter et à améliorer l'efficacité opérationnelle. Pour voir quels services et quels outils SORT fournit pour votre produit, voyez la fiche de données :

https://sort.veritas.com/data/support/SORT_Data_Sheet.pdf

Table des matières

Chapitre 1 Utilisation de NetBackup WebSocket Service (NBWSS) pour la communication avec une application cloud 7

A propos du NetBackup WebSocket Service (NBWSS) 7
Présentation de la tâche de configuration de la communication NBWSS 9
Remarques sur les connexions de NetBackup aux applications cloud 10
Formats de message NBWSS 11
Appels d'API sur NBWSS 14
Notifications de NBWSS 15
Exemples de messages NBWSS 18
NetBackup demande une connexion au terminal client 18
L'application cloud demande d'effectuer un appel REST API 19
Messages de notification de NetBackup pour un travail de sauvegarde 21
Autres messages de notification NetBackup 26

Chapitre 2 Configuration des terminaux client WebSocket pour NBWSS 30

A propos des connexions de NetBackup aux terminaux client WebSocket 30
Informations du terminal client WebSocket et son formatage 31
Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket 35
Boîte de dialogue de Serveur WebSocket 39
Suppression des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket 41
Configuration des propriétés de NetBackup WebSocket Service (NBWSS) 42
Démarrage d'une connexion de NetBackup à une application cloud 45

Chapitre 3 Dépannage NBWSS 47

Consignation de NBWSS 47
Problèmes NBWSS 48
Des problèmes de validation du serveur de terminal client dans la boîte de dialogue WebSocket Server 48
Problèmes d'enregistrement des informations d'authentification dans la boîte de dialogue Serveur WebSocket 50
Problèmes de suppression de terminal client du serveur WebSocket à partir de NetBackup 51
Problèmes d'affichage de la liste des serveurs WebSocket qui ont été ajoutées dans NetBackup 52
Problèmes d'activation ou de désactivation du serveur de terminal client 53
Problèmes NBWSS supplémentaires 53

Chapitre 1

Utilisation de NetBackup WebSocket Service (NBWSS) pour la communication avec une application cloud

Ce chapitre traite des sujets suivants :

- A propos du NetBackup WebSocket Service (NBWSS)
- Présentation de la tâche de configuration de la communication NBWSS
- Remarques sur les connexions de NetBackup aux applications cloud
- Formats de message NBWSS
- Appels d'API sur NBWSS
- Notifications de NBWSS
- Exemples de messages NBWSS

A propos du NetBackup WebSocket Service (NBWSS)

Veritas fournit un NetBackup WebSocket Service (NBWSS) qui permet aux applications dans le cloud de communiquer avec un serveur maître NetBackup qui

se trouve derrière un pare-feu. NBWSS utilise le protocole WebSocket pour créer une connexion sécurisée au serveur de l'application dans le cloud. Sur cette connexion, l'application peut interagir avec NetBackup en appelant REST API et peut recevoir des notifications de NetBackup.

NetBackup communique avec l'application basée sur le cloud via une interface Web que l'application cloud rend disponible. Cette interface est appelée terminal client WebSocket. Lorsqu'il existe une connexion entre NetBackup et les terminaux client de l'application cloud, l'application peut utiliser les messages NBWSS pour guider NetBackup à effectuer des services de protection des données.

Figure 1-1 Présentation de NBWSS

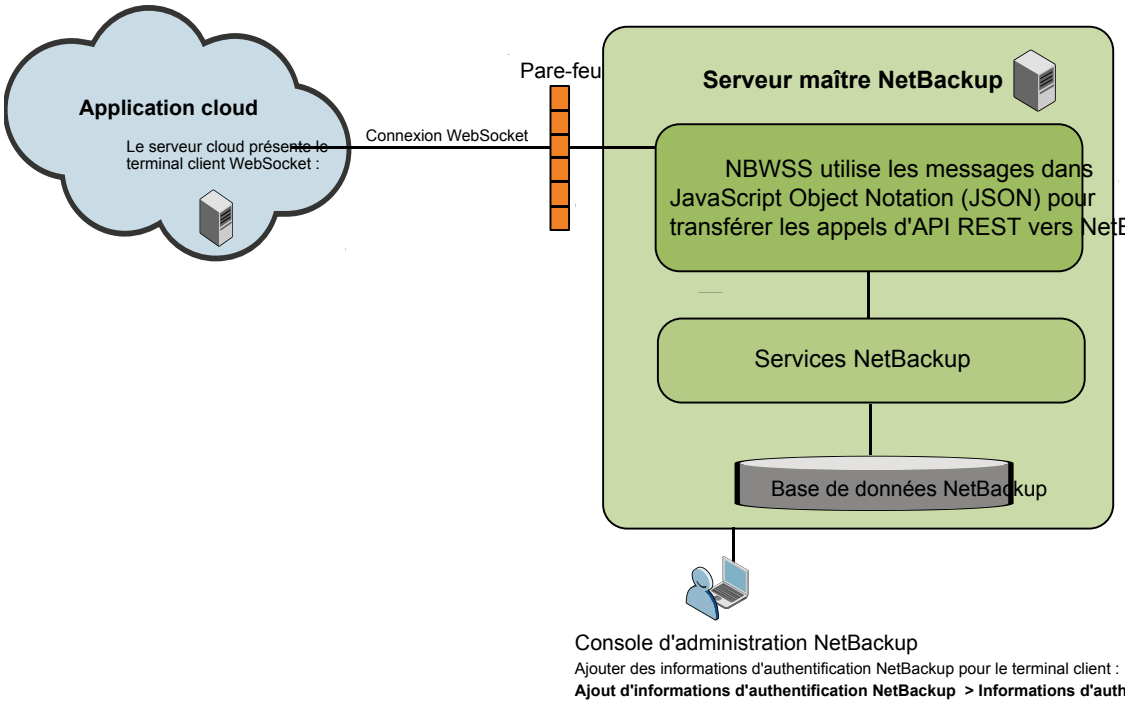


Tableau 1-1 répertorie les phases dans le processus de communication NBWSS.

Tableau 1-1 Processus de communication NBWSS

Phase	Description
Phase 1	Avec ses informations d'authentification de terminal client, NetBackup envoie une demande de connexion à l'application cloud. Par exemple : Se reporter à "NetBackup demande une connexion au terminal client" à la page 18.
Phase 2	L'application cloud lit la demande de connexion et envoie à NetBackup une réponse. Par exemple : Se reporter à "NetBackup demande une connexion au terminal client" à la page 18.
Phase 3	Lorsqu'une connexion est établie, le composant NBWSS de l'application cloud peut appeler les NetBackup API pour effectuer des services de protection des données (par exemple, la sauvegarde ou la restauration). L'application cloud doit également interpréter chaque réponse à partir de NetBackup. Par exemple : Se reporter à "L'application cloud demande d'effectuer un appel REST API" à la page 19. Se reporter à "Remarques sur les connexions de NetBackup aux applications cloud" à la page 10.
Phase 4	NetBackup envoie des notifications à l'application cloud concernant les images de sauvegarde (création, mise à jour, suppression) et de travaux (de début et de fin). L'application cloud interprète et reconnaît les notifications. Par exemple : Se reporter à "Messages de notification de NetBackup pour un travail de sauvegarde" à la page 21. Se reporter à "Notifications de NBWSS" à la page 15.

Présentation de la tâche de configuration de la communication NBWSS

Tableau 1-2 répertorie les tâches de configuration de communication NetBackup à l'aide d'une application basée sur le cloud.

Tableau 1-2 Configuration de la communication NBWSS entre NetBackup et une application basée sur le cloud

Ordre	Tâches
Tâche 1	Le fournisseur de services développe un composant de l'application cloud qui communique avec NetBackup au moyen de messages NBWSS. Pour plus d'informations, consultez les rubriques suivantes : Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.
Tâche 2	Le fournisseur de services envoie des détails du terminal client WebSocket de l'application cloud à l'administrateur NetBackup.
Tâche 3	Pour ajouter le terminal client à NetBackup, l'administrateur NetBackup enregistre les détails du terminal client en tant qu'informations d'authentification d'accès. Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.
Tâche 4	L'administrateur NetBackup peut régler les propriétés de NBWSS. Par exemple, vous pouvez modifier l'intervalle de temps auquel NetBackup démarre une nouvelle connexion à une application cloud. Se reporter à "Configuration des propriétés de NetBackup WebSocket Service (NBWSS)" à la page 42. Se reporter à "Démarrage d'une connexion de NetBackup à une application cloud" à la page 45.

Remarques sur les connexions de NetBackup aux applications cloud

NBWSS utilise les règles suivantes pour établir une connexion à un terminal client :

- S'il n'existe aucune connexion active à un terminal client dans un groupe de serveurs, NetBackup tente de se connecter au terminal client qui a la priorité la plus élevée.
- S'il est impossible de se connecter à un terminal client au sein d'un groupe de serveurs (le serveur est arrêté), NetBackup tente de se connecter au terminal client qui a la priorité le plus élevée suivante dans ce groupe de serveurs.

Notez ces règles supplémentaires et limitations :

- Au maximum une connexion peut exister par terminal client à la fois.
- Au maximum une connexion peut exister par groupe de serveurs à la fois.
- NBWSS ne ferme pas automatiquement une connexion existante lorsqu'une connexion de priorité plus élevée est en ligne. Par exemple, supposons que ce groupe de serveurs `sg1` a deux terminaux client (`ep1` et `ep2`) avec des priorités de 1 et 2, respectivement. Si NBWSS est actuellement connecté à `ep2` (priorité

2) et `ep1` (priorité 1) est en ligne, NBWSS ne se connecte pas automatiquement à `ep1`. L'application cloud doit fermer la connexion à `ep2` avant que NBWSS ne tente de se connecter à `ep1`.

- Un processus de connexion s'exécute sur un minuteur qui répond aux modifications de connexion de terminal client (comme pour la connexion aux nouveaux terminaux client ou la déconnexion à partir de terminaux client supprimés). La durée par défaut pour cette tâche est de 60 secondes. Par conséquent, cela peut prendre jusqu'à 1 minute avant que les modifications du terminal client n'entrent en vigueur.
  Vous pouvez utiliser la propriété `connectionInfo.period` pour configurer cette tâche.
  Se reporter à "Configuration des propriétés de NetBackup WebSocket Service (NBWSS)" à la page 42.
- Lorsque le service de la console de gestion Web NetBackup est redémarré, le serveur web de NetBackup prend quelques minutes pour démarrer. En conséquence, les terminaux client actuellement configurés s'affichent après quelques minutes dans la console d'administration NetBackup. Les terminaux client s'affichent sous **Gestion des médias et des périphériques > Informations d'authentification > serveurs WebSocket**.
- Une connexion établie ne dispose pas de limite de temps ; la connexion peut exister indéfiniment. Dans certains cas, la connexion devra peut-être être ré-établies, comme lorsque le jeton que NetBackup envoie à l'application cloud a expiré. Dans ce cas, les informations d'authentification de NetBackup pour le terminal client doivent être à nouveau ajoutées avec un nouveau jeton valide. La connexion est rétablie à la prochaine exécution du processus de connexion (déterminée par la propriété `connectionInfo.period`).

Formats de message NBWSS

Pour communiquer avec les terminaux client WebSocket, le NetBackup WebSocket Service (NBWSS) utilise son propre format de message avec la JavaScript Object Notation (JSON). Le format JSON permet à NBWSS et aux applications sur les terminaux client d'effectuer le suivi des messages par ID et de déterminer leur type et sous-type.

Les messages fonctionnent sous forme de demande et de réponse : chaque demande a une réponse associée.

Voici ci-dessous un exemple d'une demande de connexion NBWSS :

```
{
      "version": "1.0",
```

```
        "id": "0CEAB6C2-0BBF-4F60-974D-C1F3EF39B872",
        "type": "CONNECT",
        "subType": "REQUEST",
        "timeStamp": 1444944181,
        "payload": {
              "token": "qwerrtrtrtrt2234344==="
        }
}
```

Un exemple de réponse d'une application :

```
{
        "version": "1.0",
        "id": "0CEAB6C2-0BBF-4F60-974D-C1F3EF39B872",
        "type": "CONNECT",
        "subType": "RESPONSE",
        "timeStamp": 1444944191,
        "payload": {
              "valid": true
        }
}
```

Veuillez prendre en compte les éléments suivants :

- Le message commence par une accolade gauche ({}) et se termine par une accolade droite (}).
- La réponse doit avoir la même valeur pour « `id` » que pour la demande.
- Les entrées se composent de paires `clé : valeur` qui sont séparées par une virgule.
- Le message comprend une `charge utile`. Pour les messages de type `SE CONNECTER` ou `COMMANDE`, la charge utile contient un *objet* entre les accolades {}. Pour les messages de type `NOTIFICATION`, la charge utile contient une *baie de disques* entre les crochets [].
- Pour la tâche de fond sur le formatage JSON, consultez la note de groupe de travail réseau sur JavaScript Object Notation : http://www.ietf.org/rfc/rfc4627.txt?number=4627

Tableau 1-3 décrit les champs dans les messages NBWSS.

Tableau 1-3 Champs de message NBWSS

Clé	Description
`version:`	La version du message. Dans cette version, la version disponible est `1.0`.
`id:`	Un identificateur unique pour le message. Quand NBWSS envoie un message de demande, un UUID est généré et est inséré dans ce champ. Lorsque l'application au niveau des terminaux client répond avec un message de réponse, NBWSS attend la réponse pour contenir le même ID que le message de demande. L'ID permet à NBWSS de mapper le message de demande pour le message de réponse. Quand NBWSS reçoit un message de demande, son message de réponse contient le même ID que le message de demande. L'ID permet à l'application de terminal client de mapper la demande pour la réponse si nécessaire.
`type :`	Le type de message. Les types disponibles sont : ■ `CONNEXION` Pour demander une connexion à un terminal client. ■ `COMMANDE` Pour demander l'exécution d'un appel de REST API. ■ `NOTIFICATION` Pour générer un rapport sur l'état des événements NetBackup, tels que l'état d'un travail de sauvegarde.
`Sous-type :`	Le sous-type du message. Les sous-types disponibles sont `DEMANDE` ou `RÉPONSE`.
`horodatage :`	Une représentation numérique de la durée de l'époque UNIX (en secondes) lorsque le message est envoyé.
`charge utile :`	Le corps du message. Le corps du message varie en fonction du type et du sous-type du message. Les rubriques suivantes incluent de plus amples détails et exemples : Se reporter à "Appels d'API sur NBWSS" à la page 14. Se reporter à "Notifications de NBWSS" à la page 15. Se reporter à "Exemples de messages NBWSS" à la page 18.

Appels d'API sur NBWSS

Le NetBackup WebSocket Service (NBWSS) permet à une application basée sur le cloud d'effectuer des appels REST API vers NetBackup via une connexion sécurisée. L'application cloud envoie des messages à NBWSS en JavaScript Object Notation (JSON). Les messages en JSON contiennent l'appel REST API que l'application cloud veut exécuter. Ensuite, NBWSS passe l'appel d'API au nom de l'application cloud et renvoie une réponse à l'application.

Ce qui suit est un exemple de demande pour effectuer un appel NetBackup REST API :

```
{
      "version": "1.0",
      "id": "9CD2B69F-0BBF-3F60-974D-C1F2EF37B872",
      "type": "COMMAND",
      "subType": "REQUEST",
      "timeStamp": 1444806222,
      "payload": {
            "uri": "/netbackup/config/servers/vmservers/vCenter1.domain
                  .com",
            "method": "GET",
            "headers": {
                  "Content-Type": "application/json"
            }
      }
}
```

Veuillez prendre en compte les éléments suivants :

- Pour passer un appel d'API, le champ `"type"` doit être « `COMMANDE"` et le champ « `Sous-type"` doit être « `DEMANDE"`.
- Le champ « `charge utile"` dépend du type d'API à appeler.
  - Dans cet exemple, le champ `"uri"` contient l'URI de l'appel REST API. NBWSS garantit que le nom et le port de l'hôte sont correctement inclus dans la demande REST complète.
  - Le champ « `méthode"` indique le type d'appel d'API à effectuer. Dans cet exemple, il s'agit de « `OBTENIR"` (une demande pour obtenir des informations sur vCenter1).
  - Le champ « `en-têtes"` contient toutes les en-têtes HTTP à inclure à l'appel d'API. Dans cet exemple, `"Content-Type"` est défini sur `"application/json"`, pour indiquer que la demande est envoyée au format JSON.

Notifications de NBWSS

Lorsque NetBackup est connecté à un terminal client NBWSS, le terminal client reçoit des notifications à partir de NetBackup sous la forme d'un message `NOTIFICATION REQUEST`. Lorsque le terminal client reçoit la notification, le terminal client doit répondre par un message `NOTFICATION RESPONSE`.

Tableau 1-4 décrit les types de notifications que NetBackup envoie.

Tableau 1-4 Types de notification de NetBackup

Types de notification	Description
Notifications de travail NetBackup	Quand un travail démarre, NetBackup envoie une notification de l'état actuel du travail : `"QUEUED"`, `"ACTIVE"`, ou `"DONE"`. Notez que NetBackup interroge à propos de l'état du travail de manière régulière. Quand un travail se termine, NetBackup envoie une notification indiquant que l'état du travail est `"DONE"`. NetBackup émet cette notification, si le travail a réussi ou a échoué.
Notifications d'image de sauvegarde de NetBackup	Quand NetBackup crée une image de sauvegarde, il émet une notification selon laquelle l'état de l'image est `"CREATE"` ou `"UPDATE"`. Quand une image de sauvegarde est mise à jour, NetBackup envoie une notification selon laquelle l'état de l'image est `"UPDATE"`. Quand une image de sauvegarde est supprimée, NetBackup envoie une notification selon laquelle l'état de l'image est `"DELETE"`. Quand une copie d'image expire, si toutes les copies locales restantes sont des copies de réplique qui ne peuvent pas être restaurées, NetBackup envoie la notification `"NO_LOCAL_COPY_AVAILABLE"`.

Format de message de notification

A. Demande de notification

NetBackup envoie des notifications à un terminal client sous la forme d'un message `NOTIFICATION REQUEST`. Ce message peut avoir une ou plusieurs notifications au sein de sa charge utile.

Ce qui suit est un exemple de demande de notification :

```
{
      "version": "1.0",
      "id": "EDD85CD7-8553-47E4-8A19-01C65092F220",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811679,
```

```
"payload": [
      {
            "notificationType": "INFO",
            "object": "JOB",
            "data": [
                  {
                        "scheduleType": "ST_FULL",
                        "clientName": "mserver2.acme.com",
                        "status": 0,
                        "startTime": 1459829674,
                        "state": "ACTIVE",
                        "policyName": "vmware2",
                        "parentJobId": 144,
                        "jobId": 144,
                        "policyType": "VMWARE",
                        "jobType": "BACKUP"
                  }
            ]
      }
]
}
```

Dans les messages de demande, le type de valeur `"payload"` est une baie de disques. Chaque élément de la baie contient un type d'objet de notification différent (`"JOB"` ou `"IMAGE"`). L'élément a toutes les notifications qui sont liées à ce type d'objet. Cette baie de disques permet à NetBackup de regrouper les notifications d'un même type.

Par exemple, pour début du travail et travail effectué, la charge utile dispose d'un élément : un objet de notification de type `"JOB"`. Dans la section des données de l'objet de notification `"JOB"`, il y a deux éléments, un pour chaque notification. Pour un exemple de notifications par lots dans un seul message, consultez « Plusieurs notifications dans un seul message » dans la rubrique suivante :

Se reporter à "Autres messages de notification NetBackup" à la page 26.

Chaque objet de notification possède les champs suivants :

- `notificationType :`
  Une chaîne qui affiche le type de notification. Dans cette version, le seul type est `"INFO"`.
- `objet :`
  Une chaîne qui affiche l'objet de la notification. Dans cette version, les seuls objets sont `"JOB"` et `"IMAGE"`.

- `données :`

  Une baie de disques qui contient les informations pour chaque type d'objet. Chaque élément de baie de disques de données est une notification séparée. Les champs de la baie de disques de données sont spécifiques à chaque type de notification.

  Se reporter à "Exemples de messages NBWSS" à la page 18.

B. Réponse de notification

Pour chaque demande de notification, un message `NOTIFICATION RESPONSE` est attendu. Le champ `"id"` de cette réponse doit être identique à la `"id"` de la demande et le champ `"payload"` doit être un tableau vide.

Par exemple :

```
{
      "version": "1.0",
      "id": "EDD85CD7-8553-47E4-8A19-01C65092F220",
      "type": "NOTIFICATION",
      "subType": "RESPONSE",
      "timeStamp": 1445036999,
      "payload": []
}
```

Quand NetBackup reçoit la réponse, les notifications qui ont été envoyées au sein de la demande sont considérées comme reconnues et les nouvelles notifications peuvent être envoyées dans le cas où elles se produisent. Si une demande de notification n'est pas reconnue dans le délai configuré, la notification est renvoyée. Aucune nouvelle notification n'est envoyée à ce terminal client jusqu'à ce que la notification soit reconnue.

La période de temps peut être configurée dans le fichier `nbwss.properties` au moyen de l'option `notification.scheduledRate`. La valeur par défaut est de 5 secondes. La rubrique suivante contient plus d'informations sur les options dans le fichier `nbwss.properties` :

Se reporter à "Configuration des propriétés de NetBackup WebSocket Service (NBWSS)" à la page 42.

Garantie de livraison

Pour éviter les problèmes de livraison, NetBackup garantit la livraison de notifications envoyées dans les cas suivants : la connexion entre NetBackup et le terminal client est abandonnée, le serveur du terminal client est hors ligne ou un problème se produit avec les Services Web de NetBackup. Si un serveur de terminal client est hors ligne, les notifications atteignent le serveur du terminal client suivant dans le groupe de serveurs.

Se reporter à "Remarques sur les connexions de NetBackup aux applications cloud" à la page 10.

Exemples de messages NBWSS

Voici des exemples de messages NBWSS et des notifications, avec notes explicatives.

NetBackup demande une connexion au terminal client

A. NetBackup lance la demande de connexion

```
{
      "version": "1.0",
      "id": "0CEAB6C2-0BBF-4F60-974D-C1F3EF39B872",
      "type": "CONNECT",
      "subType": "REQUEST",
      "timeStamp": 1444944181,
      "payload": {
            "token": "qwerrtrtrtrt2234344==="
      }
}
```

Remarques : Dans ce message, le champ `"type"` est `"CONNECT"` et le `"subType"` est `"REQUEST"`. La clé `"token"` contient le jeton de validation d'application qui a été ajouté lors de la configuration du terminal client dans NetBackup. L'application basée sur le cloud valide ce jeton et envoie un message `CONNECT RESPONSE` avec les résultats de la validation (voir l'exemple suivant).

B. Le terminal client répond à la demande de NetBackup

Le `"subType"` est `"RESPONSE"`.

```
{
      "version": "1.0",
      "id": "0CEAB6C2-0BBF-4F60-974D-C1F3EF39B872",
      "type": "CONNECT",
      "subType": "RESPONSE",
      "timeStamp": 1444944191,
      "payload": {
            "valid": true
      }
}
```

Remarques : Si le jeton est validé, l'application réagit avec le champ `"valid"` défini sur `true`. NetBackup tient alors compte de la connexion à établir et les opérations peuvent continuer. Si le jeton n'est pas valide, l'application doit réagir avec `"valid"` défini sur `false`, ce qui entraîne la fermeture de la connexion par NetBackup.

Remarque : La réponse doit toujours avoir le même `"id"` que la demande.

L'application cloud demande d'effectuer un appel REST API

A. L'application cloud demande d'ajouter des informations à NetBackup à propos d'un serveur vCenter (POST)

```
{
      "version": "1.0",
      "id": "99B9BD8C-9E3E-406A-A7EE-33B88531C7D9",
      "type": "COMMAND",
      "subType": "REQUEST",
      "timeStamp": 1444856264,
      "payload": {
            "uri": "/netbackup/config/servers/vmservers",
            "method": "POST",
            "headers": {
                  "Content-Type": "application/json"
                  "Authorization": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1N"
            },
            "parameters": "{\"serverName\": \"vcenterServer1\",
            \"proxyServerName\": \"\",\"vmType\": \"VMWARE_VIRTUAL_
            CENTER_SERVER\",\"userId\": \"administrator\",
            \"password\": \"password@123\",\"port\": 0 }"
      }
}
```

Remarques : La demande et sa réponse doivent toujours la même valeur pour `"id"`.

Le champ `"type"` est `"COMMAND"` et le champ `« Sous-type"` est `"REQUEST"`. La `« méthode »« charge utile »` est `"POST"`, qui ajoute les informations `vcenterServer1` dans NetBackup.

Pour `« Sous-type » "REQUEST"`, les `« En-têtes » :` doivent contenir les éléments suivants :

- `« Type de contenu » : « application/json »` est le formulaire de la demande.

- « Autorisation » est le jeton Web JSON (JWT) qui a été reçu dans une réponse précédente.

Le champ « paramètres » est une chaîne d'échappement JSON : les guillemets doubles autour de chaque valeur (tels que « serverName ») sont échappés avec une barre oblique inverse (\).

B. L'application cloud vous demande de lire des informations sur un serveur vCenter (GET)

```
{
      "version": "1.0",
      "id": "9CD2B89F-0BBF-4F60-974D-C1F3EF39B872",
      "type": "COMMAND",
      "subType": "REQUEST",
      "timeStamp": 1444806222,
      "payload": {
            "uri": "/netbackup/config/servers/vmservers/vCenter2
            .domain.com",
            "method": "GET",
            "headers": {
                  "Content-Type": "application/json"
                  "Authorization": "eyJ0eXAiOiJKV1QiLCJhbGciOiJSUzI1N"
            }
      }
}
```

Remarques : Le champ « type » est "COMMAND" et le champ « Sous-type » est "REQUEST". La « méthode »« charge utile » est "GET", qui lit les informations à propos de vCenter2.domain.com qui sont enregistrées dans NetBackup.

C. NetBackup répond à la demande du terminal client

```
{
      "version": "1.0",
      "id": "9CD2B89F-0BBF-4F60-974D-C1F3EF39B872",
      "type": "COMMAND",
      "subType": "RESPONSE",
      "timeStamp": 1444806444,
      "payload": {
            "headers": {
                  "date": "Thu, 14 Jan 2016 20:58:11 GMT",
                  "cache-control": "private",
                  "server": "Apache-Coyote/1.1",
                  "content-type": "application/json",
```

```
                        "transfer-encoding": "chunked",
                        "expires": "Wed, 31 Dec 1969 16:00:00 PST"
                  },
                  "responseCode": 200,
                  "body": "{\"vmServer\":{\"serverName\":\"vCenter2.domain
                  .com\",\"vmType\":\"VMWARE_VIRTUAL_CENTER_SERVER\",
                  \"userId\":\"root\",\"password\":\"\",\"port\":0},
                  \"links\":[{\"rel\":\"self\",\"href\":\"https://xuanbl5vm9:
                  8443/config/servers/vmservers/vCenter2.domain.com\"}]}"
            }
}
```

Remarques:

La « `charge utile` » contient la réponse HTTP (« `en-têtes` », « `code de réponse` », et « `corps du message` ») que NetBackup a reçu de l'API.

Messages de notification de NetBackup pour un travail de sauvegarde

Les exemples de **A** à **G** sont les notifications qui NetBackup a envoyées à un terminal client pour une sauvegarde à partir d'une politique intelligente VMware.

A. Démarrage d'un travail de sauvegarde parent (découverte)

```
{
      "version": "1.0",
      "id": "EDD85CD7-8555-47E4-8A19-01C35093F220",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811679,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "masterserver2.domain.com",
                              "status": 0,
                              "startTime": 1459829674,
                              "state": "ACTIVE",
                              "policyName": "vmware2",
```

```
                              "parentJobId": 144,
                              "jobId": 144,
                              "policyType": "VMWARE",
                              "jobType": "BACKUP"
                        }
                  ]
            }
      ]
}
```


B. Début du travail de snapshot enfant


```
{
      "version": "1.0",
      "id": "7C0FD14E-089E-46C8-AA2B-344D69AA0C67",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811689,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "DummyTestVM",
                              "status": 0,
                              "startTime": 1459829686,
                              "state": "ACTIVE",
                              "policyName": "vmware2",
                              "parentJobId": 144,
                              "jobId": 145,
                              "policyType": "VMWARE",
                              "jobType": "BACKUP"
                        }
                  ]
            }
      ]
}
```

C. Début du travail de sauvegarde enfant (sauvegarde réelle)


```
{
      "version": "1.0",
      "id": "EF507ECE-4B1C-4D87-AAB0-032ADBC915FC",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811704,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "DummyTestVM",
                              "status": 0,
                              "startTime": 1459829698,
                              "state": "ACTIVE",
                              "policyName": "vmware2",
                              "parentJobId": 145,
                              "jobId": 146,
                              "policyType": "VMWARE",
                              "jobType": "BACKUP"
                        }
                  ]
            }
      ]
}
```


D. Création d’image


```
{
      "version": "1.0",
      "id": "608FE0C1-B03C-421D-8876-E3730A7855AF",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811724,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "IMAGE",
                  "data": [
```

```
                        {
                              "clientType": "VMWARE",
                              "clientName": "DummyTestVM",
                              "backupTime": 1459811698,
                              "createdTime": 1459829720,
                              "operationId": "CREATE",
                              "backupId": "DummyTestVM_1459811698"
                        },
                        {
                              "clientType": "VMWARE",
                              "clientName": "DummyTestVM",
                              "backupTime": 1459811686,
                              "createdTime": 1459829721,
                              "operationId": "UPDATE",
                              "backupId": "DummyTestVM_1459811686"
                        }
                  ]
            }
      ]
}
```


E. travail de sauvegarde complet (travail de sauvegarde réel)


```
{
      "version": "1.0",
      "id": "608FE0C1-B03C-421D-8876-E3730A7855AF",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811724,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "DummyTestVM",
                              "status": 0,
                              "startTime": 1459829698,
                              "state": "DONE",
                              "policyName": "vmware2",
                              "parentJobId": 145,
                              "jobId": 146,
```

```
                                    "policyType": "VMWARE",
                                    "jobType": "BACKUP"
                              }
                        ]
                  }
            ]
}
```

F. Travail de snapshot complet

```
{
      "version": "1.0",
      "id": "F97BAE8F-D1E3-4242-A5EC-FB1C9B8F46E3",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811734,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "DummyTestVM",
                              "status": 0,
                              "startTime": 1459829686,
                              "state": "DONE",
                              "policyName": "vmware2",
                              "parentJobId": 144,
                              "jobId": 145,
                              "policyType": "VMWARE",
                              "jobType": "BACKUP"
                        }
                  ]
            }
      ]
}
```

G. Travail de sauvegarde parent complet

```
{
      "version": "1.0",
      "id": "F97BAE8F-D1E3-4242-A5EC-FB1C9B8F46E3",
      "type": "NOTIFICATION",
```

```
      "subType": "REQUEST",
      "timeStamp": 1459811734,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
                              "scheduleType": "ST_FULL",
                              "clientName": "masterserver2.domain.com",
                              "status": 0,
                              "startTime": 1459829674,
                              "state": "DONE",
                              "policyName": "vmware2",
                              "parentJobId": 144,
                              "jobId": 144,
                              "policyType": "VMWARE",
                              "jobType": "BACKUP"
                        }
                  ]
            }
      ]
}
```


Autres messages de notification NetBackup

Les messages suivants sont les notifications que NetBackup a envoyées à un terminal client pour un travail de restauration et pour la suppression d'image. Le troisième message est un exemple de plusieurs notifications dans un seul message.

Travail de restauration effectué


```
{
      "version": "1.0",
      "id": "8E909940-AD50-4543-8AEA-B52003818925",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459812309,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
                  "data": [
                        {
```

```
                                    "scheduleType": "ST_FULL",
                                    "clientName": "masterserver2.domain.com",
                                    "status": 0,
                                    "startTime": 1459830185,
                                    "state": "DONE",
                                    "policyName": "",
                                    "parentJobId": 147,
                                    "jobId": 147,
                                    "policyType": "STANDARD",
                                    "jobType": "RESTORE"
                              }
                        ]
                  }
      ]
}
```


Suppression d’image


```
{
      "version": "1.0",
      "id": "15AAF7BA-C082-4996-A55D-7C4745D4D1E9",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459814495,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "IMAGE",
                  "data": [
                        {
                              "clientType": "VMWARE",
                              "clientName": "localhost",
                              "backupTime": 1458601200,
                              "createdTime": 1459832492,
                              "operationId": "DELETE",
                              "backupId": "localhost_1458601200"
                        }
                  ]
            }
      ]
}
```


Remarque : Si le serveur maître NetBackup utilise la réplication automatique d’image (AIR), la notification suivante peut être délivrée à propos de la suppression d’image :

```
{
  "version": "1.0",
  "id": "E38DD102-98BC-4590-8E09-85B0A0EA31CE",
  "type": "NOTIFICATION",
  "subType": "REQUEST",
  "timeStamp": 1471471464,
  "payload": [
    {
      "notificationType": "INFO",
      "object": "IMAGE",
      "data": [
        {
          "clientType": "STANDARD",
          "clientName": "localhost",
          "backupTime": 1471469619,
          "createdTime": 1471485862,
          "operationId": "UPDATE",
          "backupId": "localhost_1471469619"
        },
        {
          "clientType": "STANDARD",
          "clientName": "localhost",
          "backupTime": 1471469619,
          "createdTime": 1471485862,
          "operationId": "NO_LOCAL_COPY_AVAILABLE",
          "backupId": "localhost_1471469619"
        }
      ]
    }
  ]
}
```

Plusieurs notifications dans un seul message

```
{
      "version": "1.0",
      "id": "608FE0C1-B03C-421D-8876-E3730A7855AF",
      "type": "NOTIFICATION",
      "subType": "REQUEST",
      "timeStamp": 1459811724,
      "payload": [
            {
                  "notificationType": "INFO",
                  "object": "JOB",
```

```
                "data": [
                        {
                                "scheduleType": "ST_FULL",
                                "clientName": "DummyTestVM",
                                "status": 0,
                                "startTime": 1459829698,
                                "state": "DONE",
                                "policyName": "vmware2",
                                "parentJobId": 145,
                                "jobId": 146,
                                "policyType": "VMWARE",
                                "jobType": "BACKUP"
                        }
                ]
        },
        {
                "notificationType": "INFO",
                "object": "IMAGE",
                "data": [
                        {
                                "clientType": "VMWARE",
                                "clientName": "DummyTestVM",
                                "backupTime": 1459811698,
                                "createdTime": 1459829720,
                                "operationId": "UPDATE",
                                "backupId": "DummyTestVM_1459811698"
                        },
                        {
                                "clientType": "VMWARE",
                                "clientName": "DummyTestVM",
                                "backupTime": 1459811686,
                                "createdTime": 1459829721,
                                "operationId": "UPDATE",
                                "backupId": "DummyTestVM_1459811686"
                        }
                ]
        }
    ]
}
```


La rubrique suivante contient des informations supplémentaires sur les notifications :

Se reporter à "Notifications de NBWSS" à la page 15.

Chapitre 2

Configuration des terminaux client WebSocket pour NBWSS

Ce chapitre traite des sujets suivants :

- A propos des connexions de NetBackup aux terminaux client WebSocket
- Informations du terminal client WebSocket et son formatage
- Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket
- Boîte de dialogue de Serveur WebSocket
- Suppression des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket
- Configuration des propriétés de NetBackup WebSocket Service (NBWSS)
- Démarrage d'une connexion de NetBackup à une application cloud

A propos des connexions de NetBackup aux terminaux client WebSocket

Pour établir une connexion à une application basée sur le cloud, NetBackup communique avec une interface Web que l'application cloud rend disponible. Cette interface est appelée terminal client WebSocket. Pour la connexion, NetBackup nécessite certaines informations sur le terminal client. Tableau 2-1 décrit les étapes pour la préparation de ces informations.

Tableau 2-1 Préparation des informations d'authentification NetBackup pour la connexion à un terminal client d'application cloud

Tâche	Description
Obtenez les informations du terminal client.	Pour les informations du terminal client, contactez le fournisseur de services cloud. La rubrique suivante décrit les informations requises des terminaux client : Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.
Si nécessaire, formatez les informations du terminal client pour NetBackup.	Les informations du terminal client doivent être disponibles pour NetBackup de l'une des manières suivantes : ■ Dans un fichier texte qui utilise JavaScript Object Notation (JSON). ■ Dans une URL que le fournisseur de services génère. NetBackup utilise l'URL pour demander les informations de terminal client. La rubrique suivante décrit comment enregistrer les détails dans un fichier au format JSON : Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.
Enregistrez les informations du terminal client en tant qu'informations d'authentification NetBackup.	Dans la console d'administration NetBackup, utilisez l'option **Gestion des médias et des périphériques > Informations d'authentification > Serveurs WebSocket** pour enregistrer les informations d'authentification NetBackup pour le terminal client de l'application cloud. Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.

Informations du terminal client WebSocket et son formatage

Pour communiquer avec une application basée sur le cloud, NetBackup utilise le protocole WebSocket pour établir une connexion sécurisée avec l'application cloud. NetBackup se connecte à une interface d'application cloud qui est appelée terminal client WebSocket. Pour vous connecter, NetBackup a besoin de certaines informations concernant le terminal client.

Tableau 2-2 décrit les informations qui sont requises pour un terminal client WebSocket.

Tableau 2-2 Entrées qui définissent un terminal client WebSocket

Détails du terminal client	Description
`jeton`	Le jeton de sécurité de l'application cloud. Quand NetBackup lance une connexion à l'application cloud, il envoie le jeton à l'application. L'application valide alors le jeton. Si l'application accepte le jeton, une connexion sécurisée est établie entre NetBackup et l'application. Si l'application n'accepte pas le jeton, la connexion n'est pas établie.
`priorité`	Priorité du terminal client dans son groupe. Un nombre inférieur a priorité plus élevée. La priorité permet à NetBackup de décider de l'ordre de la tentative de connexions pour ce groupe de serveurs. Une seule connexion peut être active par groupe de serveurs.
`groupId`	Un identificateur unique du groupe auquel appartient le terminal client.
`hostname`	Le nom d'hôte ou l'adresse IP du serveur cloud qui contient le terminal client.
`url`	L'URL complète du terminal client WebSocket à laquelle NetBackup se connecte. L'URL WebSocket commence par`wss://` **Remarque :** `ws://`La version n'est pas prise en charge.

IMPORTANT : Il est possible que vous deviez travailler avec le fournisseur de services cloud pour obtenir les informations du terminal client. Les informations du terminal client doivent être disponibles pour NetBackup d'une des manières suivantes :

- Dans un fichier qui est formaté dans JavaScript Object Notation (un fichier JSON). Si le fournisseur de services ne fournit pas les informations du terminal client dans un fichier JSON, vous pouvez vous-même formater les informations dans un fichier JSON.

  Remarque : Les informations du terminal client doivent inclure un jeton de sécurité pour accéder à l'application cloud. Le fournisseur de services doit faire attention d'envoyer le jeton d'application de façon sécurisée.

- Au moyen d'une URL. NetBackup utilise l'URL pour demander les détails du terminal client à partir de l'application cloud.

Remarque : NetBackup ne prend pas en charge une apostrophe (') n'importe où dans les informations du terminal client.

Informations du terminal client WebSocket dans un fichier JSON

L'exemple suivant montre les informations du terminal client WebSocket dans JavaScript Object Notation (JSON) :

```
{
      "token": "security_token...",
      "priority": numeric_value,
      "groupId": "group_ID",
      "hostName": "host_name.domain",
      "url": "wss://host_name.domain:port/uri"
}
```

Veuillez prendre en compte les éléments suivants :

- Dans cette version de NetBackup, chaque fichier JSON doit spécifier un terminal client unique, pas plusieurs terminaux client.
- Le fichier commence par une accolade gauche ({) et se termine par une accolade droite (}).
- Les entrées se composent de `nom : valeur`paires sont séparées par une virgule.
- Chaque chaîne est entre guillemets doubles (" ») excepté la valeur de priorité.
- Les cinq paires `nom : valeur` (`jeton`,`priorité`,`ID de groupe`,`nom d'hôte`,`URL`) peuvent apparaître dans n'importe quel ordre.
- NetBackup ne prend pas en charge une apostrophe (') n'importe où dans le fichier.
- Enregistrez les informations au format JSON comme un fichier texte dans un emplacement auquel le serveur maître NetBackup peut accéder.
- Pour la tâche de fond sur le formatage JSON, consultez la note de groupe de travail réseau sur JavaScript Object Notation : http://www.ietf.org/rfc/rfc4627.txt?number=4627

Ce qui suit est un exemple d'un fichier au format JSON qui définit un terminal client WebSocket :

```
{
      "token": "MIID4TCCAsmgAwIBAgIEBZCDRzANBgkqhkiG9w0BAQsFADBxMQs
DVQQGEwJVUzELMAkGA1UECBMCQ0ExFjAUBgNVBAcTDU1vdW50YWluIFZpZXcx
vzu0n2rWon48ncp6jMjOFiWqMRXnV8Q0vOEpAzUV7Qml92EMV6z0PinAgMBAA
GjgYAwfjBdBgNVHREEVjBUgiJ2b21yaGVsNnU1LXZtMDQuZW5nYmEuc3ltYW
G7IsZ2fTDWKLGxbAG5NNKwEfD11LFhKGwaHkOXYkVi+HVnFEFKK0gxVWg==",
      "priority": 1,
      "groupId": "GROUPID1",
      "hostName": "vrhel6u5-vm4.acme.com",
      "url": "wss://vrhel6u5-vm4.acme.com:14146/cfs/nbufacade"
}
```


Remarques sur l'exemple de fichier JSON :

- Cet exemple commence par le jeton. Le jeton est une chaîne que l'application cloud utilise pour authentifier NetBackup quand NetBackup demande une connexion.

  Attention : Lorsque vous obtenez les informations du terminal client à partir du fournisseur de services, assurez-vous que le jeton est fourni de façon sécurisée.

- L'entrée suivante dans le fichier est la `priorité`, suivie par la `groupID`, le `hostName` et l'`url` du serveur cloud.

Lorsque vous avez le fichier au format JSON, utilisez l'option **FICHIER** sur la boîte de dialogue NetBackup **Serveur WebSocket** pour spécifier ce fichier. NetBackup extrait les informations du terminal client à partir du fichier. Utilisez la procédure suivante :

Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.

Informations du terminal client WebSocket obtenues via le Web

L'application cloud peut générer une URL que NetBackup peut utiliser pour demander les informations du terminal client WebSocket. Utilisez la procédure suivante pour saisir l'URL dans la boîte de dialogue **Serveur WebSocket** de NetBackup :

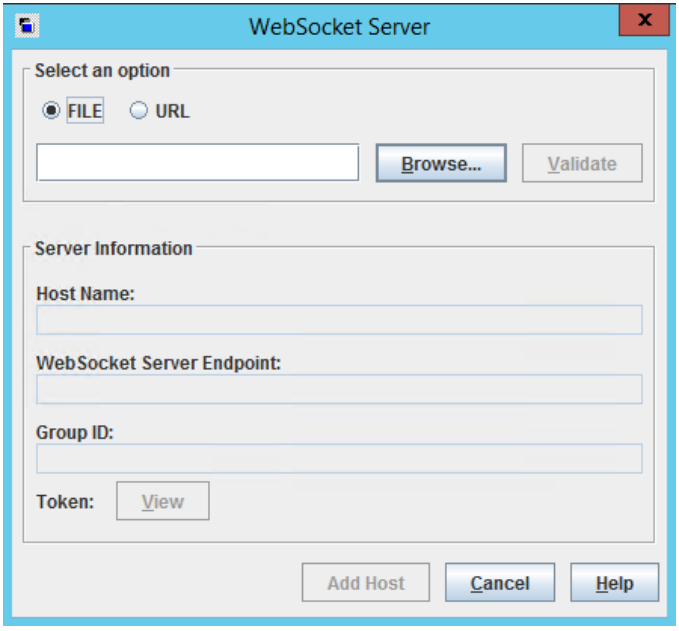
Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.

Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket

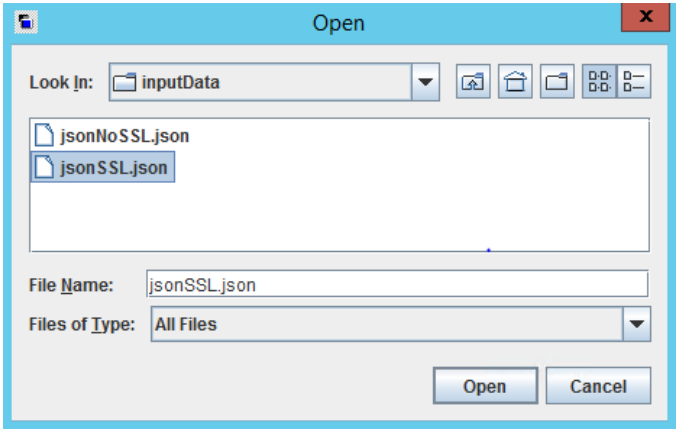
Utilisez la procédure suivante pour sélectionner le fichier JSON ou l'URL de sorte que NetBackup puisse enregistrer les détails du terminal client en tant qu'informations d'authentification.

Pour enregistrer les informations d'authentification de NetBackup pour un terminal client de serveur WebSocket server

1. Dans la console d'administration NetBackup, cliquez sur **Gestion des médias et des périphériques > Informations d'authentification > Serveurs WebSocket**.
2. Cliquez sur **Actions > Nouveau > Nouveau serveur WebSocket**.

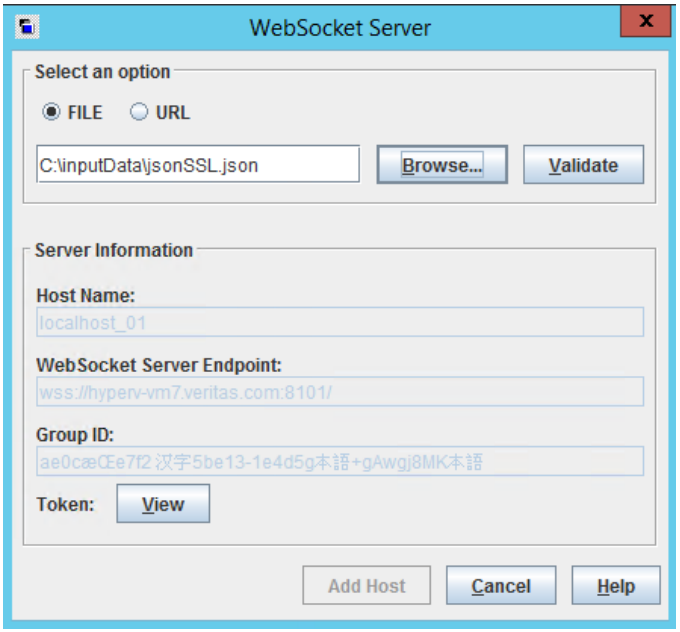


3. Dans la boîte de dialogue **Serveur WebSocket**, sélectionnez la source des informations du terminal client :
   - Pour un fichier au format JSON, cliquez sur **FICHIER**, puis cliquez sur **Parcourir**.



Vous pouvez entrer le chemin complet du fichier dans le champ **Nom de fichier**, ou utilisez le menu déroulant **Regarder dans** ou les icônes de recherche. De gauche à droite, les icônes peuvent monter d'un niveau, accéder au bureau, créer un nouveau dossier ou modifier l'affichage de liste.

Ensuite, cliquez sur le fichier JSON et puis cliquez sur **Ouvrir**. NetBackup extrait les informations du terminal client et les affiche sous **Informations sur le serveur** :



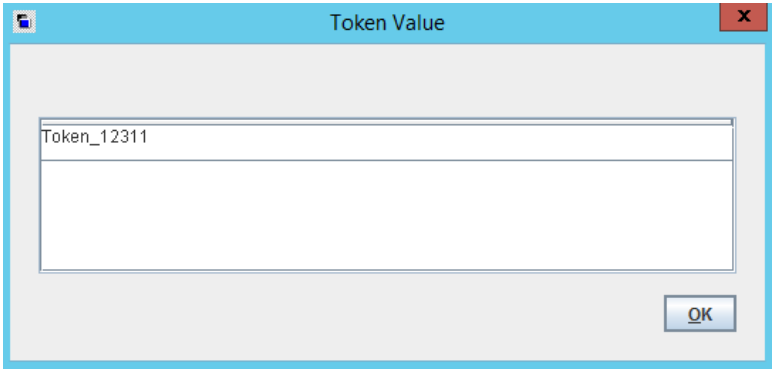
- Pour une URL, cliquez sur **URL** et saisissez l'URL qui contient les informations de terminal client. NetBackup extrait les informations de terminal client à partir de l'URL. (L'application cloud fournit l'URL.)

4 Cliquez sur **Valider**.

NetBackup présente un certificat SSL du serveur du terminal client. Par exemple :

Si vous avez utilisé l'option **URL**, NetBackup extrait les informations du terminal client et les affiche sous **Informations sur le serveur**.

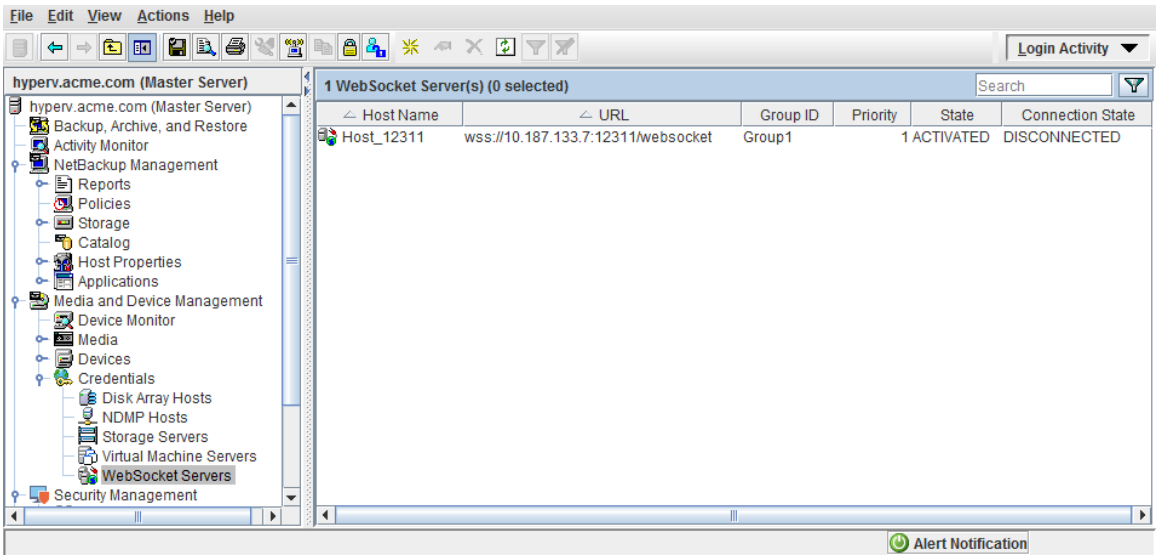
5 Pour consulter un jeton de sécurité de l'application en cloud, cliquez sur **Jeton : affichage**.



6 Pour enregistrer ces informations de terminal client en tant qu'informations d'authentification NetBackup, cliquez sur **Ajouter un hôte**.

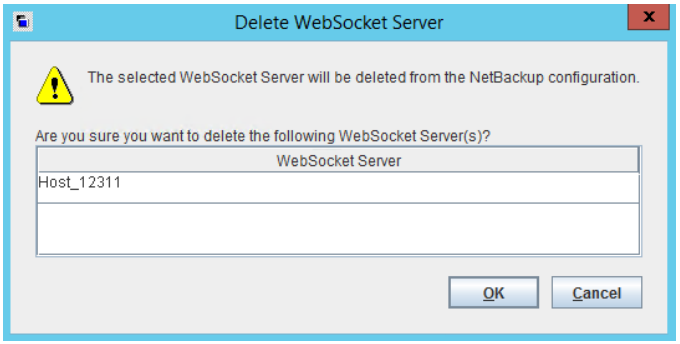
Ce qui suit apparaît :

Le nom d'hôte du terminal client, l'URL, l'ID de groupe, la priorité, l'état (ACTIVÉ ou DÉSACTIVÉ) et l'état de connexion (CONNECTÉ ou DÉCONNECTÉ) apparaissent dans le volet droit sous **Serveur(s) WebSocket**. Le jeton du terminal client est enregistré dans un emplacement sécurisé et n'est pas affiché.



7 Pour supprimer ou désactiver les informations d'authentification du terminal client, cliquez avec le bouton droit de la souris sur les informations d'authentification dans le volet droit. Les options suivantes sont disponibles :

Supprimer Supprime les informations d'authentification du terminal client.



Activer Active les informations d'authentification du terminal client. Lorsque les informations d'authentification sont activées, NBWSS peut se connecter au terminal client.

Se reporter à "Démarrage d'une connexion de NetBackup à une application cloud" à la page 45.

Désactiver Désactive les informations d'authentification du terminal client. Lorsque les informations d'authentification sont désactivées, NBWSS ne se connecte pas au terminal client.

Boîte de dialogue de Serveur WebSocket

Utilisez cette boîte de dialogue pour enregistrer des informations d'authentification NetBackup pour une connexion sécurisée à un serveur d'application dans le cloud. NetBackup utilise les informations d'authentification du serveur pour se connecter à au terminal client WebSocket du serveur cloud.

Pour utiliser cette boîte de dialogue pour enregistrer les informations d'authentification, les informations du terminal client doivent être disponibles d'une des manières suivantes :

- Dans un fichier qui est formaté dans JavaScript Object Notation (un fichier JSON).
- Dans une URL générée par l'application de cloud.

La rubrique suivante contient une procédure pour l'utilisation de cette boîte de dialogue :

Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.

Tableau 2-3 Champs dans la boîte de dialogue **Serveur WebSocket**

Champ	Description
Sélectionnez une option	Sélectionnez l'une des opérations suivantes pour spécifier les informations de terminal client : ■ **FICHIER** : Utilisez cette option pour localiser un fichier au format JSON qui contient les informations du terminal client. **Remarque :** NetBackup extrait les informations du terminal client à partir du fichier et affiche les informations dans cette boîte de dialogue. ■ **URL** : Utilisez cette option pour saisir l'URL qui contient les informations du terminal client. **Remarque :** NetBackup extrait les informations du terminal client à partir de l'URL et affiche ces informations dans cette boîte de dialogue.
Parcourir	Cliquez sur **Parcourir** pour localiser le fichier au format JSON qui contient les informations du terminal client. Utilisez le menu déroulant **Regarder dans** ou les icônes de recherche. De gauche à droite, les icônes peuvent monter d'un niveau, accéder au bureau, créer un nouveau dossier ou modifier l'affichage de liste. Comme alternative, vous pouvez entrer le chemin complet du fichier dans le champ **Nom de fichier**.
Valider	**REQUIS** : Une fois que vous avez sélectionné les informations du terminal client (**FICHIER** or **URL**), cliquez sur **Valider** pour afficher le certificat SSL du terminal client. **Remarque :** Si vous avez saisi une URL pour les informations du terminal client, cliquez sur **Valider** pour extraire les informations et les afficher sous **Informations sur le serveur**.
Informations sur le serveur	Les champs suivants affichent les informations du terminal client que NetBackup a extraites à partir du fichier JSON ou de l'URL.

Champ	Description
Nom d'hôte :	Le nom complet de l'hôte ou de l'adresse IP du serveur cloud qui contient le terminal client. Cette adresse IP ou ce nom d'hôte doit être unique : il ne doit pas s'agir du nom d'hôte ou de l'adresse IP d'un terminal client qui a déjà été ajouté.
Terminal client du serveur WebSocket :	L'URL complète, le port et n'importe quel identifiant supplémentaire du terminal client WebSocket. Exemple de terminal client : `wss://cloudhost7.nebula.com:8080/netbackup/face1` **Remarque :** `ws://` n'est pas pris en charge.
ID du groupe :	Le groupe de serveurs auquel appartient le terminal client.
Jeton : Affichage	Cliquez sur **Affichage** pour afficher le jeton de sécurité que l'application cloud utilise pour valider l'identité de NetBackup.
Ajouter un hôte	Si les informations du terminal client extraites sont correctes, cliquez sur **Ajouter un hôte** pour enregistrer ces informations comme les informations d'authentification du terminal client de NetBackup. À un intervalle configurable, une tâche planifiée recherche les mises à jour des terminaux client dans la base de données NetBackup et agit en conséquence. Cela peut prendre jusqu'à la durée configurée (le paramètre par défaut est de 5 minutes) pour vous connecter après avoir ajouté un terminal client. Se reporter à "Configuration des propriétés de NetBackup WebSocket Service (NBWSS)" à la page 42.

La rubrique suivante décrit les informations du terminal client et son formatage de manière plus détaillée :

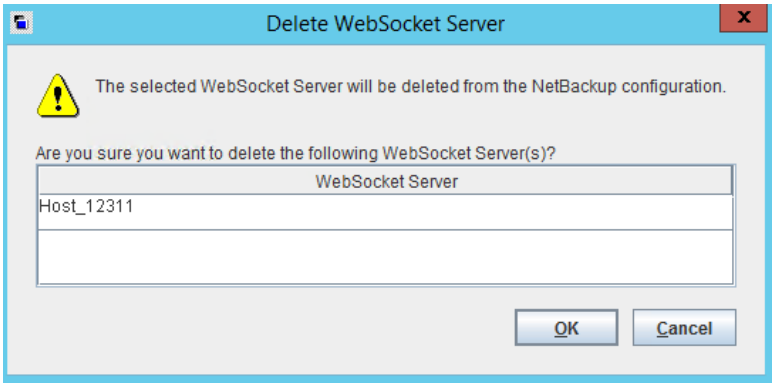
Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

Suppression des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket

Utilisez la procédure suivante pour supprimer les informations d'authentification du terminal client pour une application cloud.

Pour supprimer les informations d'authentification de NetBackup pour un terminal client WebSocket

1. Dans la console d'administration NetBackup, cliquez sur **Gestion des médias et des périphériques > Informations d'authentification > Serveurs WebSocket**.
2. Dans le volet droit, cliquez avec le bouton droit de la souris sur les informations d'authentification du terminal client, sélectionnez **Supprimer** puis cliquez sur **OK** pour confirmer la suppression.



Configuration des propriétés de NetBackup WebSocket Service (NBWSS)

Tableau 2-4 décrit les propriétés configurables de NBWSS et leurs valeurs par défaut. Les propriétés sont dans le fichier texte `nbwss.properties` sur le serveur maître NetBackup. (Pour l'emplacement de ce fichier, consultez la procédure dans cette rubrique.)

Chaque propriété apparaît sur une seule ligne sous la forme suivante :

```
clé=valeur
```

Un exemple de fichier `.properties` est inclus après le tableau. Pour modifier les propriétés, utilisez la procédure à la fin de cette rubrique.

Tableau 2-4 Propriétés configurables de NBWSS

Clés	Description
`exception.ignoreDecoder`	Valeur booléenne Détermine si NBWSS ignore ou pas une exception de décodeur. Une exception de décodeur se produit généralement lorsque NBWSS ne peut pas comprendre un message qu'il reçoit. Le paramètre par défaut est faux : NBWSS ferme la connexion quand une exception de décodeur se produit.
`notification.sendTimeout=`	Nombre entier Détermine combien de temps (en millisecondes) NBWSS attend pour communiquer avec un terminal client (pour envoyer ou recevoir une notification). Par défaut, une tâche de notification attend 2 secondes avant que la tâche se termine. La tâche de notification essaye à nouveau après le délai que la propriété `notification.scheduledRate` définit. Le paramètre par défaut est 2 000 millisecondes (2 secondes). Dans la plupart des cas, Veritas recommande le paramètre par défaut.
`notification.scheduledRate=`	Nombre entier Détermine la fréquence (en secondes) à laquelle NetBackup demande de nouvelles notifications. Cette valeur détermine également combien de temps NetBackup attend pour recevoir un accusé de réception d'une notification avant de renvoyer la notification. La valeur par défaut est de 5 secondes.
`keepAlive.scheduledRate=`	Nombre entier Détermine la fréquence (en secondes) à laquelle NBWSS envoie une commande ping à chaque terminal client en tant qu'élément de ses fonctionnalités de persistance de connexion. Si NetBackup reçoit une commande pong en réponse à chaque commande ping, la connexion du terminal client est toujours valide. La valeur par défaut est de 30 secondes.
`keepAlive.maxPongMissAllowed=`	Nombre entier Détermine combien de pongs (réponses aux commandes ping) peuvent être manqués pour une connexion de terminal client. Lorsque NBWSS envoie une commande ping à un terminal client et que pong n'est pas reçu, il est considéré comme un pong manqué. Quand le maximum est atteint, NBWSS ferme la connexion au terminal client. Le paramètre par défaut est de 10 pongs manqués.

Clés	Description
`connectionInfo.period=`	Nombre entier Détermine le nombre de secondes entre chaque mise à jour de la connexion NBWSS. Chaque mise à jour détermine les terminaux client qui sont actuellement configurés dans NetBackup, et se connecte aux nouveaux terminaux client ou se déconnecte des terminaux client qui n'existent plus. **Remarque :** Après avoir ajouté un terminal client, il peut prendre jusqu'à la durée configurée pour se connecter à ce terminal client. La valeur par défaut est de 60 secondes.
`scheduledExecutor.threadPoolSize=`	Nombre entier Détermine le nombre de threads que NetBackup utilise pour maintenir la connexion de terminal client et pour traiter les notifications. Le paramètre par défaut est 1 thread. Il peut être utile d'augmenter cette valeur si le nombre de tâches planifiées augmente.
Les propriétés `mise en veille prolongée`	Ces propriétés sont pour l'utilisation de la prise en charge Veritas.

Voici le fichier `nbwss.properties` avec ses paramètres par défaut (voir la procédure suivante pour l'emplacement de ce fichier) :

```
#Properties file for NetBackup WebSocket Service
exception.ignoreDecoder=false
notification.sendTimeout=2000
notification.scheduledRate=5
keepAlive.scheduledRate=30
keepAlive.maxPongMissAllowed=10
connectionInfo.period=60
scheduledExecutor.threadPoolSize=1

#Hibernate properties
hibernate.format_sql=true
hibernate.show_sql=false
hibernate.hbm2ddl.auto=update
hibernate.dialect=org.hibernate.dialect.SybaseDialect
```

Pour configurer les propriétés de NetBackup WebSocket Service (NBWSS)

1. Utilisez un éditeur de texte pour ouvrir le fichier `nbwss.properties`.

   Le fichier se trouve dans l'emplacement suivant sur le serveur maître NetBackup :

   Sous Windows :

   install_path`\NetBackup\wmc\webserver\webapps_api\nbwss\WEB-INF\classes\nbwss.properties`

   Sous Linux :

   `/usr/openv/wmc/webserver/webapps_api/nbwss/WEB-INF/classes/nbwss.properties`

2. Modifiez la valeur de la propriété que vous voulez changer et enregistrez le fichier.

   Tableau 2-4 décrit les propriétés NBWSS et leurs valeurs par défaut.

3. Pour que les modifications entrent en vigueur, il est possible qu'il faille redémarrer le service **Console de gestion Web NetBackup** sur le serveur maître NetBackup.

Démarrage d'une connexion de NetBackup à une application cloud

Pour parler à une application cloud, NetBackup utilise une interface Web que le serveur cloud rend disponible. Cette interface est appelée terminal client WebSocket.

Un processus NetBackup demande automatiquement une connexion au terminal client WebSocket selon une planification prédéfinie. Par défaut, le processus de connexion s'exécute toutes les 60 secondes. Ce processus est contrôlé par la propriété `connectionInfo.period=` dans le fichier `nbwss.Pproperties` sur le serveur maître NetBackup. Chaque fois que le processus de connexion s'exécute, il met à jour (ajoute ou supprime) les connexions de NetBackup aux terminaux client. Par exemple, si un nouveau terminal client a été ajouté, le processus vérifie si NetBackup est déjà connecté à un autre terminal client dans le même groupe de serveurs. Si NetBackup n'est pas connecté à un autre terminal client dans le même groupe de serveurs, le processus lance une connexion au nouveau terminal client.

Pour contrôler l'intervalle de temps auquel NetBackup démarre une connexion à une application cloud

- Sur le serveur maître NetBackup, modifiez la propriété `connectionInfo.period=` dans le fichier `nbwss.properties`.

  Pour l'emplacement de ce fichier et de plus amples détails :

  Se reporter à "Configuration des propriétés de NetBackup WebSocket Service (NBWSS)" à la page 42.

  Se reporter à "Remarques sur les connexions de NetBackup aux applications cloud" à la page 10.

Remarque : Pour démarrer une connexion, NetBackup doit disposer des informations d'authentification correctes afin d'accéder au terminal client du serveur cloud :

Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

Se reporter à "Enregistrement des informations d'authentification de NetBackup pour un terminal client de serveur WebSocket" à la page 35.

Chapitre 3

Dépannage NBWSS

Ce chapitre traite des sujets suivants :

- Consignation de NBWSS
- Problèmes NBWSS

Consignation de NBWSS

Pour les messages concernant les opérations de NetBackup WebSocket Service (NBWSS), consultez les répertoires de journaux NetBackup suivants.

Tableau 3-1 Journaux NetBackup pour NBWSS

Répertoire de journal	Contient les messages relatifs à	Emplacement
Windows *chemin_installation*\NetBackup\logs\nbwebservice UNIX, Linux /usr/openv/Logs/nbwebservice nbwebservice utilise la consignation unifiée : 485 d'ID de créateur. Consultez le *Guide de référence de consignation NetBackup* pour plus d'informations sur la manière d'utiliser les journaux unifiés.	Ajout d'informations d'authentification du terminal client de NetBackup et des interactions NBWSS avec l'application cloud.	Serveur maître NetBackup

Pour créer d'autres répertoires de journal NetBackup

- Sur les serveurs NetBackup, exécutez la commande suivante :

  Windows :

  chemin_installation\NetBackup\logs\mklogdir.bat

  UNIX, Linux:

  /usr/openv/netbackup/logs/mklogdir

Pour obtenir des conseils sur l'utilisation de la consignation de NetBackup, consultez le *Guide de référence de consignation NetBackup* disponible à l'emplacement suivant :

https://www.veritas.com/support/en_US/article.DOC5332

Problèmes NBWSS

Les rubriques suivantes fournissent une aide dans la résolution des problèmes NBWSS ainsi que la boîte de dialogue **WebSocket Server** de NetBackup.

Des problèmes de validation du serveur de terminal client dans la boîte de dialogue WebSocket Server

Cette rubrique décrit les problèmes qui peuvent se produire quand vous cliquez sur **Valider** sur la boîte de dialogue **Serveur WebSocket** de NetBackup pour enregistrer les informations d'authentification de NetBackup pour un terminal client.

Problèmes avec les détails du terminal client dans un fichier au format JSON

Tableau 3-2 Problèmes d'ajout des détails du terminal client à partir d'un fichier au format JSON

Erreur	Explication et opération recommandée
Les contenus JSON ne sont pas valides	Les informations de terminal client dans le fichier JSON ne sont pas valides. Par exemple : un ou plusieurs champs dans le fichier JSON est vide ou contient des caractères non pris en charge. Notez que NetBackup ne prend pas en charge une apostrophe (') n'importe où dans le fichier. Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31. Corrigez le fichier JSON en conséquence.

Erreur	Explication et opération recommandée

`Protocole websocket non valide. Protocole wss uniquement pris en charge`
Ou
`URL incorrecte :`
	Le format de l'URL WebSocket dans le fichier JSON n'est pas pris en charge.
	Spécifiez l'URL comme décrit dans le tableau dans la rubrique suivante :
	Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

`Impossible d'établir la connexion avec l'hôte : <nomserveur WebSocket>`	Les détails du serveur sont incorrects, ou il y a un problème de réseau. ■ Assurez-vous que le nom d'hôte du serveur WebSocket (ou l'adresse IP) et port sont corrects. ■ Assurez-vous que vous pouvez effectuer un test Ping sur le serveur WebSocket. ■ Vérifiez que la recherche DNS fonctionne.

Problèmes avec les détails du terminal client dans une URL

Tableau 3-3 Problèmes de l'ajout des détails du terminal client à partir d'une URL

Erreur	Explication et opération recommandée

`paramètre de commande non valide`
Ou
`URL incorrecte :`
	L'URL WebSocket n'est pas au format pris en charge.
	Spécifiez l'URL comme décrit dans le tableau dans la rubrique suivante :
	Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

`Echec d'ouverture d'une connexion vers l'objet distant mentionné par l'URL`	NetBackup n'a pas pu obtenir le certificat SSL à partir de l'URL du terminal client. Assurez-vous que le serveur WebSocket possède un certificat SSL valide.
`Impossible d'établir la connexion avec l'hôte : <NomServeur Websocket>`	Les détails du serveur sont incorrects, ou il y a un problème de réseau. ■ Assurez-vous que le nom d'hôte du serveur WebSocket (ou l'adresse IP) et port sont corrects. ■ Assurez-vous que vous pouvez effectuer un test Ping sur le serveur WebSocket. ■ Vérifiez que la recherche DNS fonctionne.
`InvalidPacketException Impossible d'analyser le contenu JSON`	Les données qui sont hébergées sur l'URL de terminal client ne correspondent pas au format de la table dans la rubrique suivante : Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

Problèmes d'enregistrement des informations d'authentification dans la boîte de dialogue Serveur WebSocket

Cette rubrique décrit les problèmes qui peuvent se produire quand vous cliquez sur **Ajouter un hôte** sur la boîte de dialogue **Serveur WebSocket** de NetBackup pour enregistrer les informations d'authentification de NetBackup pour un terminal client.

Tableau 3-4 Problèmes d'enregistrement des détails du terminal client en tant qu'informations d'authentification NetBackup

Erreur	Explication et opération recommandée
`Les contenus JSON ne sont pas valides`	Les informations de terminal client dans le fichier JSON ne sont pas valides. Par exemple : un ou plusieurs champs dans le fichier JSON est vide ou contient des caractères non pris en charge. Notez que NetBackup ne prend pas en charge une apostrophe (') n'importe où dans le fichier. Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31. Corrigez le fichier JSON en conséquence.
`Protocole websocket non valide. Protocole wss uniquement pris en charge`	Le format de l'URL WebSocket dans le fichier JSON n'est pas pris en charge. Spécifiez l'URL comme décrit dans le tableau dans la rubrique suivante : Se reporter à "Informations du terminal client WebSocket et son formatage" à la page 31.

`Echec de la communication avec EMM`
Ou
`Impossible d'établir la connexion avec l'hôte : <Websocket servername>`
	Les détails du serveur sont incorrects, ou il y a un problème de réseau.
	■ Assurez-vous que le nom d'hôte du serveur WebSocket (ou l'adresse IP) et port sont corrects.
	■ Assurez-vous que vous pouvez effectuer un test Ping sur le serveur WebSocket.
	■ Vérifiez que la recherche DNS fonctionne.

`Les services web ne parviennent pas à se connecter à EMM. Conseil : vérifiez vos paramètres de sécurité ; Config WebServices ne sont pas compatibles avec NBAC`	Le mode NetBackup Access Control (NBAC) est activé. Le `Config Webservices` ne prend pas en charge vos paramètres NBAC actuels. Passez en revue les paramètres NBAC. Envisagez de désactiver NBAC.

Erreur	Explication et opération recommandée
`cette entité existe déjà`	Assurez-vous qu'un serveur de terminal client portant le même nom n'a pas déjà été ajouté dans NetBackup. Pour afficher les terminaux client enregistrés, cliquez sur l'option Actualiser dans la barre d'outils **Console d'administration** :  Pour obtenir de l'aide supplémentaire, contactez le support technique de Veritas.
`Le certificat ne correspondait pas à celui accepté par l'utilisateur. Vérifiez le certificat`	Le certificat SSL que vous avez accepté avec l'option **Valider** sur la boîte de dialogue **Serveur WebSocket** ne correspond pas à l'URL obtenu quand vous avez cliqué sur **Ajouter un hôte**. Assurez-vous que le certificat SSL sur le serveur de terminal client n'a pas été changé après avoir cliqué sur **Valider** pour accepter le certificat.

`Echec de configuration de la sécurité SSL`
Ou
`Echec d'ouverture d'une connexion vers l'objet distant mentionné par l'URL`
	NetBackup n'a pas pu obtenir le certificat SSL à partir de l'URL du terminal client.
	Assurez-vous que le serveur WebSocket possède un certificat SSL valide.

`Un problème s'est produit pendant le stockage du certificat SSL dans le truststore`
Ou
`Erreur de chargement du keystore`
	NetBackup n'a pas pu enregistrer le certificat SSL du serveur de terminal client sur le magasin d'approbation NetBackup.
	Pour obtenir de l'aide supplémentaire, contactez le support technique de Veritas.

Problèmes de suppression de terminal client du serveur WebSocket à partir de NetBackup

Cette rubrique décrit les problèmes qui peuvent se produire quand vous supprimez les informations d'authentification de terminal client à partir du volet **WebSocket Server(s)** de la console d'administration de NetBackup.

Tableau 3-5 Problèmes de suppression des informations d'authentification du terminal client de NetBackup

Erreur	Explication et opération recommandée

`Impossible de supprimer le certificat pour l'hôte : <nom du serveur Websocket>`
Ou
`Erreur de chargement du keystore`
	NetBackup n'a pas pu supprimer le certificat SSL du serveur de terminal client à partir de la banque de confiance NBWSS.
	Pour obtenir de l'aide supplémentaire, contactez le support technique de Veritas.

Problèmes d'affichage de la liste des serveurs WebSocket qui ont été ajoutées dans NetBackup

Cette rubrique décrit les problèmes qui peuvent se produire quand vous cliquez sur **Gestion des médias et des périphériques > Informations d'authentification > Serveurs WebSocket** dans la console d'administration NetBackup. Les terminaux client qui ont été ajoutées doivent apparaître dans le volet **Serveur (s) WebSocket**.

Tableau 3-6 Problèmes d'obtention de la liste des terminaux client du serveur WebSocket qui ont été ajoutés dans NetBackup

Erreur	Explication et opération recommandée
`aucune entité n'a été trouvée`	NetBackup n'a pas pu obtenir les terminaux client du serveur WebSocket ou n'a pas pu obtenir avec succès les informations concernant un terminal client spécifique. Pour obtenir de l'aide supplémentaire, contactez le support technique de Veritas.
`Les services web ne parviennent pas à se connecter à EMM. Conseil : vérifiez vos paramètres de sécurité ; Config WebServices ne sont pas compatibles avec NBAC`	Le mode NetBackup Access Control (NBAC) est activé. Le `Config Webservices` ne prend pas en charge vos paramètres NBAC actuels. Passez en revue les paramètres NBAC. Envisagez de désactiver NBAC.

Problèmes d'activation ou de désactivation du serveur de terminal client

Cette rubrique décrit les problèmes qui peuvent se produire quand vous essayez d'activer ou de désactiver le serveur de terminal client sur le volet **WebSocket Servers** de la console d'administration.

Tableau 3-7 Problèmes d'activation ou de désactivation du serveur de terminal client

Erreur	Explication et opération recommandée
`Impossible d'établir la connexion avec l'hôte : <NomServeur Websocket>`	Les détails du serveur sont incorrects, ou il y a un problème de réseau. ■ Assurez-vous que le nom d'hôte du serveur WebSocket (ou l'adresse IP) et port sont corrects. ■ Assurez-vous que vous pouvez effectuer un test Ping sur le serveur WebSocket. ■ Vérifiez que la recherche DNS fonctionne.

Problèmes NBWSS supplémentaires

Cette rubrique décrit des problèmes de NetBackup WebSocket Service (NBWSS) supplémentaires.

Tableau 3-8 Problèmes de dépannage supplémentaires

Erreur	Opération recommandée
L' **Etat de la connexion** du serveur WebSocket est `Déconnecté`	Vérifiez les éléments suivants : ■ Le serveur WebSocket est en cours d'exécution. ■ Le message `CONNECT RESPONSE` du serveur WebSocket contient des informations valides. Se reporter à "NetBackup demande une connexion au terminal client" à la page 18. ■ Le service NetBackup Web Management Console est en cours d'exécution.
Les notifications ne sont pas envoyées	Vérifiez les éléments suivants : ■ Le serveur WebSocket est en cours d'exécution. ■ L' **Etat** du serveur WebSocket est `Activé` et son **Etat de la connexion** est `Connecté`. ■ Le service NetBackup Web Management Console est en cours d'exécution.