



Format du fichier journal d'audit

StorageGRID 11.9

NetApp
November 08, 2024

Sommaire

- Format du fichier journal d'audit 1
- Format du fichier journal d'audit 1
- Utiliser l'outil d'explication d'audit 2
- Utiliser l'outil audit-sum 4

Format du fichier journal d'audit

Format du fichier journal d'audit

Les fichiers journaux d'audit se trouvent sur chaque nœud d'administration et contiennent un ensemble de messages d'audit individuels.

Chaque message d'audit contient les éléments suivants :

- Temps universel coordonné (UTC) de l'événement qui a déclenché le message d'audit (ATIM) au format ISO 8601, suivi d'un espace :

YYYY-MM-DDTHH:MM:SS.UUUUUU, où *UUUUUU* sont des microsecondes.

- Le message d'audit lui-même, entre crochets et commençant par AUDT.

L'exemple suivant montre trois messages d'audit dans un fichier journal d'audit (sauts de ligne ajoutés pour la lisibilité). Ces messages ont été générés lorsqu'un locataire a créé un compartiment S3 et a ajouté deux objets dans ce compartiment.

2019-08-07T18:43:30.247711

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991681] [TIME (UI64) :73520] [SAI
P (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [AVER (UI32) :10] [ATIM (UI64) :1565203410247711]
[ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (FC32) :S3RQ] [ATID (UI64) :7074142
142472611085]]
```

2019-08-07T18:43:30.783597

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991696] [TIME (UI64) :120713] [SA
IP (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [S3KY (CSTR) : "fh-small-0"]
[CBID (UI64) :0x779557A069B2C037] [UUID (CSTR) : "94BA6949-38E1-4B0C-BC80-
EB44FB4FCC7F"] [CSIZ (UI64) :1024] [AVER (UI32) :10]
[ATIM (UI64) :1565203410783597] [ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (F
C32) :S3RQ] [ATID (UI64) :8439606722108456022]]
```

2019-08-07T18:43:30.784558

```
[AUDT: [RSLT (FC32) :SUCS] [CNID (UI64) :1565149504991693] [TIME (UI64) :121666] [SA
IP (IPAD) : "10.224.2.255"] [S3AI (CSTR) : "17530064241597054718"]
[SACC (CSTR) : "s3tenant"] [S3AK (CSTR) : "SGKH9100SCkNB8M3MTWnt-
PhoTDwB9Jok7PtyLkQmA=="] [SUSR (CSTR) : "urn:sgws:identity::175300642415970547
18:root"]
[SBAI (CSTR) : "17530064241597054718"] [SBAC (CSTR) : "s3tenant"] [S3BK (CSTR) : "buc
ket1"] [S3KY (CSTR) : "fh-small-2000"]
[CBID (UI64) :0x180CBD8E678EED17] [UUID (CSTR) : "19CE06D0-D2CF-4B03-9C38-
E578D66F7ADD"] [CSIZ (UI64) :1024] [AVER (UI32) :10]
[ATIM (UI64) :1565203410784558] [ATYP (FC32) :SPUT] [ANID (UI32) :12454421] [AMID (F
C32) :S3RQ] [ATID (UI64) :13489590586043706682]]
```

Dans leur format par défaut, les messages d'audit dans les fichiers journaux d'audit ne sont pas faciles à lire ou à interpréter. Vous pouvez utiliser le ["outil d'audit-explication"](#) pour obtenir des résumés simplifiés des messages d'audit dans le journal d'audit. Vous pouvez utiliser le ["outil de somme d'audit"](#) pour résumer le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.

Utiliser l'outil d'explication d'audit

Vous pouvez utiliser `audit-explain` l'outil pour traduire les messages d'audit dans le

journal d'audit dans un format facile à lire.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

L' `audit-explain` outil, disponible sur le nœud d'administration principal, fournit des résumés simplifiés des messages d'audit dans un journal d'audit.



Cet `audit-explain` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-explain` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l' `audit-explain` outil. Ces quatre "**SPUT**" messages d'audit ont été générés lorsque le locataire S3 associé à l'ID de compte 92484777680322627870 a utilisé des demandes PUT S3 pour créer un compartiment nommé « `bucket1` » et ajouter trois objets à ce compartiment.

```
SPUT S3 PUT bucket bucket1 account:92484777680322627870 usec:124673
SPUT S3 PUT object bucket1/part1.txt tenant:92484777680322627870
cbid:9DCB157394F99FE5 usec:101485
SPUT S3 PUT object bucket1/part2.txt tenant:92484777680322627870
cbid:3CFBB07AB3D32CA9 usec:102804
SPUT S3 PUT object bucket1/part3.txt tenant:92484777680322627870
cbid:5373D73831ECC743 usec:93874
```

L' `audit-explain` outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-explain audit.log
```

```
audit-explain 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-explain audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-explain /var/local/log/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

```
grep SPUT audit.log | audit-explain
```

```
grep bucket-name audit.log | audit-explain
```

Comme les journaux d'audit peuvent être très volumineux et lents à analyser, vous gagnez du temps en filtrant

les parties que vous souhaitez consulter et exécuter `audit-explain` sur les pièces, au lieu du fichier entier.



`audit-explain` L'outil n'accepte pas les fichiers compressés en tant qu'entrée de tuyauterie. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l' `zcat` outil pour décompresser d'abord les fichiers. Par exemple :

```
zcat audit.log.gz | audit-explain
```

Utilisez l' `help (-h)` option pour voir les options disponibles. Par exemple :

```
$ audit-explain -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

```
$ audit-explain /var/local/log/audit.log
```

L' `audit-explain` outil imprime des interprétations lisibles de tous les messages du ou des fichiers spécifiés.



Pour réduire la longueur des lignes et faciliter la lisibilité, les horodatages ne sont pas affichés par défaut. Si vous voulez voir les horodatages, utilisez l' `(-t)` option horodatage).

Utiliser l'outil `audit-sum`

Vous pouvez utiliser `audit-sum` l'outil pour compter les messages d'audit d'écriture, de lecture, de tête et de suppression et pour afficher le temps minimal, maximal et moyen (ou la taille) pour chaque type d'opération.

Avant de commencer

- Vous avez "[autorisations d'accès spécifiques](#)".
- Vous devez avoir le `Passwords.txt` fichier.
- Vous devez connaître l'adresse IP du nœud d'administration principal.

Description de la tâche

L'`audit-sum`outil, disponible sur le nœud d'administration principal, récapitule le nombre d'opérations d'écriture, de lecture et de suppression consignées, ainsi que la durée de ces opérations.



Cet `audit-sum` outil est principalement destiné au support technique lors des opérations de dépannage. Le traitement des `audit-sum` requêtes peut consommer une grande quantité de puissance CPU, ce qui peut avoir un impact sur les opérations StorageGRID.

Cet exemple montre les résultats typiques de l'`audit-sum`outil. Cet exemple montre la durée des opérations de protocoles.

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

`audit-sum`L'outil fournit le nombre et l'heure des messages d'audit S3, Swift et ILM suivants dans un journal d'audit.



Les codes d'audit sont supprimés du produit et de la documentation, car les fonctionnalités sont obsolètes. Si vous rencontrez un code d'audit qui n'est pas répertorié ici, consultez les versions précédentes de cette rubrique pour connaître les versions antérieures de SG. Par exemple "[StorageGRID 11.8 à l'aide de la documentation de l'outil de somme d'audit](#)", .

Code	Description	Reportez-vous à la section
IDEL	ILM initialisée – journaux lorsque l'ILM démarre le processus de suppression d'un objet.	" IDEL : suppression initiée ILM "
SDEL	SUPPRESSION S3 : journal une transaction réussie pour supprimer un objet ou un compartiment.	" SDEL : SUPPRESSION S3 "
SGET	S3 GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un compartiment.	" SGET : OBTENEZ S3 "

Code	Description	Reportez-vous à la section
SHEA	TÊTE S3 : consigne une transaction réussie pour vérifier l'existence d'un objet ou d'un compartiment.	"SHEA : TÊTE S3"
SPUT	S3 PUT : enregistre la réussite d'une transaction pour créer un nouvel objet ou un compartiment.	"SPUT : PUT S3"
WDEL	SUPPRESSION Swift : enregistre une transaction réussie pour supprimer un objet ou un conteneur.	"WDEL : SUPPRESSION rapide"
C'EST PARTI	SWIFT GET : log une transaction réussie pour récupérer un objet ou répertorier les objets dans un conteneur.	"WGET: SWIFT GET"
WHEA	SWIFT HEAD : consigne une transaction réussie afin de vérifier l'existence d'un objet ou d'un conteneur.	"WHEA: TÊTE SWIFT"
WPUT	SWIFT PUT : consigne une transaction réussie pour créer un nouvel objet ou conteneur.	"WPUT : PUT SWIFT"

L'`audit-sum`outil peut effectuer les opérations suivantes :

- Traiter les journaux d'audit bruts ou compressés. Par exemple :

```
audit-sum audit.log
```

```
audit-sum 2019-08-12.txt.gz
```

- Traitez plusieurs fichiers simultanément. Par exemple :

```
audit-sum audit.log 2019-08-12.txt.gz 2019-08-13.txt.gz
```

```
audit-sum /var/local/log/*
```

- Acceptez l'entrée d'un canal, qui vous permet de filtrer et de prétraiter l'entrée à l'aide de la `grep` commande ou d'autres moyens. Par exemple :

```
grep WGET audit.log | audit-sum
```

```
grep bucket1 audit.log | audit-sum
```

```
grep SPUT audit.log | grep bucket1 | audit-sum
```




Cet outil n'accepte pas les fichiers compressés comme entrée de pipettes. Pour traiter des fichiers compressés, indiquez leurs noms de fichiers en tant qu'arguments de ligne de commande ou utilisez l'`zcat`outil pour décompresser d'abord les fichiers. Par exemple :

```
audit-sum audit.log.gz

zcat audit.log.gz | audit-sum
```

Vous pouvez utiliser les options de ligne de commande pour résumer les opérations sur des compartiments séparément des opérations sur des objets ou pour regrouper les résumés de messages par nom de compartiment, par période ou par type de cible. Par défaut, les résumés affichent le temps de fonctionnement minimal, maximal et moyen, mais vous pouvez utiliser l'`size (-s)`option pour examiner la taille de l'objet à la place.

Utilisez l'`help (-h)`option pour voir les options disponibles. Par exemple :

```
$ audit-sum -h
```

Étapes

1. Connectez-vous au nœud d'administration principal :
 - a. Entrez la commande suivante : `ssh admin@primary_Admin_Node_IP`
 - b. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.
 - c. Entrez la commande suivante pour basculer en root : `su -`
 - d. Saisissez le mot de passe indiqué dans le `Passwords.txt` fichier.

Lorsque vous êtes connecté en tant que root, l'invite passe de \$ à #.

2. Pour analyser tous les messages liés aux opérations d'écriture, de lecture, de tête et de suppression, procédez comme suit :
 - a. Entrez la commande suivante, où `/var/local/log/audit.log` représente le nom et l'emplacement du ou des fichiers à analyser :

```
$ audit-sum /var/local/log/audit.log
```

Cet exemple montre les résultats typiques de l'`audit-sum`outil. Cet exemple montre la durée des opérations de protocoles.

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
IDEL	274		
SDEL	213371	0.004	20.934
0.352			
SGET	201906	0.010	1740.290
1.132			
SHEA	22716	0.005	2.349
0.272			
SPUT	1771398	0.011	1770.563
0.487			

Dans cet exemple, les opérations SGET (S3 GET) sont les opérations les plus lentes en moyenne à 1.13 secondes, mais les opérations SGET et SPUT (S3 PUT) affichent toutes les deux de longues périodes de pire des cas d'environ 1,770 secondes.

- b. Pour afficher les opérations de récupération 10 les plus lentes, utilisez la commande `grep` pour sélectionner uniquement les messages SGET et ajouter l'option de sortie longue (-l) pour inclure les chemins d'objet :

```
grep SGET audit.log | audit-sum -l
```

Les résultats incluent le type (objet ou compartiment) et le chemin, ce qui vous permet d'afficher le journal d'audit pour les autres messages relatifs à ces objets particuliers.

```

Total:          201906 operations
Slowest:       1740.290 sec
Average:       1.132 sec
Fastest:       0.010 sec
Slowest operations:
    time(usec)      source ip          type          size(B) path
    =====
1740289662  10.96.101.125      object        5663711385
backup/r9010aQ8JB-1566861764-4519.iso
1624414429  10.96.101.125      object        5375001556
backup/r9010aQ8JB-1566861764-6618.iso
1533143793  10.96.101.125      object        5183661466
backup/r9010aQ8JB-1566861764-4518.iso
70839      10.96.101.125      object         28338
bucket3/dat.1566861764-6619
68487      10.96.101.125      object         27890
bucket3/dat.1566861764-6615
67798      10.96.101.125      object         27671
bucket5/dat.1566861764-6617
67027      10.96.101.125      object         27230
bucket5/dat.1566861764-4517
60922      10.96.101.125      object         26118
bucket3/dat.1566861764-4520
35588      10.96.101.125      object         11311
bucket3/dat.1566861764-6616
23897      10.96.101.125      object         10692
bucket3/dat.1566861764-4516

```

+ Dans cet exemple de sortie, vous pouvez constater que les trois demandes GET S3 les plus lentes étaient celles des objets d'une taille d'environ 5 Go (ce qui est beaucoup plus important que les autres objets). La grande taille tient compte des délais de récupération lents les moins importants.

3. Si vous voulez déterminer la taille des objets qui sont ingérés et récupérés à partir de votre grille, utilisez l'option `taille (-s)` :

```
audit-sum -s audit.log
```

message group average (MB)	count	min (MB)	max (MB)
=====	=====	=====	=====
IDEL 1654.502	274	0.004	5000.000
SDEL 1.695	213371	0.000	10.504
SGET 14.920	201906	0.000	5000.000
SHEA 2.967	22716	0.001	10.504
SPUT 2.495	1771398	0.000	5000.000

Dans cet exemple, la taille moyenne des objets pour SPUT est inférieure à 2.5 Mo, mais la taille moyenne pour SGET est beaucoup plus grande. Le nombre de messages SPUT est beaucoup plus élevé que le nombre de messages SGET, ce qui indique que la plupart des objets ne sont jamais récupérés.

4. Si vous voulez déterminer si les récupérations étaient lentes hier :
 - a. Exécutez la commande dans le journal d'audit approprié et utilisez l'option Group-by-time (-gt(groupe par heure), suivie de la période (par exemple, 15M, 1H, 10S) :

```
grep SGET audit.log | audit-sum -gt 1H
```

message group average(sec)	count	min(sec)	max(sec)
=====	=====	=====	=====
2019-09-05T00 1.254	7591	0.010	1481.867
2019-09-05T01 1.115	4173	0.011	1740.290
2019-09-05T02 1.562	20142	0.011	1274.961
2019-09-05T03 1.254	57591	0.010	1383.867
2019-09-05T04 1.405	124171	0.013	1740.290
2019-09-05T05 1.562	420182	0.021	1274.511
2019-09-05T06 5.562	1220371	0.015	6274.961
2019-09-05T07 2.002	527142	0.011	1974.228
2019-09-05T08 1.105	384173	0.012	1740.290
2019-09-05T09 1.354	27591	0.010	1481.867

Ces résultats montrent que S3 GÉNÈRE un trafic entre 06:00 et 07:00. Les temps maximum et moyen sont à la fois considérablement plus élevés à ces moments aussi, et ils n'ont pas augmenté progressivement à mesure que le comptage a augmenté. Cela suggère que la capacité a été dépassée quelque part, peut-être dans le réseau ou que la grille peut traiter les demandes.

- b. Pour déterminer la taille des objets récupérés chaque heure d'hier, ajoutez l'option size (-s) à la commande :

```
grep SGET audit.log | audit-sum -gt 1H -s
```

message group average (B)	count	min (B)	max (B)
=====	=====	=====	=====
2019-09-05T00 1.976	7591	0.040	1481.867
2019-09-05T01 2.062	4173	0.043	1740.290
2019-09-05T02 2.303	20142	0.083	1274.961
2019-09-05T03 1.182	57591	0.912	1383.867
2019-09-05T04 1.528	124171	0.730	1740.290
2019-09-05T05 2.398	420182	0.875	4274.511
2019-09-05T06 51.328	1220371	0.691	5663711385.961
2019-09-05T07 2.147	527142	0.130	1974.228
2019-09-05T08 1.878	384173	0.625	1740.290
2019-09-05T09 1.354	27591	0.689	1481.867

Ces résultats indiquent que des récupérations très importantes se sont produites lorsque le trafic global de récupération était à son maximum.

- c. Pour plus de détails, utilisez le "outil d'audit-explication" pour revoir toutes les opérations SGET pendant cette heure :

```
grep 2019-09-05T06 audit.log | grep SGET | audit-explain | less
```

Si la sortie de la commande grep doit être de plusieurs lignes, ajoutez la less commande pour afficher le contenu du fichier journal d'audit, une page (un écran) à la fois.

- 5. Si vous souhaitez déterminer si les opérations SPUT sur les godets sont plus lentes que les opérations SPUT pour les objets :

- a. Commencez par utiliser l'`-go`option, qui regroupe les messages pour les opérations d'objet et de compartiment séparément :

```
grep SPUT sample.log | audit-sum -go
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.bucket	1	0.125	0.125
0.125			
SPUT.object	12	0.025	1.019
0.236			

Les résultats montrent que les opérations SPUT pour les compartiments ont des caractéristiques de performances différentes de celles des opérations SPUT pour les objets.

b. Pour déterminer les compartiments ayant les opérations SPUT les plus lentes, utilisez l'option `-gb`, qui regroupe les messages par compartiment :

```
grep SPUT audit.log | audit-sum -gb
```

message group	count	min(sec)	max(sec)
average(sec)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	0.046	1770.563
1.571			
SPUT.cho-versioning	54277	0.047	1736.633
1.415			
SPUT.cho-west-region	80615	0.040	55.557
1.329			
SPUT.ldt002	1564563	0.011	51.569
0.361			

c. Pour déterminer quels compartiments ont la taille d'objet SPUT la plus élevée, utilisez les options `-gb` et `-s` :

```
grep SPUT audit.log | audit-sum -gb -s
```

message group	count	min (B)	max (B)
average (B)			
=====	=====	=====	=====
=====			
SPUT.cho-non-versioning	71943	2.097	5000.000
21.672			
SPUT.cho-versioning	54277	2.097	5000.000
21.120			
SPUT.cho-west-region	80615	2.097	800.000
14.433			
SPUT.ldt002	1564563	0.000	999.972
0.352			

Informations sur le copyright

Copyright © 2024 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 DÉLICTELLE (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.