



## Référence

### BlueXP classification

NetApp  
April 03, 2024

# Sommaire

- Référence..... 1
  - Types d’instances de classification BlueXP pris en charge ..... 1
  - Métadonnées collectées à partir des sources de données ..... 2
  - Connectez-vous au système de classification BlueXP ..... 3
  - API de classification BlueXP ..... 4

# Référence

## Types d'instances de classification BlueXP pris en charge

Le logiciel de classification BlueXP doit s'exécuter sur un hôte répondant à des exigences spécifiques en termes de système d'exploitation, de RAM, de logiciels, etc. Lors du déploiement de la classification BlueXP dans le cloud, nous vous recommandons d'utiliser un système présentant les caractéristiques « grandes » pour bénéficier de fonctionnalités complètes.

Vous pouvez déployer la classification BlueXP sur un système avec moins de processeurs et moins de RAM, mais l'utilisation de systèmes moins puissants comporte certaines limitations. ["Découvrez ces limites"](#).

Dans les tableaux suivants, si le système marqué comme « par défaut » n'est pas disponible dans la région dans laquelle vous installez la classification BlueXP, le système suivant du tableau sera déployé.

### Types d'instances AWS

Taille du système	Caractéristiques	Type d'instance
Très grand	32 processeurs, 128 Go de RAM, 1 Tio de SSD gp3	<a href="#">"m6i.8xlarge"</a> (valeur par défaut)
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	<a href="#">"m6i.4xlarge"</a> (par défaut) m6a.4xlarge m5a.4xlarge m5.4xlarge m4.4xlarge
Moyen	8 processeurs, 32 Go de RAM, SSD de 200 Gio	<a href="#">"m6i.2xlarge"</a> (par défaut) m6a.2xlarge m5a.2xlarge m5.2xlarge m4.2xlarge
Petit	8 processeurs, 16 Go de RAM, SSD de 100 Gio	<a href="#">"c6a.2xlarge"</a> (par défaut) c5a.2xlarge c5.2xlarge c4.2xlarge

### Types d'instances Azure

Taille du système	Caractéristiques	Type d'instance
Très grand	32 processeurs, 128 Go de RAM, disque OS (2,048 Gio, débit min. De 250 Mo/s) et disque de données (SSD de 1 Tio, débit min. De 750 Mo/s)	<a href="#">"Standard_D32_v3"</a> (valeur par défaut)
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	<a href="#">"Standard_D16s_v3"</a> (valeur par défaut)

### Types d'instances GCP

Taille du système	Caractéristiques	Type d'instance
Grand	16 processeurs, 64 Go de RAM, SSD de 500 Gio	<a href="#">"n2-standard-16"</a> (par défaut) n2d-standard-16 n1-standard-16

# Métadonnées collectées à partir des sources de données

La classification BlueXP collecte certaines métadonnées lors d'analyses de classification des données à partir de vos sources de données et de vos environnements de travail. La classification BlueXP peut accéder à la plupart des métadonnées dont nous avons besoin pour classer vos données, mais il existe certaines sources où nous ne pouvons pas accéder aux données dont nous avons besoin.

	Métadonnées	CIFS	NFS
<b>Timbres horaires</b>	<i>Temps de création</i>	Disponibilité	Non disponible (non pris en charge sous Linux)
	<i>Heure du dernier accès</i>	Disponibilité	Disponibilité
	<i>Heure de la dernière modification</i>	Disponibilité	Disponibilité
<b>Autorisations</b>	<i>Autorisations d'ouverture</i>	Si le groupe « TOUT LE MONDE » a accès au fichier, il est considéré comme « ouvert à l'entreprise ».	Si les « autres » ont accès au fichier, il est considéré comme « ouvert à l'entreprise ».
	<i>Accès utilisateurs/groupe</i>	Les informations relatives aux utilisateurs et aux groupes sont extraites du protocole LDAP	Non disponible (les utilisateurs NFS sont généralement gérés localement sur le serveur, par conséquent, la même personne peut avoir un UID différent sur chaque serveur)



- La classification BlueXP n'extrait pas l'heure du dernier accès des sources de données suivantes : SharePoint Online, SharePoint on-prest (SharePoint Server), OneDrive, Google Drive et Amazon S3, et bases de données.
- Les versions antérieures du système d'exploitation Windows (par exemple, Windows 7 et Windows 8) désactivent la collection de l'attribut « heure du dernier accès » par défaut car elle peut avoir un impact sur les performances du système. Lorsque cet attribut n'est pas collecté, les analyses de classification BlueXP basées sur « l'heure du dernier accès » sont impactées. Vous pouvez activer la collecte de l'heure du dernier accès sur ces anciens systèmes Windows si nécessaire.

## Horodatage du dernier accès

Lorsque la classification BlueXP extrait des données des partages de fichiers, le système d'exploitation les considère comme accédant aux données et modifie l'« heure du dernier accès » en conséquence. Après l'analyse, la classification BlueXP tente de rétablir l'horodatage d'origine pour l'heure du dernier accès. Si la classification BlueXP ne dispose pas d'autorisations d'attributs d'écriture dans CIFS, ou si elle ne dispose pas d'autorisations d'écriture dans NFS, le système ne peut pas rétablir l'heure du dernier accès à l'horodatage d'origine. Les volumes ONTAP configurés avec SnapLock disposent d'autorisations en lecture seule et ne peuvent pas non plus rétablir l'horodatage du dernier accès.

Par défaut, si la classification BlueXP ne dispose pas de ces autorisations, le système n'analyse pas ces fichiers dans vos volumes, car la classification BlueXP ne peut pas rétablir l'heure du dernier accès à

l'horodatage d'origine. Cependant, si vous ne vous souciez pas si l'heure du dernier accès est réinitialisée à l'heure d'origine dans vos fichiers, vous pouvez cliquer sur le commutateur **Scan en cas d'autorisations d'écriture d'attributs manquantes** en bas de la page de configuration pour que la classification BlueXP analyse les volumes indépendamment des autorisations.

Scan	Storage Repository (Share)	Protocol	Access	Scan Status	Required Action
Map Map & Classify	\\10.1.7.16\CIFS_LABS_SHARE6	CIFS	Continuously Scanning	Mapped: 5.8K Classified: 5.8K	...
Map Map & Classify	\\10.1.7.16\CIFS_LABS_SHARE7	CIFS	Continuously Scanning	Mapped: 5.8K Classified: 5.8K	...

Cette fonctionnalité s'applique aux systèmes ONTAP sur site, à Cloud Volumes ONTAP, Azure NetApp Files, FSX pour ONTAP et aux partages de fichiers non-NetApp.

Notez qu'il existe un filtre dans la page Investigation appelé *Scan Analysis Event* qui vous permet d'afficher les fichiers qui n'ont pas été classés car la classification BlueXP n'a pas pu rétablir l'heure de dernier accès, Ou les fichiers classifiés même si la classification BlueXP ne pouvait pas rétablir l'heure du dernier accès.

**Scan Analysis Event** 1 -
   
☐ Not classified - Cannot revert last access
   
☒ Classified and changed last access time

Les sélections de filtre sont les suivantes :

- « Non classé — Impossible de rétablir l'heure du dernier accès » - affiche les fichiers qui n'ont pas été classés en raison de permissions d'écriture manquantes.
- « Heure du dernier accès classifiée et mise à jour » - affiche les fichiers classés et la classification BlueXP n'a pas pu rétablir l'heure du dernier accès à la date d'origine. Ce filtre n'est pertinent que pour les environnements dans lesquels vous avez activé **Scan lorsque vous ne disposez pas des autorisations d'écriture d'attributs**.

Si nécessaire, vous pouvez exporter ces résultats dans un rapport afin de voir quels fichiers sont ou ne sont pas analysés en raison des autorisations. ["En savoir plus sur le rapport d'enquête sur les données"](#).

## Connectez-vous au système de classification BlueXP

Il se peut que vous deviez vous connecter au système de classification BlueXP pour pouvoir accéder aux fichiers journaux ou modifier les fichiers de configuration.

Lorsque la classification BlueXP est installée sur une machine Linux de votre site ou sur une machine Linux que vous avez déployée dans le cloud, vous pouvez accéder directement au fichier de configuration et au script.

Lorsque la classification BlueXP est déployée dans le cloud, vous devez établir une connexion SSH avec l'instance de classification BlueXP. Vous vous SSH dans le système en saisissant l'utilisateur et le mot de passe, ou en utilisant la clé SSH fournie lors de l'installation du connecteur BlueXP. La commande SSH est :

```
ssh -i <path_to_the_ssh_key> <machine_user>@<datasense_ip>
* <path_to_the_ssh_key> = emplacement des clés d'authentification ssh
* <machine_utilisateur> :
```

+

#### **Pour AWS : utilisez <utilisateur ec2>**

Pour Azure : utilisez l'utilisateur créé pour l'instance BlueXP

\*\* Pour GCP : utilisez l'utilisateur créé pour l'instance BlueXP

- <dataense\_ip> = adresse IP de l'instance de la machine virtuelle

Notez que vous devrez modifier les règles entrantes du groupe de sécurité pour accéder au système dans le cloud. Pour plus de détails, voir :

- ["Règles de groupe de sécurité dans AWS"](#)
- ["Règles de groupe de sécurité dans Azure"](#)
- ["Règles de pare-feu dans Google Cloud"](#)

## **API de classification BlueXP**

Les fonctionnalités de classification de BlueXP disponibles via l'interface utilisateur web sont également disponibles via l'API swagger.

Quatre catégories de classification BlueXP correspondent aux onglets de l'interface utilisateur :

- Enquête
- La conformité
- La gouvernance
- Configuration

Les API de la documentation swagger vous permettent de rechercher, d'agréger des données, de suivre vos analyses et de créer des actions telles que la copie, le déplacement, etc.

### **Présentation**

L'API vous permet d'effectuer les fonctions suivantes :

- Informations d'exportation
  - Tout ce qui est disponible dans l'interface utilisateur peut être exporté via l'API (à l'exception des rapports)
  - Les données sont exportées au format JSON (facile à analyser et à envoyer vers des applications tierces, telles que Splunk)
- Créez des requêtes à l'aide des instructions « ET » et « OU », incluez et excluez des informations, etc.

Par exemple, vous pouvez localiser des fichiers *sans* informations personnelles identifiables (PII) spécifiques (fonctionnalité non disponible dans l'interface utilisateur). Vous pouvez également exclure des champs spécifiques pour l'opération d'exportation.

- Effectuer des actions
  - Mettre à jour les informations d'identification CIFS
  - Afficher et annuler des actions
  - Ré-analyser les répertoires
  - Supprimez, copiez, étiquetez et affectez des utilisateurs aux données
  - Cloner et copier des fichiers
  - Exporter les données

L'API est sécurisée et utilise la même méthode d'authentification que l'interface utilisateur. Vous trouverez des informations sur l'authentification dans : [https://docs.netapp.com/us-en/bluexp-automation/platform/get\\_identifiers.html](https://docs.netapp.com/us-en/bluexp-automation/platform/get_identifiers.html)

## Accès à la référence de l'API swagger

Pour entrer dans swagger, vous devez disposer de l'adresse IP de votre instance de classification BlueXP. Dans le cas d'un déploiement cloud, vous utiliserez l'adresse IP publique. Ensuite, vous devrez entrer dans ce terminal :

`https://<classification_ip>/documentation`

## Exemple d'utilisation des API

L'exemple suivant montre un appel d'API pour copier des fichiers.

### Demande d'API

Vous devrez d'abord obtenir tous les champs et options pertinents pour un environnement de travail pour afficher tous les filtres dans l'onglet investigation.

```
curl -X GET "http://{classification_ip}/api/{classification_version}
/search/options?data_mode=ALL_EXTRACTABLE" -H "accept: application/json"
-H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR....." -H "x-agent-id:
hOXsZNvnA5LsthwMILtjL9xZFyBQxAwMclients"
```

### Réponse

```
{
  "options": [
    {
      "active_directory_affected": false,
      "data_mode": "ALL_SCANNED",
      "field": "string",
      "is_rulable": true,
      "name": "string",
      "operators": [
        "EQUALS"
      ],
      "optional_values": [
```

```

        {}
    ],
    "secondary": {},
    "server_data": false,
    "type": "TEXT"
}
]
}
{
    "options": [
        {
            "active_directory_affected": false,
            "data_mode": "ALL_EXTRACTABLE",
            "field": "POLICIES",
            "name": "Policies",
            "operators": [
                "IN",
                "NOT_IN"
            ],
            "server_data": true,
            "type": "SELECT"
        },
        {
            "active_directory_affected": false,
            "data_mode": "ALL_EXTRACTABLE",
            "field": "EXTRACTION_STATUS_RANGE",
            "name": "Scan Analysis Status",
            "operators": [
                "IN"
            ],
            "server_data": true,
            "type": "SELECT"
        },
        {
            "active_directory_affected": false,
            "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
            "field": "SCAN_ANALYSIS_ERROR",
            "name": "Scan Analysis Event",
            "operators": [
                "IN"
            ],
            "server_data": true,
            "type": "SELECT"
        },
        {
            "active_directory_affected": false,

```



```

    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "PUBLIC_ACCESS",
    "name": "Open Permissions",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": true,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "USERS_PERMISSIONS_COUNT_RANGE",
    "name": "Number of Users with Access",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": true,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "USER_GROUP_PERMISSIONS",
    "name": "User / Group Permissions",
    "operators": [
        "IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_OWNER",
    "name": "File Owner",
    "operators": [
        "EQUALS",
        "CONTAINS"
    ],
    "server_data": true,
    "type": "TEXT"
},
{

```

```

    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ENVIRONMENT_TYPE",
    "name": "Working Environment Type",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ENVIRONMENT",
    "name": "Working Environment",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_SCANNED",
    "field": "SCAN_TASK",
    "name": "Storage Repository",
    "operators": [
        "IN",
        "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
},
{
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_PATH",
    "name": "File / Directory Path",
    "operators": [
        "MULTI_CONTAINS",
        "MULTI_EXCLUDE"
    ],
    "server_data": true,
    "type": "MULTI_TEXT"
}

```

```

},
{
  "active_directory_affected": false,
  "data_mode": "ALL_DASHBOARD_EXTRACTABLE",
  "field": "CATEGORY",
  "name": "Category",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "PATTERN_SENSITIVITY_LEVEL",
  "name": "Sensitivity Level",
  "operators": [
    "IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
  "field": "NUMBER_OF_IDENTIFIERS",
  "name": "Number of identifiers",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,
  "type": "SELECT"
},
{
  "active_directory_affected": false,
  "data_mode": "ALL_EXTRACTABLE",
  "field": "PATTERN_PERSONAL",
  "name": "Personal Data",
  "operators": [
    "IN",
    "NOT_IN"
  ],
  "server_data": true,

```

```

    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "PATTERN_SENSITIVE",
    "name": "Sensitive Personal Data",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "DATA_SUBJECT",
    "name": "Data Subject",
    "operators": [
      "EQUALS",
      "CONTAINS"
    ],
    "server_data": true,
    "type": "TEXT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "DIRECTORIES",
    "field": "DIRECTORY_TYPE",
    "name": "Directory Type",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "FILE_TYPE",
    "name": "File Type",
    "operators": [
      "IN",
      "NOT_IN"
    ]
  }

```

```

    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "FILE_SIZE_RANGE",
    "name": "File Size",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_CREATION_RANGE_RETENTION",
    "name": "Created Time",
    "operators": [
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "DISCOVERED_TIME_RANGE",
    "name": "Discovered Time",
    "operators": [
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_LAST_MODIFICATION_RETENTION",
    "name": "Last Modified",
    "operators": [
      "IN"
    ],

```

```

    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_FILESYSTEM_EXTRACTABLE",
    "field": "FILE_LAST_ACCESS_RANGE_RETENTION",
    "name": "Last Accessed",
    "operators": [
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "FILES",
    "field": "IS_DUPLICATE",
    "name": "Duplicates",
    "operators": [
      "EQUALS",
      "IN"
    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "FILES",
    "field": "FILE_HASH",
    "name": "File Hash",
    "operators": [
      "EQUALS",
      "IN"
    ],
    "server_data": true,
    "type": "TEXT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "USER_DEFINED_STATUS",
    "name": "Tags",
    "operators": [
      "IN",
      "NOT_IN"
    ]
  }

```

```

    ],
    "server_data": true,
    "type": "SELECT"
  },
  {
    "active_directory_affected": false,
    "data_mode": "ALL_EXTRACTABLE",
    "field": "ASSIGNED_TO",
    "name": "Assigned to",
    "operators": [
      "IN",
      "NOT_IN"
    ],
    "server_data": true,
    "type": "SELECT"
  }
]
}

```

Nous utiliserons cette réponse dans nos paramètres de demande pour filtrer les fichiers que nous voulons copier.

Vous pouvez appliquer une action à plusieurs éléments. Les types d'action pris en charge sont notamment : déplacer, supprimer, copier, attribuer à, FlexClone, exporter les données, renumériser et étiqueter.

Nous allons créer l'action de copie :

### Demande d'API

Cette API suivante est cette API d'action et elle vous permet de créer plusieurs actions.

```

curl -X POST "http://
{classification_ip}/api/{classification_version}/actions" -H "accept:
application/json" -H "Authorization: Bearer eyJhbGciOiJSUzI1NiIsInR..... "
-H "x-agent-id: hOXsZNvnA5LsthwMILtjL9xZFYBQxAwMclients " -H "Content-
Type: application/json" -d "{ \"action_type\": \"COPY\", \"data_mode\":
\"FILES\", \"policy_id\": 0, \"request_params\": { destination_nfs_path:
\"{ontap_ip}/{share_name} \" },
\"requested_query\":{\"condition\":\"AND\",\"rules\":[{\"field\":\"ENVIRONMENT_TYPE
\",\"operator\":\"IN\",\"value\":[\"ONPREM\"]},{\"field\":\"CATEGORY\",\"operator\":\"IN\",
\"value\":[\"21\"]}]}}}"

```

### Réponse

La réponse renvoie l'objet d'action, de sorte que vous pouvez utiliser les API GET et DELETE pour obtenir le statut de l'action ou pour l'annuler.

```
{
  "action_type": "COPY",
  "creation_time": "2023-08-08T12:37:21.705Z",
  "data_mode": "FILES",
  "end_time": "2023-08-08T12:37:21.705Z",
  "estimated_time_to_complete": 0,
  "id": 0,
  "policy_id": 0,
  "policy_name": "string",
  "priority": 0,
  "request_params": {},
  "requested_query": {},
  "result": {
    "error_message": "string",
    "failed": 0,
    "in_progress": 0,
    "succeeded": 0,
    "total": 0
  },
  "start_time": "2023-08-08T12:37:21.705Z",
  "status": "QUEUED",
  "title": "string",
  "user_id": "string"
}
```



## 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.