Référence

Cloud Backup

NetApp
November 17, 2022

Table des matières

Référence

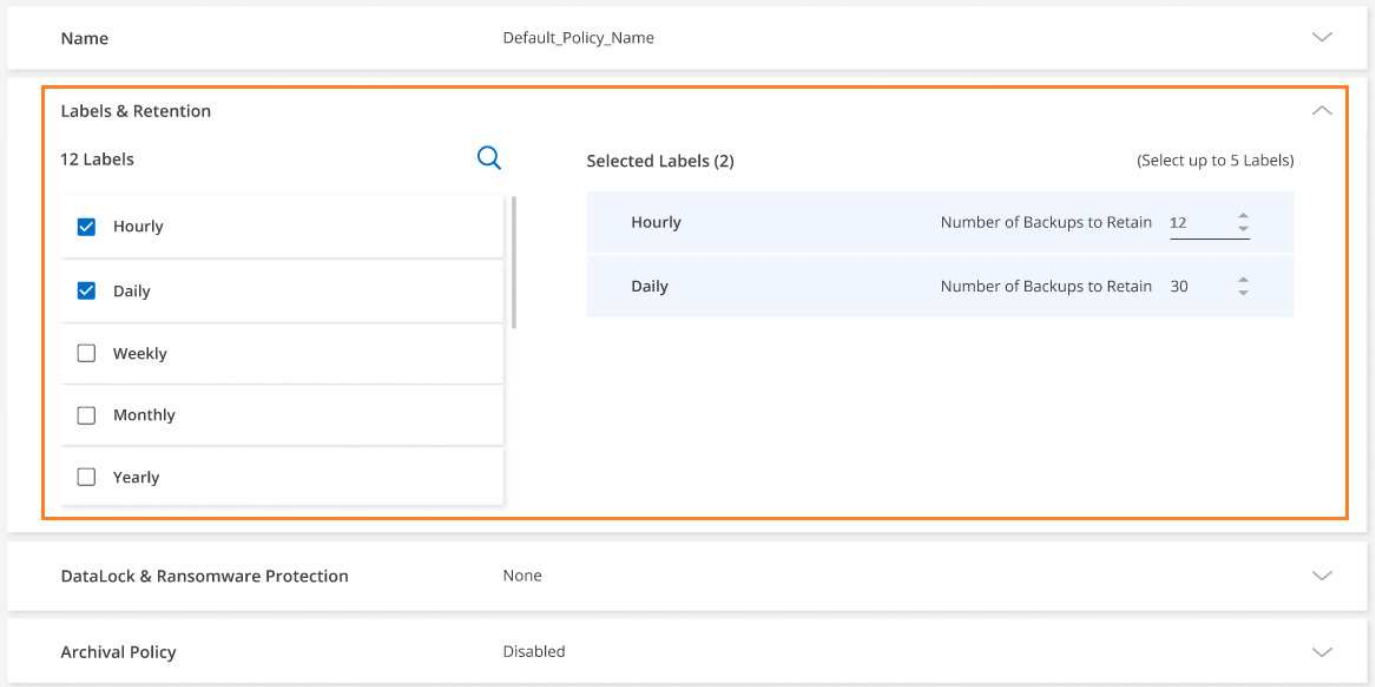
Paramètres de configuration de la politique de Cloud Backup

Ce document décrit les paramètres de configuration de la stratégie de sauvegarde des systèmes ONTAP sur site et Cloud Volumes ONTAP utilisés avec Cloud Backup Service.

Planifications de sauvegarde

Cloud Backup vous permet de créer plusieurs règles de sauvegarde avec des planifications uniques pour chaque environnement de travail (cluster). Vous pouvez attribuer différentes stratégies de sauvegarde à des volumes ayant différents objectifs de point de récupération (RPO).

Chaque stratégie de sauvegarde fournit une section pour *Labels & Retention* que vous pouvez appliquer à vos fichiers de sauvegarde.



Il y a deux parties du calendrier : l'étiquette et la valeur de conservation :

- Le **label** définit la fréquence à laquelle un fichier de sauvegarde est créé (ou mis à jour) à partir du volume. Vous pouvez sélectionner l'un des types d'étiquettes suivants :
  - Vous pouvez choisir une ou une combinaison de **horaire**, **quotidien**, **hebdomadaire**, **mensuel**, et **calendriers annuels**.
  - Vous pouvez sélectionner une des règles définies par le système qui assure la sauvegarde et la conservation pendant 3 mois, 1 an ou 7 ans.
  - Si vous avez créé des règles de protection des sauvegardes personnalisées sur le cluster à l'aide de ONTAP System Manager ou de l'interface de ligne de commandes ONTAP, vous pouvez sélectionner l'une de ces règles.
- La valeur **rétention** définit le nombre de fichiers de sauvegarde pour chaque étiquette (délai). Lorsque le

nombre maximal de sauvegardes est atteint dans une catégorie ou un intervalle, les anciennes sauvegardes sont supprimées afin que vous ayez toujours les sauvegardes les plus récentes. Cela vous permet également d'économiser de l'espace de stockage, car les sauvegardes obsolètes ne prennent pas toujours de l'espace dans le cloud.

Par exemple, dites que vous créez une stratégie de sauvegarde qui crée 7 sauvegardes **hebdomadaires** et 12 **mensuelles** :

- chaque semaine et chaque mois, un fichier de sauvegarde est créé pour le volume
- au cours de la 8e semaine, la première sauvegarde hebdomadaire est supprimée, et la nouvelle sauvegarde hebdomadaire est ajoutée pour la 8e semaine (pour un maximum de 7 sauvegardes hebdomadaires).
- au 13ème mois, la première sauvegarde mensuelle est supprimée, et la nouvelle sauvegarde mensuelle du 13ème mois est ajoutée (en conservant un maximum de 12 sauvegardes mensuelles)

Notez que les sauvegardes annuelles sont automatiquement supprimées du système source après leur transfert vers le stockage objet. Ce comportement par défaut peut être modifié "Dans la page Paramètres avancés" Pour l'environnement de travail.

Protection des données par verrouillage et protection contre les ransomwares

Cloud Backup prend en charge le verrouillage des données et la protection contre les attaques par ransomware pour vos sauvegardes de volumes. Ces fonctionnalités vous permettent de verrouiller vos fichiers de sauvegarde et de les analyser afin de détecter un ransomware possible dans les fichiers de sauvegarde. Il s'agit d'un paramètre facultatif que vous pouvez définir dans vos stratégies de sauvegarde lorsque vous souhaitez bénéficier d'une protection supplémentaire pour vos sauvegardes de volume d'un cluster.

Ces deux fonctionnalités protègent vos fichiers de sauvegarde, afin que vous puissiez toujours disposer d'un fichier de sauvegarde valide à même de récupérer vos données en cas d'attaque par ransomware lorsqu'elles sont présentes sur vos données source. Il est également utile de respecter certaines exigences réglementaires dans lesquelles les sauvegardes doivent être verrouillées et conservées pendant un certain temps. Lorsque le verrouillage des données et la protection contre les attaques par ransomware sont activés, le compartiment cloud provisionné dans le cadre de l'activation de Cloud Backup active le verrouillage des objets et le contrôle des versions des objets.

Cette fonction n'assure pas la protection de vos volumes source, uniquement pour les sauvegardes de ces volumes source. Faites confiance à NetApp "Cloud Insights et Cloud Secure", ou une partie du "Protections contre les ransomwares fournies par ONTAP" pour protéger vos volumes source.

- Si vous prévoyez d'utiliser DataLock et protection contre les attaques par ransomware, vous devez l'activer lors de la création de votre première stratégie de sauvegarde et de l'activation de Cloud Backup pour ce cluster.
- Il est impossible de désactiver le verrouillage des données et la protection contre les attaques par ransomware pour un cluster après sa configuration. N'activez pas cette fonctionnalité sur un cluster pour l'essayer.

Qu'est-ce que DataLock

DataLock protège vos fichiers de sauvegarde contre les modifications ou les suppressions pendant un certain temps. Cette fonctionnalité utilise la technologie du fournisseur de stockage objet pour le « verrouillage des objets ». La période pendant laquelle le fichier de sauvegarde est verrouillé (et conservé) est appelée période de rétention de DataLock. Il est basé sur le programme de stratégie de sauvegarde et le paramètre de conservation que vous avez définis, plus une mémoire tampon de 14 jours. Toute stratégie de rétention

DataLock inférieure à 30 jours est arrondie à 30 jours minimum.

Notez que les anciennes sauvegardes sont supprimées après l'expiration de la période de rétention de DataLock, et non après l'expiration de la période de conservation de la stratégie de sauvegarde.

Voyons quelques exemples de fonctionnement de cette méthode :

- Si vous créez un programme de sauvegarde mensuel avec 12 rétentions, chaque sauvegarde est verrouillée pendant 12 mois (plus 14 jours) avant sa suppression.
- Si vous créez une stratégie de sauvegarde qui crée 30 sauvegardes quotidiennes, 7 sauvegardes hebdomadaires et 12 sauvegardes mensuelles, trois périodes de conservation seront verrouillées. Les 30 sauvegardes quotidiennes seront conservées pendant 44 jours (30 jours plus 14 jours de mémoire tampon), les 7 sauvegardes hebdomadaires seraient conservées pendant 9 semaines (7 semaines plus 14 jours) et les 12 sauvegardes mensuelles seront conservées pendant 12 mois (plus 14 jours).
- Si vous créez un programme de sauvegarde horaire avec 24 rétentions, vous pensez peut-être que les sauvegardes sont verrouillées pendant 24 heures. Cependant, étant donné qu'elle est inférieure au minimum de 30 jours, chaque sauvegarde est verrouillée et conservée pendant 44 jours (30 jours plus 14 jours de mémoire tampon).

  Dans ce dernier cas, si chaque fichier de sauvegarde est verrouillé pendant 44 jours, vous obtenez beaucoup plus de fichiers de sauvegarde qu'avec une stratégie de rétention horaire/24. En règle générale, lorsque Cloud Backup crée le 25e fichier de sauvegarde, il supprime la sauvegarde la plus ancienne pour conserver le maximum de retentions à 24 (selon la règle). Dans ce cas, le paramètre de rétention DataLock remplace le paramètre de conservation de la stratégie de sauvegarde de votre stratégie de sauvegarde. Cela peut affecter vos coûts de stockage car vos fichiers de sauvegarde seront enregistrés dans le magasin d'objets pendant une période plus longue.

Protection contre les ransomwares

La protection par ransomware analyse vos fichiers de sauvegarde pour rechercher la preuve d'une attaque par ransomware. La détection des attaques par ransomware est effectuée à l'aide d'une comparaison des checksums. Si un ransomware potentiel est identifié dans un fichier de sauvegarde par rapport au fichier de sauvegarde précédent, ce fichier de sauvegarde plus récent est remplacé par le fichier de sauvegarde le plus récent, qui ne montre aucun signe d'attaque par un ransomware. (Le fichier identifié comme ayant subi une attaque par ransomware est supprimé 1 jour après son remplacement.)

Les analyses par ransomware se produisent à 3 points lors du processus de sauvegarde et de restauration :

- Lorsqu'un fichier de sauvegarde est créé

  Le scan n'est pas effectué sur le fichier de sauvegarde lors de l'écriture initiale sur le stockage cloud, mais lorsque le fichier de sauvegarde **Next** est écrit. Par exemple, si vous avez défini un programme de sauvegarde hebdomadaire pour mardi, le mardi 14, une sauvegarde est créée. Puis, mardi, une nouvelle sauvegarde est créée. Le scan par ransomware est alors exécuté sur le fichier de sauvegarde depuis le 14.

- Lorsque vous tentez de restaurer des données à partir d'un fichier de sauvegarde

  Vous pouvez choisir d'exécuter une analyse avant de restaurer les données d'un fichier de sauvegarde ou d'ignorer cette analyse.

- Manuellement

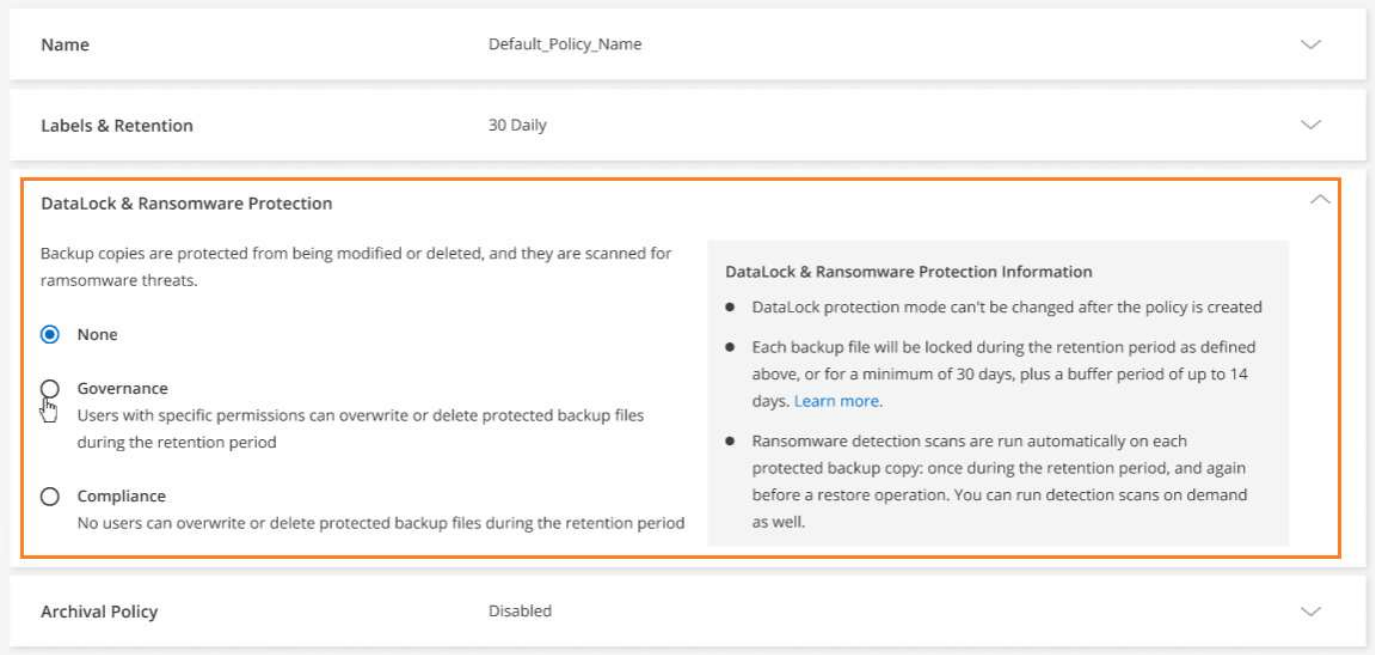
  Vous pouvez à tout moment exécuter une analyse de protection par ransomware à la demande pour

vérifier l'état d'un fichier de sauvegarde spécifique. Ceci peut être utile si vous avez rencontré un problème de ransomware sur un volume en particulier et que vous souhaitez vérifier que les sauvegardes de ce volume ne sont pas affectées.

Une analyse par ransomware requiert que le fichier de sauvegarde soit téléchargé dans votre environnement BlueXP (où le connecteur est installé). En cas de déploiement de votre connecteur sur site, vous pouvez donc prévoir des coûts de sortie supplémentaires de votre fournisseur de cloud. Nous vous recommandons donc de déployer le connecteur dans le cloud et d'utiliser la même région que le compartiment dans lequel vos sauvegardes sont stockées.

Paramètres de verrouillage des données et de protection contre les ransomwares

Chaque stratégie de sauvegarde fournit une section pour *DataLock et protection contre les attaques par ransomware* que vous pouvez appliquer à vos fichiers de sauvegarde.



Vous pouvez choisir parmi les paramètres suivants pour chaque stratégie de sauvegarde :

- Aucun (par défaut)

  La protection contre les verrous et les attaques par ransomware sont désactivées.

- Gouvernance (non disponible avec StorageGRID)

  DataLock est défini sur *Governance* mode où les utilisateurs avec des autorisations spécifiques ("voir ci-dessous") peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

- La conformité

  DataLock est défini sur le mode *Compliance*, où aucun utilisateur ne peut écraser ou supprimer des fichiers de sauvegarde pendant la période de rétention. La protection contre les ransomwares est activée.

La fonction de verrouillage d'objet StorageGRID S3 fournit un mode de verrouillage de données unique équivalent au mode de conformité. Un mode de gouvernance équivalent n'est pas pris en charge. Par conséquent, aucun utilisateur n'a la possibilité de contourner les paramètres de rétention, d'écraser les sauvegardes protégées ou de supprimer les sauvegardes verrouillées.

Environnements de travail et fournisseurs de stockage objet pris en charge

Vous pouvez activer la protection des données et des attaques par ransomware sur les volumes ONTAP à partir de plusieurs environnements de travail lorsque vous utilisez le stockage objet dans plusieurs fournisseurs de cloud public et privé. D'autres fournisseurs de cloud seront ajoutés dans les prochaines versions.

Environnement de travail source	Destination du fichier de sauvegarde ifdef::aws[]
Cloud Volumes ONTAP dans AWS	Amazon S3 endif::aws[] ifdef::Azure[] endif::Azure[] ifdef::gcp[] endif::gcp[]
Système ONTAP sur site	Ifdef::aws[] Amazon S3 endif::aws[] ifdef::Azure[] endif::Azure[] ifdef::gcp[] fdef::gcp[] dnif::gcp[] NetApp StorageGRID

De formation

- Vos clusters doivent exécuter ONTAP 9.11.1 ou version supérieure
- Vous devez utiliser BlueXP 3.9.21 ou supérieur
- Pour StorageGRID :
  - Le connecteur doit être déployé sur votre site (il peut être installé sur un site avec ou sans accès Internet)
  - StorageGRID 11.6.0.3 et supérieur sont requis pour la prise en charge complète des capacités de verrouillage de données

Restrictions

- Data Lock et protection contre les attaques par ransomware n'est pas disponible si vous avez configuré le stockage d'archivage dans la stratégie de sauvegarde.
- L'option DataLock que vous sélectionnez lors de l'activation de Cloud Backup (gouvernance ou conformité) doit être utilisée pour toutes les stratégies de sauvegarde de ce cluster. Vous ne pouvez pas utiliser le verrouillage des modes gouvernance et conformité sur un seul cluster.
- Si vous activez DataLock, toutes les sauvegardes de volume seront verrouillées. Vous ne pouvez pas combiner des sauvegardes de volume verrouillées et non verrouillées pour un même cluster.
- La protection des données et des attaques par ransomware est applicable pour les nouvelles sauvegardes de volumes grâce à une stratégie de sauvegarde avec DataLock et protection contre les attaques par ransomware activées. Vous ne pouvez pas activer cette fonctionnalité après l'activation de Cloud Backup.

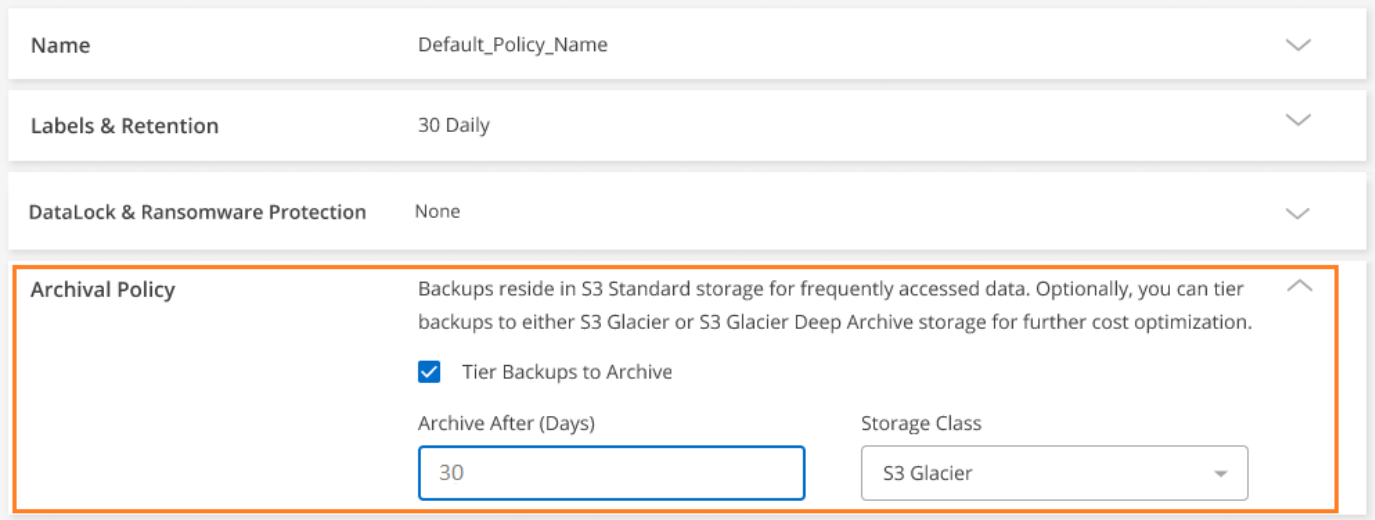
Paramètres de stockage d'archivage

Si vous utilisez un certain stockage cloud, vous pouvez déplacer d'anciens fichiers de sauvegarde vers un Tier de stockage/accès moins onéreux après un certain nombre de jours. Notez que le stockage d'archives ne peut pas être utilisé si vous avez activé DataLock.

Les données des niveaux d'archivage ne sont pas accessibles immédiatement lorsque cela s'avère

nécessaire. Par conséquent, les coûts de récupération des données sont plus élevés, vous devez déterminer la fréquence à laquelle restaurer les données à partir des fichiers de sauvegarde archivés.

Lors de la création de fichiers de sauvegarde dans AWS ou Azure, chaque règle de sauvegarde fournit une section intitulée *Archival* que vous pouvez appliquer à vos fichiers de sauvegarde.



- Dans GCP, les sauvegardes sont associées par défaut à la classe de stockage *Standard*.

  Vous pouvez utiliser la classe de stockage *Nearline* moins chère ou les classes de stockage *Coldline* ou *Archive*. Toutefois, vous configurez ces autres classes de stockage via Google, et non via l'interface utilisateur de Cloud Backup. Consultez la rubrique Google "Classes de stockage" Pour plus d'informations sur la modification de la classe de stockage par défaut d'un compartiment Google Cloud Storage.

- Dans StorageGRID, les sauvegardes sont associées à la classe de stockage *Standard*.

  Il n'y a pas de niveau d'archivage disponible pour le moment.

Classes de stockage d'archivage AWS S3 et délais de récupération des données

Cloud Backup prend en charge deux classes de stockage d'archivage S3 ainsi que la plupart des régions.

Classes de stockage d'archivage S3 prises en charge pour Cloud Backup

Lorsque des fichiers de sauvegarde sont créés initialement, ils sont stockés dans le stockage S3 *Standard*. Il est optimisé pour stocker les données peu utilisées, mais vous pouvez également y accéder immédiatement. Après 30 jours, les sauvegardes passent à la classe de stockage S3 *Standard-Infrequent Access* pour réduire les coûts.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes vers un stockage *S3 Glacier* ou *S3 Glacier Deep Archive* après un certain nombre de jours (généralement plus de 30 jours) pour optimiser les coûts. Les données de ces niveaux ne sont pas accessibles immédiatement lorsque cela s'avère nécessaire. Par conséquent, les coûts de récupération sont plus élevés, vous devez déterminer la fréquence à laquelle vous devrez peut-être restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section à propos de data from archival

storage,restauration des données à partir du stockage d'archivage.

Si vous choisissez *S3 Glacier* ou *S3 Glacier Deep Archive* dans votre première stratégie de sauvegarde lors de l'activation de Cloud Backup, ce Tier sera le seul niveau d'archivage disponible pour les futures stratégies de sauvegarde de ce cluster. Si vous sélectionnez aucun niveau d'archivage dans votre première stratégie de sauvegarde, alors *S3 Glacier* sera votre seule option d'archivage pour les futures stratégies.

Notez que, lorsque vous configurez Cloud Backup avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du compartiment dans votre compte AWS.

"Découvrez les classes de stockage S3".

Restauration des données à partir du stockage d'archivage

Le stockage de fichiers de sauvegarde plus anciens dans un stockage d'archivage est bien moins coûteux que le stockage Standard ou Standard-IA. L'accès aux données à partir d'un fichier de sauvegarde dans un stockage d'archivage à des fins de restauration prendra plus de temps et coûtera plus d'argent.

Combien coûte la restauration des données à partir d'Amazon S3 Glacier et d'Amazon S3 Glacier ?

Il existe 3 priorités en matière de restauration pour la récupération des données depuis Amazon S3 Glacier et 2 priorités en matière de restauration lors de la récupération des données depuis Amazon S3 Glacier Deep Archive. Les frais d'archivage en profondeur S3 Glacier sont inférieurs à ceux de S3 Glacier :

Tier d'archivage	Restaurer les priorités et les coûts		
	Haut	**Standard**	**Faible**
Glacier S3	Récupération plus rapide, coût le plus élevé	Récupération plus lente, coûts réduits	Récupération la plus lente, coût le plus bas
Archive en profondeur du glacier S3		Récupération plus rapide, coûts supérieurs	Récupération plus lente, coûts réduits

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification S3 Glacier par région AWS, rendez-vous sur le "Page tarifaire d'Amazon S3".

Combien de temps faut-il pour restaurer mes objets archivés dans Amazon S3 Glacier ?

Deux parties composent la durée totale de restauration :

- **Heure de récupération** : le moment de récupérer le fichier de sauvegarde à partir de l'archive et de le placer dans le stockage standard. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie.

Tier d'archivage	Restauration de la priorité et de l'heure de récupération		
	Haut	**Standard**	**Faible**
Glacier S3	3-5 minutes	3-5 heures	5-12 heures
Archive en profondeur du glacier S3		12 heures	48 heures

- **Temps de restauration** : temps de restauration des données à partir du fichier de sauvegarde dans le stockage standard. Ce temps n'est pas différent de l'opération de restauration standard directement depuis le stockage standard - lorsque vous n'utilisez pas de niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Amazon S3 Glacier et S3 Glacier Deep Archive, consultez "Forum aux questions d'Amazon sur ces classes de stockage".

Niveaux d'archivage Azure et délais de récupération

Cloud Backup prend en charge un Tier d'accès d'archivage Azure ainsi que la plupart des régions.

Tiers d'accès Azure Blob pris en charge pour la sauvegarde dans le cloud

Lorsque les fichiers de sauvegarde sont créés initialement, ils sont stockés dans le niveau d'accès *Cool*. Il est optimisé pour le stockage des données rarement utilisées, mais à la demande, il est possible d'y accéder immédiatement.

Si vos clusters source exécutent ONTAP 9.10.1 ou version ultérieure, vous pouvez choisir de classer les sauvegardes entre *Cool* et *Azure Archive* Storage après un certain nombre de jours (généralement plus de 30 jours) afin d'optimiser les coûts. Vous n'avez pas accès immédiatement aux données de ce niveau quand vous en avez besoin. Par conséquent, vos coûts de récupération sont plus élevés. Vous devez donc déterminer la fréquence à laquelle vous devrez restaurer les données à partir de ces fichiers de sauvegarde archivés. Reportez-vous à la section suivante sur data from archival storage,restauration des données à partir du stockage d'archivage.

Notez que lorsque vous configurez Cloud Backup avec ce type de règle de cycle de vie, vous ne devez pas configurer de règles de cycle de vie lors de la configuration du conteneur dans votre compte Azure.

"Découvrez les niveaux d'accès d'Azure Blob".

Restauration des données à partir du stockage d'archivage

Le stockage d'anciens fichiers de sauvegarde dans des archives est bien moins coûteux que le stockage Cool, mais l'accès aux données à partir d'un fichier de sauvegarde dans Azure Archive à des fins de restauration prendra plus de temps et coûtera plus cher.

Combien coûte la restauration des données à partir d'Azure Archive ?

Vous pouvez choisir deux priorités en matière de restauration lors de la récupération des données à partir d'Azure Archive :

- **Élevé**: Récupération la plus rapide, coût plus élevé
- **Standard** : récupération plus lente, coût moindre

Chaque méthode propose des frais de récupération différents par Go et par demande. Pour en savoir plus sur la tarification d'Azure Archive par région Azure, rendez-vous sur la "Page tarifaire d'Azure".

Quel est le délai de restauration des données archivées dans Azure Archive ?

La durée de restauration est fonction de deux parties :

- **Temps de récupération** : le temps de récupérer le fichier de sauvegarde archivé à partir d'Azure Archive et de le placer dans Cool Storage. Ce temps est parfois appelé le temps de « réhydratation ». La durée de récupération varie en fonction de la priorité de restauration choisie :
  - **Haut**: < 1 heure
  - **Standard**: < 15 heures

- **Restore Time** : le temps de restauration des données à partir du fichier de sauvegarde dans Cool Storage. Ce temps n'est pas différent de l'opération de restauration typique directement depuis Cool Storage - lorsque vous n'utilisez pas un niveau d'archivage.

Pour plus d'informations sur les options de récupération d'Azure Archive, reportez-vous à "Forum aux questions sur Azure".

Configurer la sauvegarde pour l'accès à plusieurs comptes dans Azure

Avec Cloud Backup, vous pouvez créer des fichiers de sauvegarde dans un compte Azure différents de l'emplacement de vos volumes Cloud Volumes ONTAP source. Et ces deux comptes peuvent être différents du compte où réside le connecteur BlueXP.

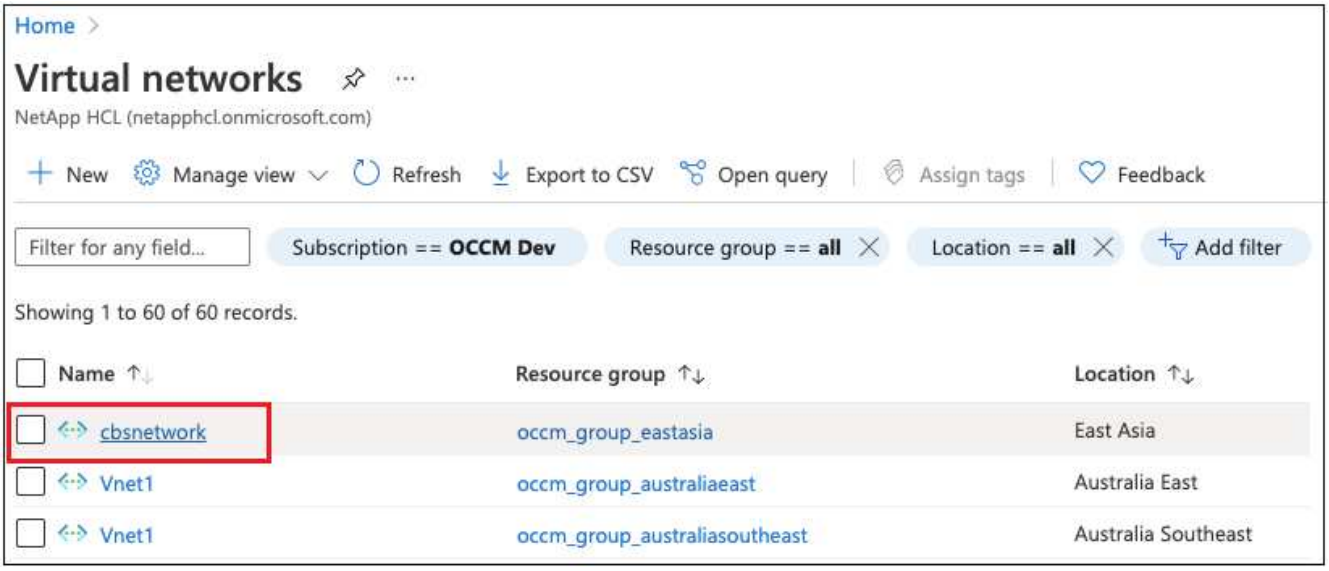
Ces étapes sont requises uniquement lorsque vous l'êtes "Sauvegarde des données Cloud Volumes ONTAP dans le stockage Azure Blob".

Suivez simplement les étapes ci-dessous pour configurer votre configuration de cette façon.

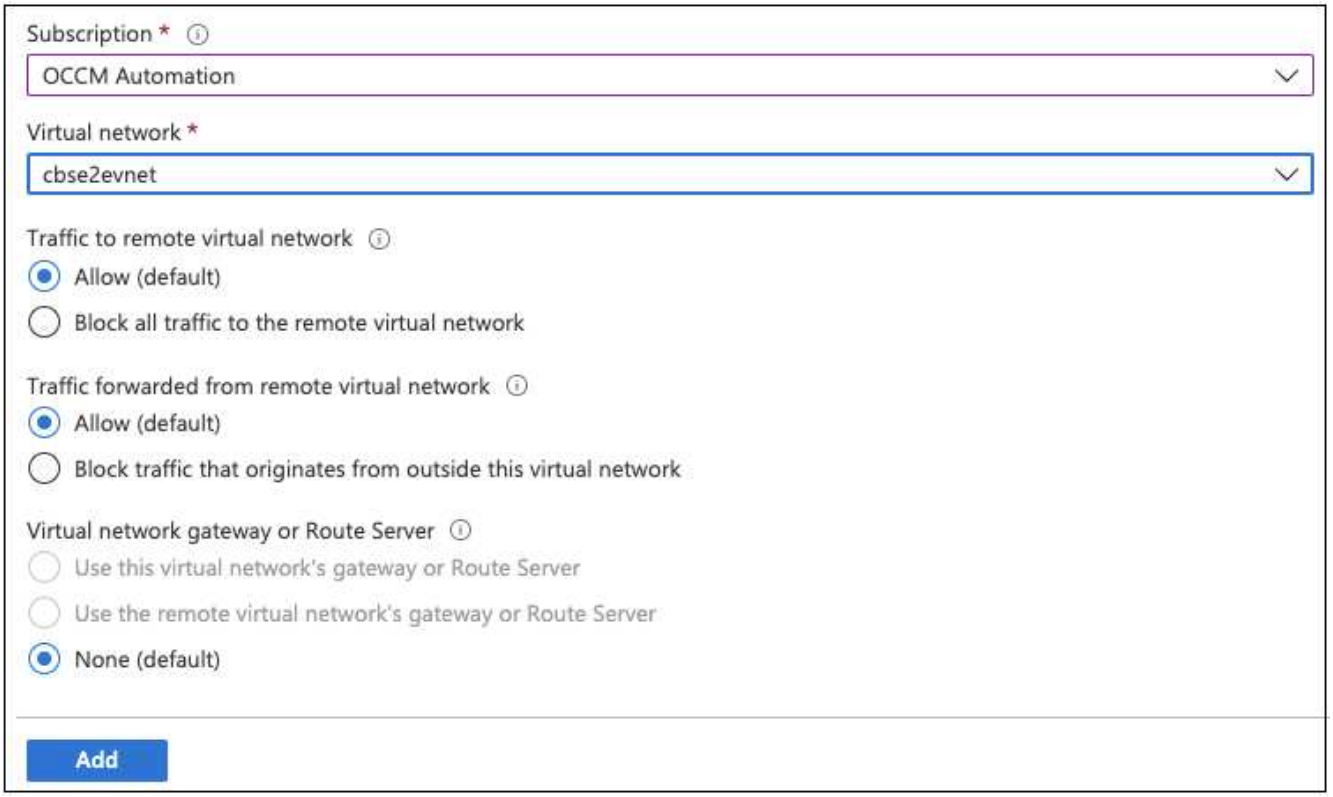
Configurez le peering de vnet entre comptes

Notez que si vous souhaitez que BlueXP gère votre système Cloud Volumes ONTAP dans un autre compte/région, vous devez configurer VNet peering. Le peering de vnet n'est pas requis pour la connectivité du compte de stockage.

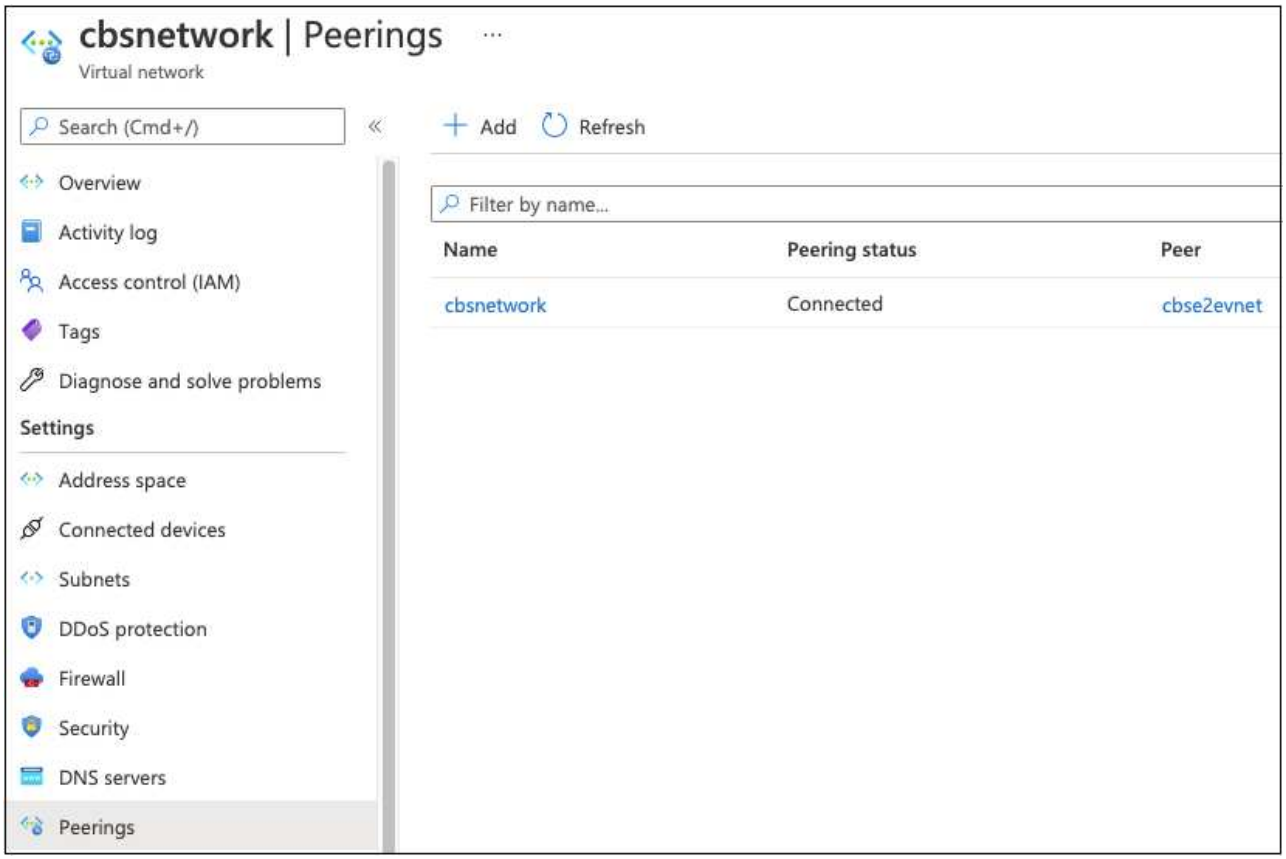
1. Connectez-vous au portail Azure et depuis domicile, sélectionnez Virtual Networks.
2. Sélectionnez l'abonnement que vous utilisez en tant qu'abonnement 1 et cliquez sur le vnet où vous souhaitez configurer le peering.



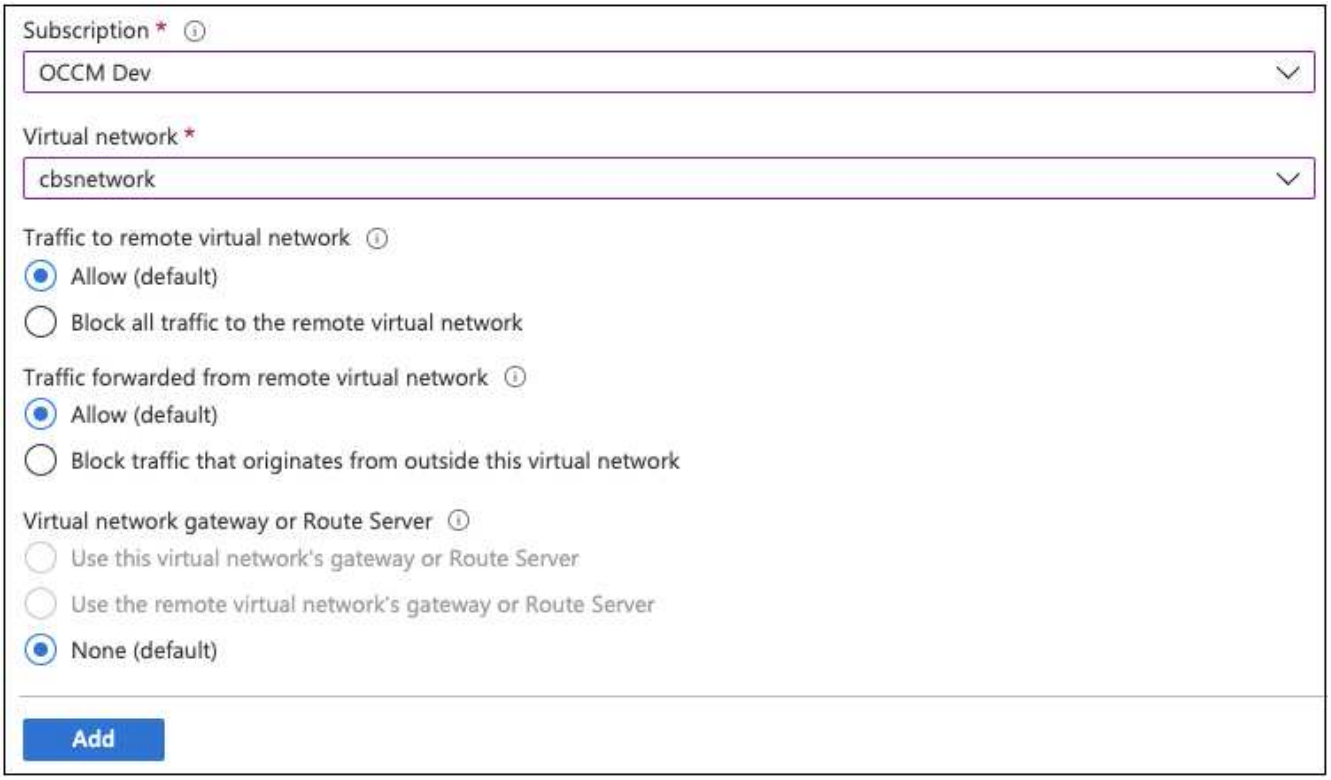
3. Sélectionnez **cbsnetwork** et, dans le panneau de gauche, cliquez sur **Peerings**, puis cliquez sur **Add**.



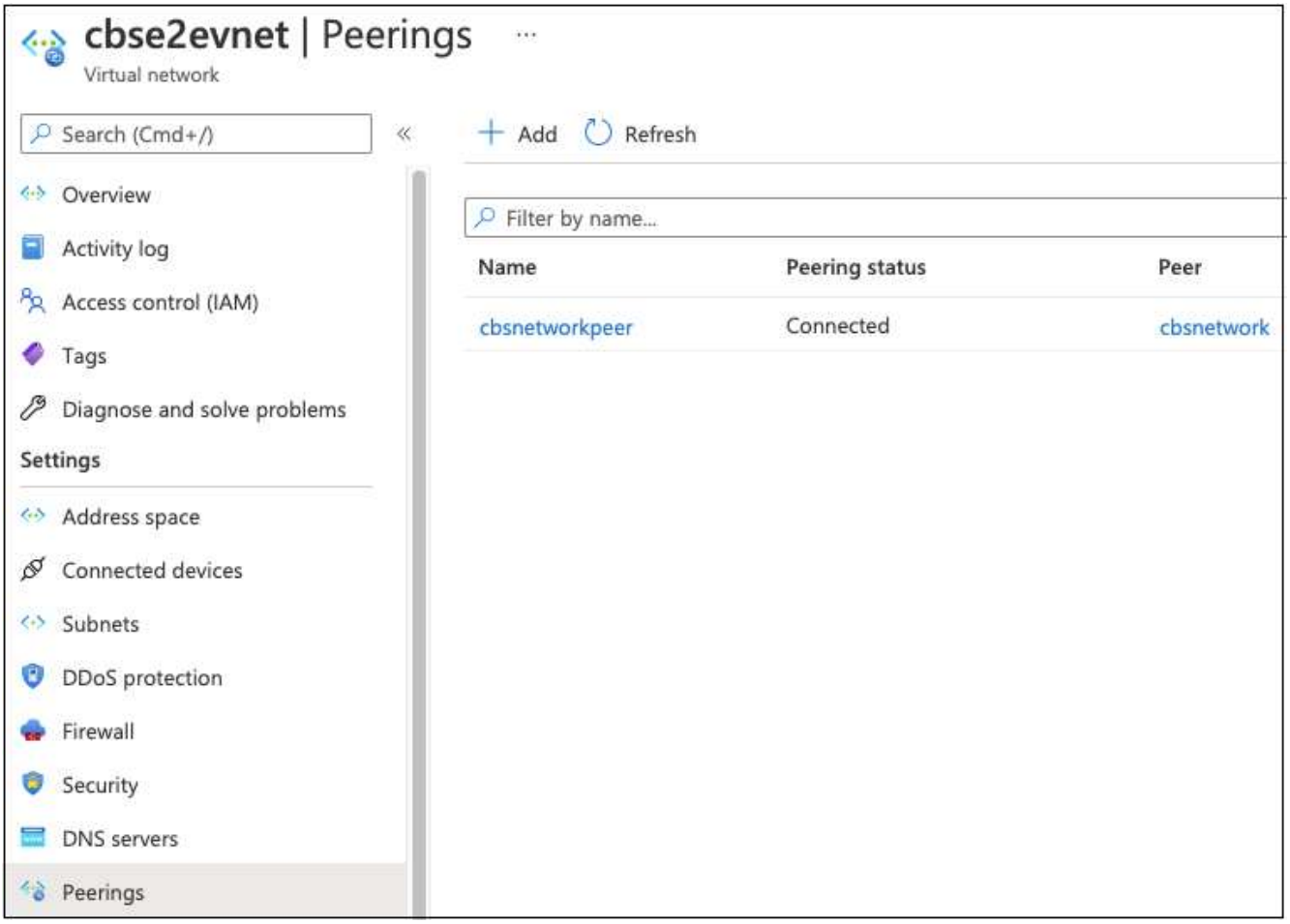
4. Entrez les informations suivantes sur la page peering, puis cliquez sur **Ajouter**.
   - Nom de la liaison de peering pour ce réseau : vous pouvez donner un nom quelconque afin d'identifier la connexion de peering.
   - Nom de la liaison de peering de réseau virtuel distant : entrez un nom pour identifier le vnet distant.
   - Conserver toutes les sélections comme valeurs par défaut.
   - Sous abonnement, sélectionnez l'abonnement 2.
   - Réseau virtuel, sélectionnez le réseau virtuel dans l'abonnement 2 auquel vous souhaitez configurer le peering.



5. Effectuez les mêmes étapes dans Subscription 2 VNet et spécifiez les détails de l'abonnement et de vnet distant de l'abonnement 1.



Les paramètres de peering sont ajoutés.



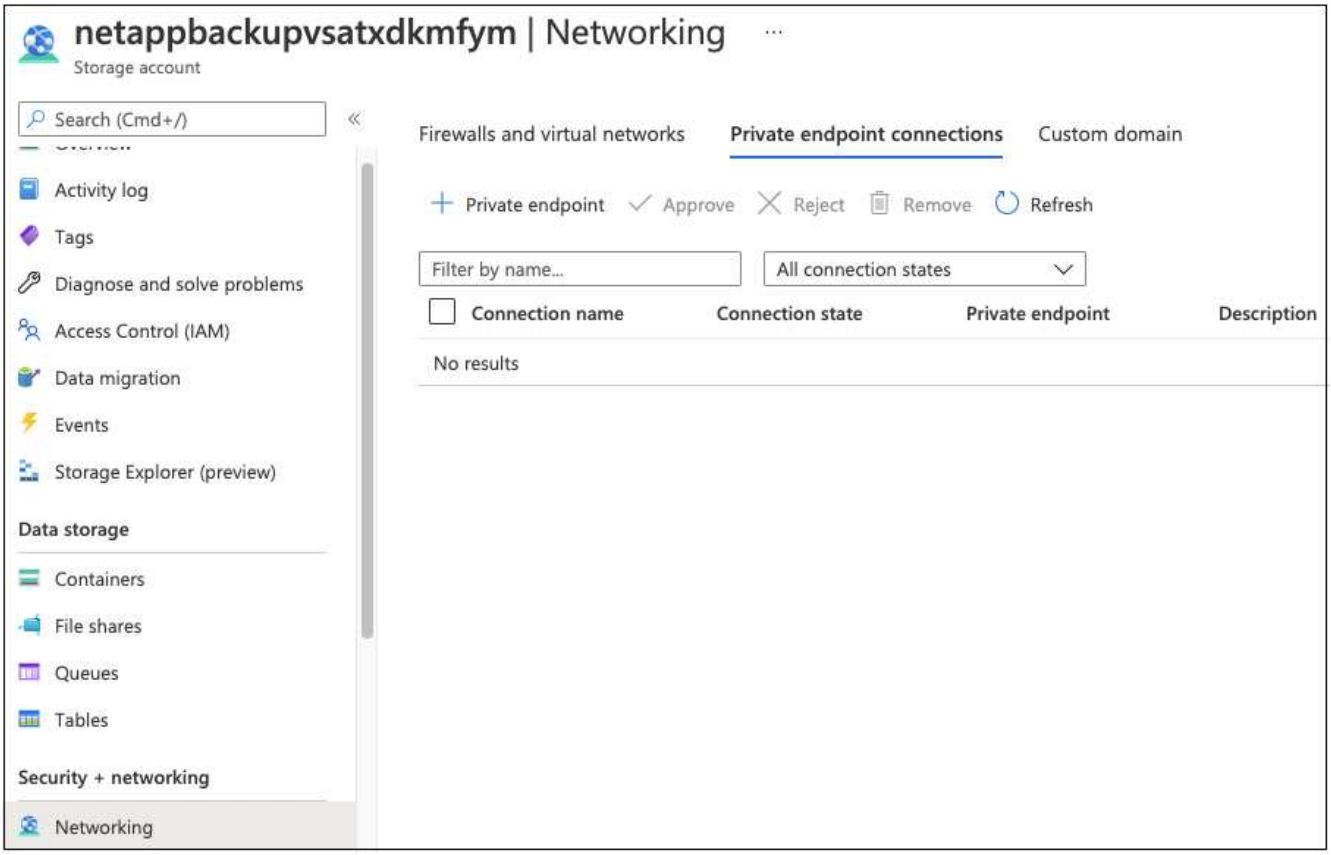
Créez un terminal privé pour le compte de stockage

Il est maintenant nécessaire de créer un terminal privé pour le compte de stockage. Dans cet exemple, le compte de stockage est créé dans l'abonnement 1 et le système Cloud Volumes ONTAP fonctionne dans l'abonnement 2.

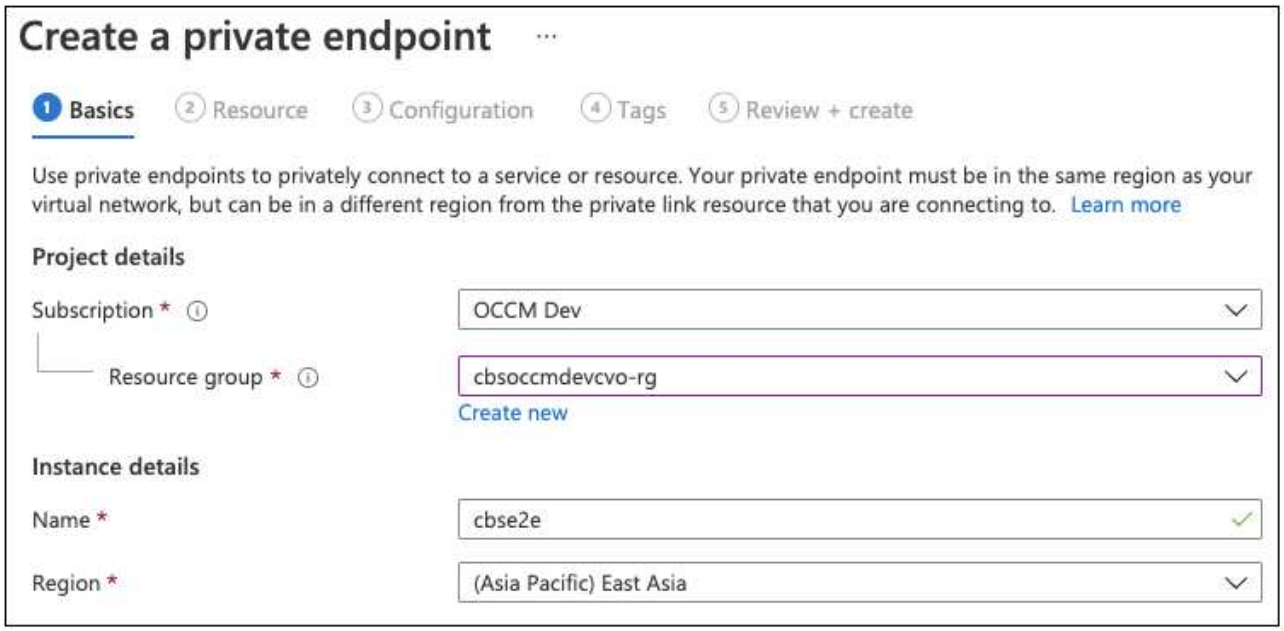
Vous avez besoin de l'autorisation de contributeur réseau pour effectuer l'action suivante.

```
{
  "id": "/subscriptions/d333af45-0d07-4154-
943dc25fbbce1b18/providers/Microsoft.Authorization/roleDefinitions/4d97b98
b-1d4f-4787-a291-c67834d212e7",
  "properties": {
    "roleName": "Network Contributor",
    "description": "Lets you manage networks, but not access to them.",
    "assignableScopes": [
      "/"
    ],
    "permissions": [
      {
        "actions": [
          "Microsoft.Authorization/*/read",
          "Microsoft.Insights/alertRules/*",
          "Microsoft.Network/*",
          "Microsoft.ResourceHealth/availabilityStatuses/read",
          "Microsoft.Resources/deployments/*",
          "Microsoft.Resources/subscriptions/resourceGroups/read",
          "Microsoft.Support/*"
        ],
        "notActions": [],
        "dataActions": [],
        "notDataActions": []
      }
    ]
  }
}
```

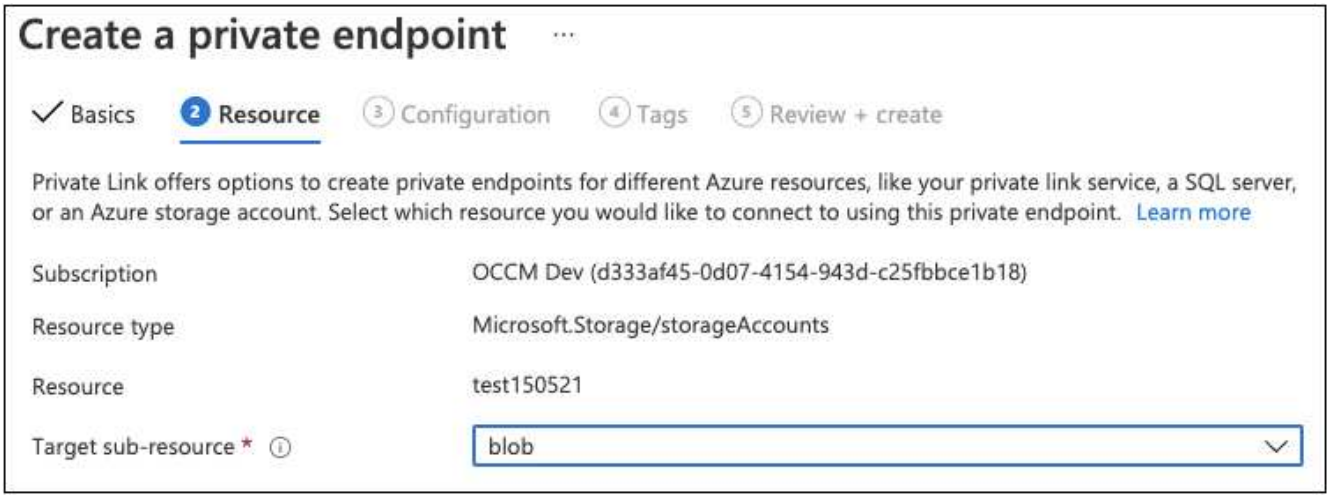
1. Accédez au compte de stockage > réseau > connexions de noeuds finaux privés et cliquez sur **+ noeud final privé**.



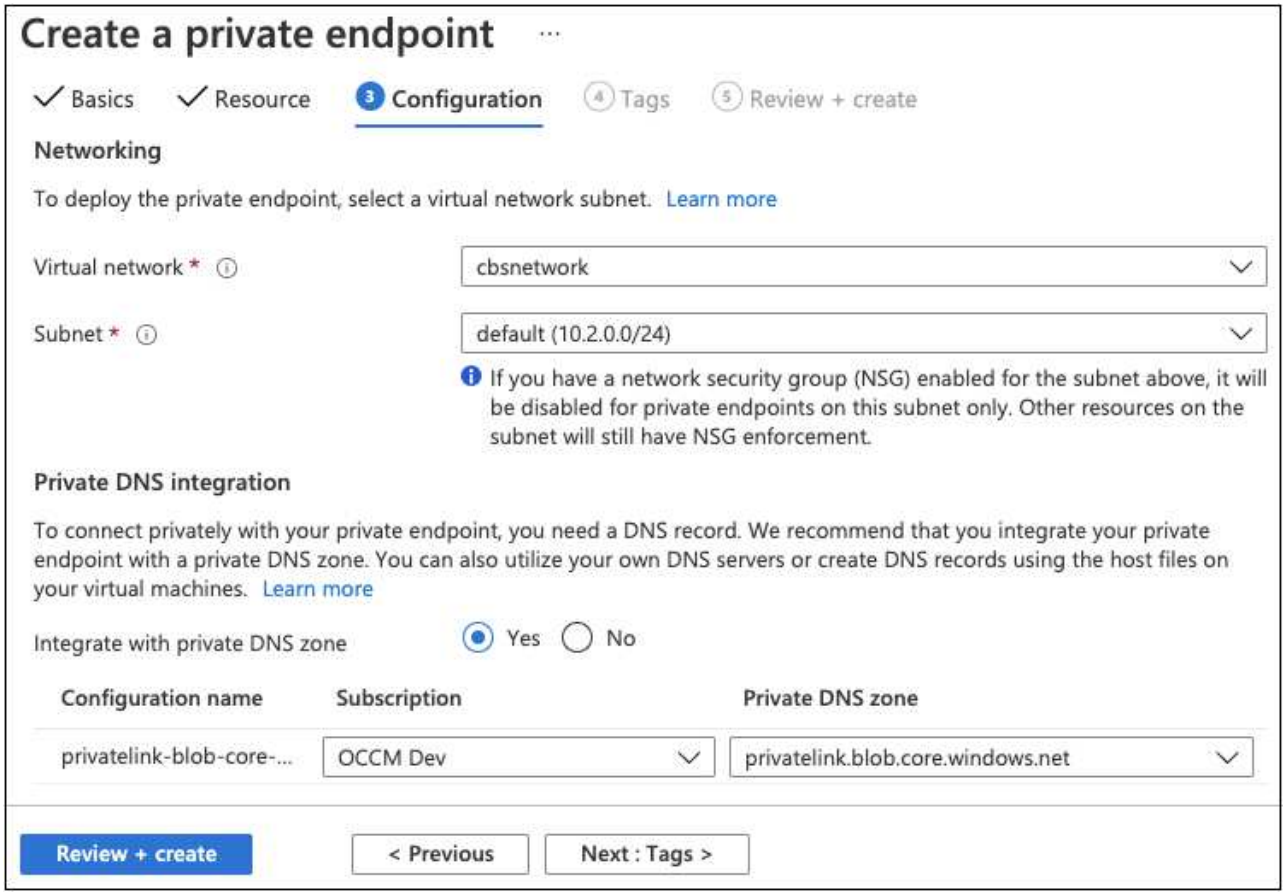
2. Dans la page Private Endpoint *Basics* :
   - Sélectionnez l'abonnement 2 (où le connecteur BlueXP et le système Cloud Volumes ONTAP sont déployés) et le groupe de ressources.
   - Entrez un nom de point final.
   - Sélectionnez la région.



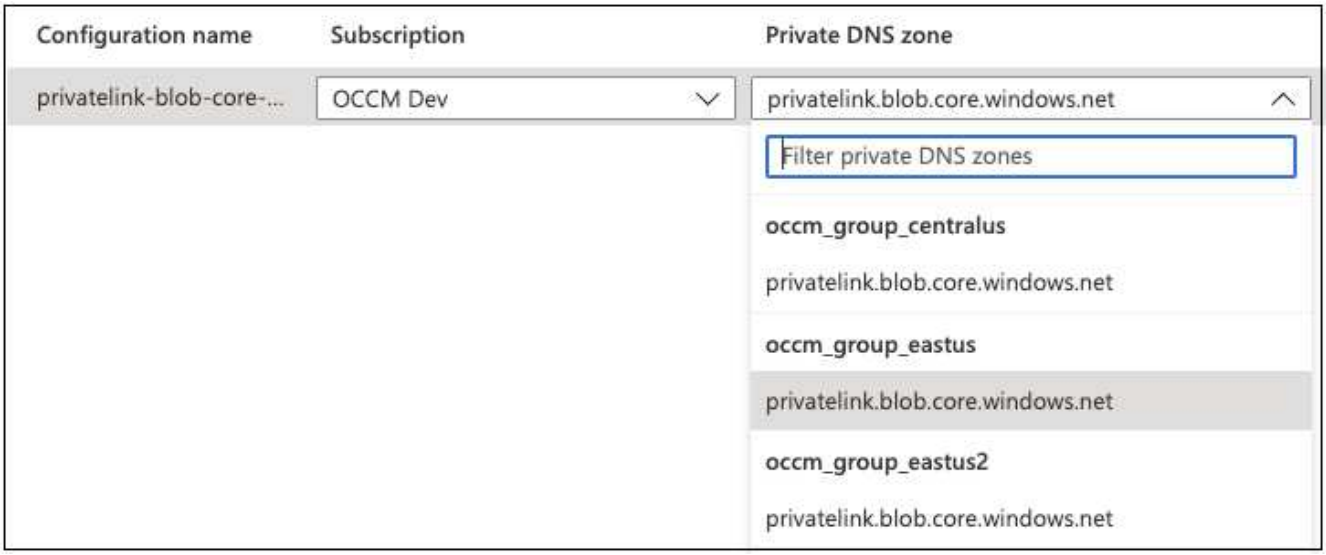
3. Dans la page *Resource*, sélectionnez sous-ressource cible comme **blob**.



4. Dans la page Configuration :
   - Sélectionnez le réseau virtuel et le sous-réseau.
   - Cliquez sur le bouton radio **Oui** pour "intégrer à la zone DNS privée".



5. Dans la liste zone DNS privée, assurez-vous que la zone privée est sélectionnée dans la région correcte, puis cliquez sur **Revue + Créer**.



Désormais, le compte de stockage (dans l'abonnement 1) a accès au système Cloud Volumes ONTAP exécuté dans l'abonnement 2.

6. Réessayez d'activer la sauvegarde dans le cloud sur le système Cloud Volumes ONTAP. Cette fois-ci, vous devriez réussir.