



FlexPod Cloud hybride pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

FlexPod

NetApp
January 21, 2025

Sommaire

FlexPod Cloud hybride pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco
Intersight. 1

 Tr-4939 : Cloud hybride FlexPod pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et
 Cisco Intersight. 1

 Composants de la solution. 3

 Installation et configuration 8

 Validation des solutions 75

 Conclusion 83

FlexPod Cloud hybride pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Tr-4939 : Cloud hybride FlexPod pour Google Cloud Platform avec NetApp Cloud Volumes ONTAP et Cisco Intersight

Ruchika Lahoti, NetApp

Introduction

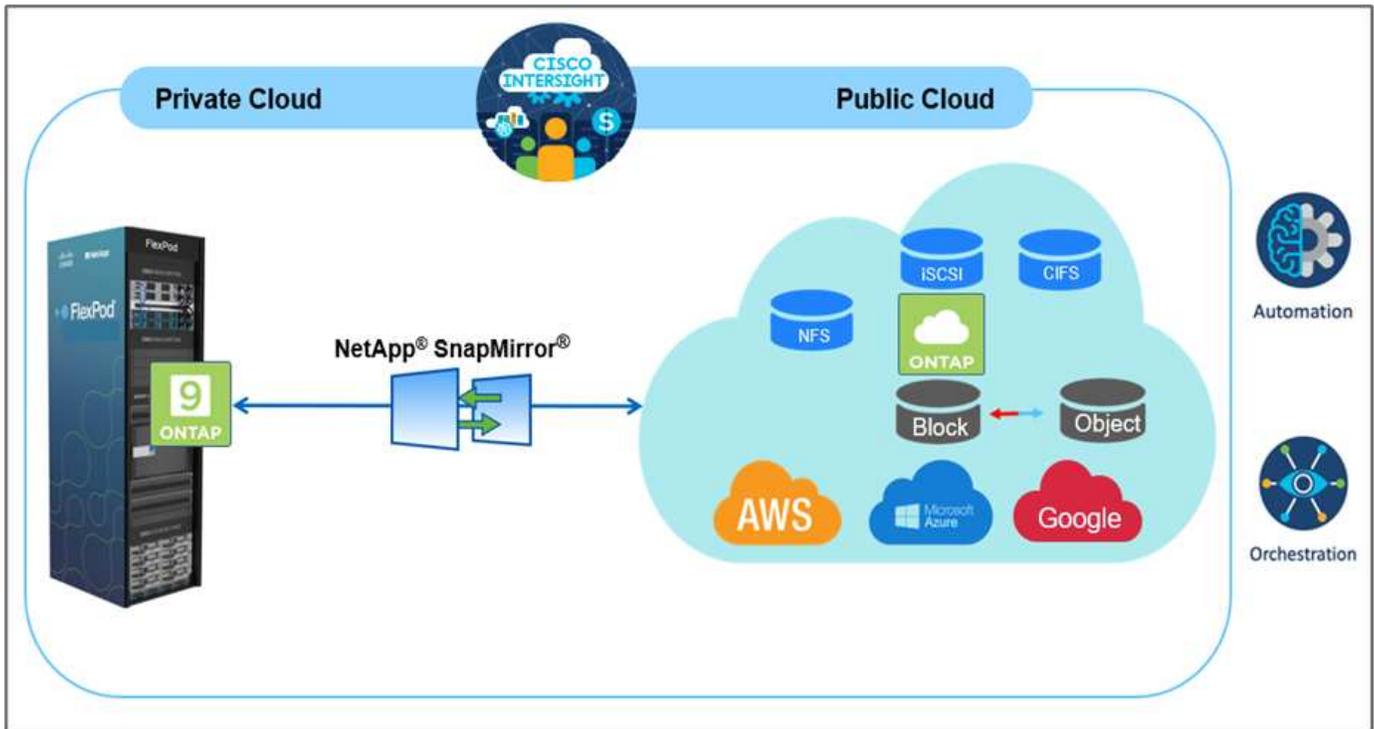
L'objectif de protection des données avec reprise après incident est essentiel à la continuité de l'activité. La reprise d'activité permet aux entreprises de basculer leurs opérations sur un emplacement secondaire, puis de restaurer et de rétablir leur fonctionnement vers le site primaire de manière efficace et fiable. Le développement d'une stratégie de reprise après incident est une priorité IT si l'on persiste avec plusieurs problèmes tels que les catastrophes naturelles, les défaillances réseau, les vulnérabilités logicielles et les erreurs humaines.

Pour la reprise après incident, toutes les charges de travail exécutées sur le site primaire doivent être fidèlement reproduites sur le site de DR. Une entreprise doit également disposer d'une copie à jour de toutes les données d'entreprise, y compris la base de données, les services de fichiers, le stockage NFS et iSCSI, etc. Comme les données de l'environnement de production sont constamment mises à jour, les modifications doivent être régulièrement transférées vers le site de reprise.

Néanmoins, pour la plupart des entreprises, déployer de tels environnements de reprise est difficile à concilier avec les exigences d'indépendance de l'infrastructure et du site. Le nombre de ressources requises et les coûts de configuration, de test et de maintenance d'un data Center secondaire peuvent être très élevés, ce qui approche généralement du coût de l'ensemble de l'environnement de production. Il est difficile de minimiser l'empreinte des données avec une protection adéquate, tout en synchronisant les données en continu et en établissant des basculements et des rétablissements transparents. Une fois le site de reprise créé, un autre défi se présente : répliquer les données depuis l'environnement de production et les synchroniser dans la suite.

Ce rapport technique rassemble la solution d'infrastructure convergée FlexPod, NetApp Cloud Volumes ONTAP sur Google Cloud et Cisco Intersight pour former un data Center dans le cloud hybride pour la reprise après incident. Dans cette solution, nous abordons la conception et l'exécution d'un workflow ONTAP sur site à l'aide de Cisco Intersight Cloud Orchestrator. Nous discutons également du déploiement de NetApp Cloud Volumes ONTAP et de l'orchestration et l'automatisation de la réplication et de la reprise après incident des données entre FlexPod et Cloud Volumes ONTAP à l'aide du service Cisco Intersight pour HashiCorp Terraform.

Le schéma suivant fournit une présentation de la solution.



Cette solution offre de nombreux avantages, notamment :

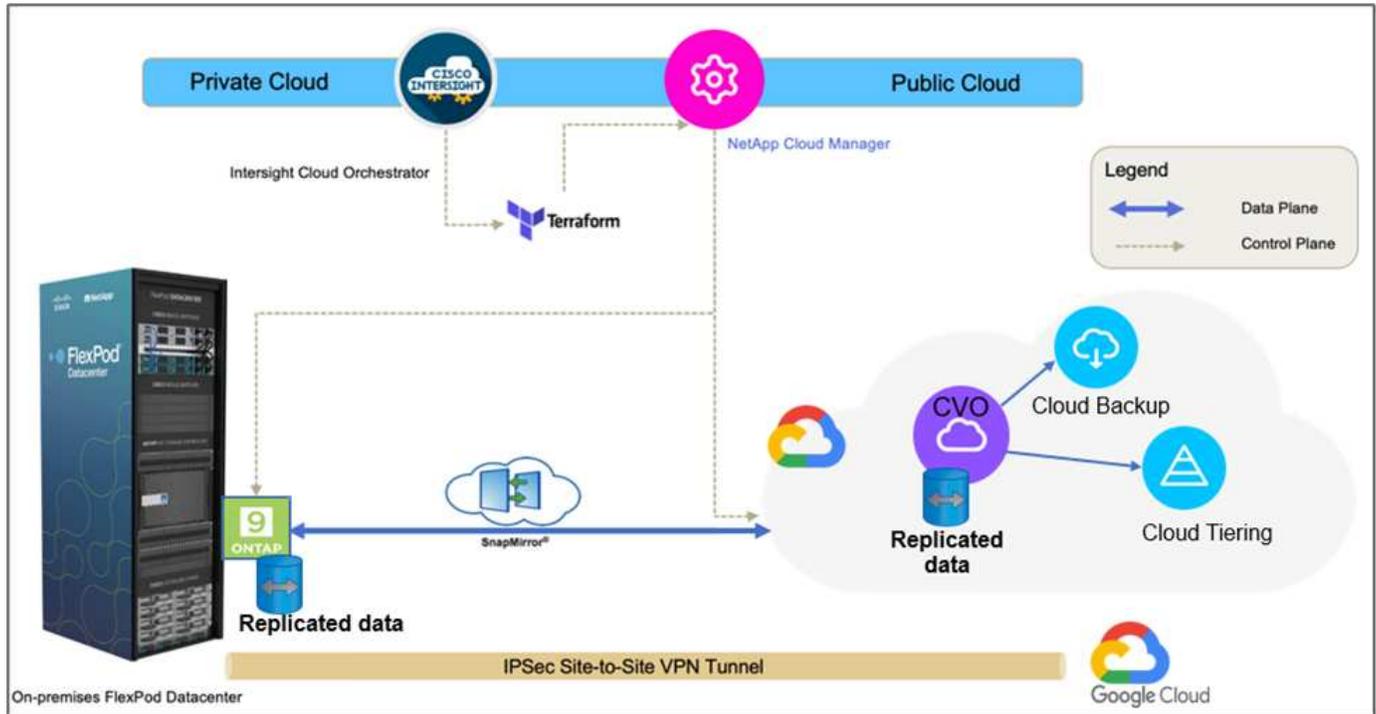
- **Orchestration et automatisation.** Cisco Intersight simplifie les opérations quotidiennes de l'infrastructure de cloud hybride FlexPod en fournissant des frameworks d'orchestration cohérents qui sont proposés via l'automatisation.
- **Protection personnalisée.** Cloud Volumes ONTAP assure la réplication des données au niveau des blocs depuis ONTAP vers le cloud afin de maintenir la destination à jour grâce à des mises à jour incrémentielles. Les utilisateurs peuvent spécifier une planification de synchronisation toutes les 5 minutes ou toutes les heures, par exemple, en fonction des modifications de la source qui sont transférées.
- **Basculement et retour arrière transparents** en cas d'incident, les administrateurs du stockage peuvent rapidement basculer vers les volumes cloud. Lorsque le site primaire est restauré, les nouvelles données créées dans l'environnement de reprise sont resynchronisées sur les volumes source et re-établissent la réplication secondaire.
- **Efficacité :** l'espace de stockage et les coûts pour la copie cloud secondaire sont optimisés grâce à la compression des données, au provisionnement fin et à la déduplication. Les données sont transférées au niveau du bloc sous forme compressée et dédoublée, ce qui accélère le transfert. Ainsi, les données sont automatiquement transférées vers un stockage objet à faible coût et sont transférées vers un stockage haute performance uniquement lors des accès, comme dans un scénario de reprise après incident. Ceci réduit considérablement les coûts réguliers de stockage.
- * Augmentation de la productivité INFORMATIQUE.* l'utilisation d'Intersight comme plateforme d'entreprise unique et sécurisée pour la gestion du cycle de vie de l'infrastructure et des applications simplifie la gestion de la configuration et l'automatisation des tâches manuelles à grande échelle pour la solution.

Public

Le public visé peut inclure, sans s'y limiter, les ingénieurs commerciaux, les consultants sur le terrain, les services professionnels, les responsables INFORMATIQUES, Ingénieurs partenaires, ingénieurs de fiabilité des sites, architectes cloud, ingénieurs cloud et clients qui souhaitent exploiter une infrastructure conçue pour optimiser l'efficacité IT et favoriser l'innovation IT.

Topologie de la solution

Cette section décrit la topologie logique de la solution. La figure ci-dessous illustre la topologie de la solution de l'environnement FlexPod sur site, de NetApp Cloud Volumes ONTAP exécuté sur Google Cloud, Cisco Intersight et NetApp Cloud Manager.



Les plans de contrôle et les plans de données sont clairement indiqués entre les points d'extrémité. Le plan de données utilise une connexion VPN site à site sécurisée pour connecter l'instance ONTAP exécutée sur FlexPod FAS 100 % Flash à l'instance NetApp Cloud Volumes ONTAP sur Google Cloud.

La réplication des données de charge de travail de FlexPod vers NetApp Cloud Volumes ONTAP est gérée par NetApp SnapMirror. Le processus global est orchestré à l'aide de Cisco Intersight Cloud Orchestrator pour les environnements sur site et cloud. Cisco Intersight Cloud Orchestrator utilise les fournisseurs de ressources Terraform pour NetApp Cloud Manager pour effectuer des opérations liées au déploiement de NetApp Cloud Volumes ONTAP et établir des relations de réplication des données.



Cette solution prend également en charge la sauvegarde et le Tiering des données inactives résidant dans l'instance NetApp Cloud Volumes ONTAP vers Google Cloud Storage.

"Ensuite, les composants de la solution."

Composants de la solution

"Précédent : présentation de la solution."

FlexPod

FlexPod est un ensemble défini de matériels et de logiciels qui constitue une base intégrée pour les solutions virtualisées et non virtualisées. FlexPod inclut le stockage NetApp ONTAP, les réseaux Cisco Nexus, les réseaux de stockage Cisco MDS et Cisco Unified Computing System (Cisco UCS). La conception est suffisamment flexible pour que le réseau, le calcul et le stockage puissent s'intégrer dans un seul rack de data

Center ou être déployés selon la conception du centre de données du client. La densité des ports permet aux composants réseau de prendre en charge plusieurs configurations.

Cisco Intersight

Cisco Intersight est une plateforme SaaS qui assure une automatisation, une observabilité et une optimisation intelligentes pour les applications et l'infrastructure classiques et cloud. La plateforme permet de stimuler les évolutions avec les équipes IT et propose un modèle d'exploitation conçu pour le cloud hybride. Cisco Intersight offre les avantages suivants :

- **Livraison plus rapide.** livraison en tant que service depuis le cloud ou dans le centre de données du client avec des mises à jour fréquentes et une innovation continue, grâce à un modèle de développement logiciel agile. Le client peut ainsi se concentrer sur l'accélération de la livraison pour le secteur d'activité.
- **Opérations simplifiées.** simplifier les opérations en utilisant un seul outil SaaS sécurisé avec inventaire, authentification et API communs pour travailler sur l'ensemble de la pile et tous les emplacements, éliminant ainsi les silos entre les équipes. De la gestion des serveurs physiques et des hyperviseurs sur site aux machines virtuelles, K8s, sans serveur, automatisation, l'optimisation et le contrôle des coûts à la fois sur site et dans les clouds publics.
- **Optimisation continue.** optimisation continue de votre environnement en utilisant l'intelligence fournie par Cisco Intersight sur chaque couche, ainsi que Cisco TAC. Cette intelligence est convertie en actions recommandées et automatisées, qui vous permettent de vous adapter en temps réel à chaque changement : du déplacement des charges de travail et du contrôle de l'état des serveurs physiques aux recommandations de réduction des coûts des clouds publics avec lesquels vous travaillez.

Il existe deux modes d'opérations de gestion possibles avec Cisco Intersight : Umm (UCSM Managed mode) et IMM (Intersight Managed mode). Vous pouvez sélectionner UMM natif ou IMM pour les systèmes Cisco UCS rattachés au fabric lors de la configuration initiale des interconnexions de fabric. Dans cette solution, l'IMM native est utilisé.

Licences Cisco Intersight

Cisco Intersight utilise une licence basée sur un abonnement avec plusieurs niveaux.

Les niveaux de licence Cisco Intersight sont les suivants :

- **Cisco Intersight Essentials.** inclut toutes les fonctionnalités de base ainsi que les fonctionnalités suivantes :
 - Cisco UCS Central
 - Droit Cisco IMC Supervisor
 - Configuration basée sur des règles avec profils de serveur
 - Gestion du firmware
 - Évaluation de la compatibilité avec la liste de compatibilité matérielle (HCL)
- **Cisco Intersight Advantage.** comprend les fonctionnalités du niveau Essentials ainsi que les fonctionnalités suivantes :
 - Widgets, inventaire, capacité, fonctionnalités d'utilisation et corrélation des inventaires interdomaines sur l'ensemble des ressources de calcul physique, réseau, stockage, virtualisation VMware et cloud public AWS.
 - Service de conseil de sécurité Cisco où les clients peuvent recevoir d'importantes alertes de sécurité et des notifications sur site sur les périphériques de point final affectés.

- **Cisco Intersight Premier.** en plus des capacités offertes par le niveau avantage, Cisco Intersight Premier propose les éléments suivants :
 - Intersight Cloud Orchestrator (ICO) pour les ressources de calcul, de réseau, de stockage, de systèmes intégrés, de virtualisation, des plateformes de conteneur et de cloud public
 - Droit d'abonnement complet pour Cisco UCS Director sans frais supplémentaires.

Vous trouverez plus d'informations sur les licences Intersight et les fonctionnalités prises en charge dans chaque licence ["ici"](#).



Dans cette solution, nous utilisons Intersight Cloud Orchestrator et Intersight Service pour HashiCorp Terraform. Ces fonctionnalités sont disponibles pour les utilisateurs disposant de la licence Intersight Premier. Par conséquent, ce niveau de licence doit être activé.

Intégration du cloud Terraform avec ICO

Vous pouvez utiliser Cisco Intersight Cloud Orchestrator (ICO) pour créer et exécuter des workflows qui appellent les API Terraform Cloud (TFC). La tâche Invoke Web API Request prend en charge Terraform Cloud comme cible et peut être configurée avec les API Terraform Cloud via des méthodes HTTP. Le workflow peut donc avoir une combinaison de tâches qui appellent plusieurs API Terraform Cloud à l'aide de tâches API génériques et d'autres opérations. Vous devez disposer d'une licence Premier pour utiliser la fonction ICO.

Assistance Cisco Intersight

Cisco Intersight aide à ajouter des périphériques de terminaison à Cisco Intersight. Un centre de données peut avoir plusieurs périphériques qui ne se connectent pas directement à Cisco Intersight. Tout périphérique pris en charge par Cisco Intersight mais qui ne se connecte pas directement à celui-ci nécessite un mécanisme de connexion. Cisco Intersight fournit ce mécanisme de connexion et vous aide à ajouter des périphériques à Cisco Intersight.

Cisco Intersight Assist est disponible au sein de Cisco Intersight Virtual Appliance, qui est distribué sous la forme d'une machine virtuelle déployable contenue dans un format de fichier OVA (Open Virtual Appliance). Vous pouvez installer l'appliance sur un serveur ESXi. Pour plus d'informations, reportez-vous à la section ["Guide de mise en route de Cisco Intersight Virtual Appliance"](#).

Après avoir réclamé Intersight Assist dans Intersight, vous pouvez demander des périphériques de terminaison à l'aide de l'option réclamation via Intersight Assist. Pour plus d'informations, voir ["Mise en route"](#).

NetApp Cloud Volumes ONTAP

- Exploitation de la déduplication intégrée et de la compression des données, du provisionnement fin et du clonage pour réduire les coûts de stockage.
- Nous garantissons une fiabilité exceptionnelle et la continuité de l'activité en cas de défaillances dans votre environnement cloud.
- Cloud Volumes ONTAP utilise la technologie de réplication leader de NetApp SnapMirror pour répliquer les données sur site vers le cloud. Les copies secondaires sont ainsi disponibles dans différents cas d'utilisation.
- Cloud Volumes ONTAP s'intègre également avec Cloud Backup Service pour fournir des fonctionnalités de sauvegarde et de restauration pour une protection et un archivage à long terme de vos données cloud.
- Basculer à la demande entre des pools de stockage hautes performances et faibles performances, sans mettre les applications hors ligne.

- Cohérence des copies Snapshot avec NetApp SnapCenter.
- Cloud Volumes ONTAP prend en charge le cryptage des données et protège contre les virus et les attaques par ransomware.
- L'intégration avec Cloud Data SENSE vous aide à comprendre le contexte des données et à identifier les données sensibles.

Cloud Central

Cloud Central est une plateforme centralisée qui permet d'accéder aux services de données cloud NetApp et de les gérer. Ces services vous permettent d'exécuter des applications stratégiques dans le cloud, de créer des sites de reprise après incident automatisés, de sauvegarder vos données SaaS et de migrer et contrôler efficacement les données sur plusieurs clouds. Pour plus d'informations, voir "[Cloud Central](#)".

Le gestionnaire Cloud

Cloud Manager est une plateforme de gestion SaaS de grande qualité qui permet aux experts IT et aux architectes cloud de gérer de manière centralisée leur infrastructure multicloud hybride à l'aide des solutions cloud NetApp. Elle offre un système centralisé pour afficher et gérer vos ressources de stockage sur site et cloud afin de prendre en charge plusieurs fournisseurs et comptes de cloud hybride. Pour plus d'informations, voir "[Le gestionnaire Cloud](#)".

Connecteur

Connector permet à Cloud Manager de gérer les ressources et les processus dans un environnement de cloud public. Une instance de connecteur est requise pour utiliser de nombreuses fonctionnalités fournies par Cloud Manager et peut être déployée dans le réseau dans le cloud ou sur site. Le connecteur est pris en charge aux emplacements suivants :

- AWS
- Microsoft Azure
- Google Cloud
- Sur site

NetApp Active IQ Unified Manager

Avec NetApp Active IQ Unified Manager, vous pouvez contrôler vos clusters de stockage ONTAP à partir d'une interface intuitive unique, reconçue pour l'intelligence artificielle et les connaissances de la communauté. Il offre des informations complètes sur les opérations, les performances et le mode proactif de l'environnement de stockage et des machines virtuelles qui s'exécutent sur celui-ci. Lorsqu'un problème se produit avec l'infrastructure de stockage, Unified Manager vous informe des détails du problème pour vous aider à identifier la cause première. Le tableau de bord des machines virtuelles vous offre un aperçu des statistiques de performances de la machine virtuelle. Vous pouvez ainsi examiner l'ensemble du chemin d'E/S depuis l'hôte vSphere vers le réseau, et enfin vers le stockage.

Certains événements fournissent également des mesures correctives que vous pouvez prendre pour corriger le problème. Vous pouvez configurer des alertes personnalisées en cas d'événements afin que, lorsque des problèmes se produisent, vous soyez averti par e-mail et des interruptions SNMP. Active IQ Unified Manager vous permet de planifier les besoins en stockage de vos utilisateurs en anticipant les besoins en stockage et en vous permettant d'anticiper les problèmes, ce qui évite de prendre des décisions réactives à court terme et même d'engendrer des problèmes supplémentaires à long terme.

VMware vSphere

VMware vSphere est une plateforme de virtualisation qui permet de gérer de manière holistique de vastes ensembles d'infrastructures (ressources notamment les processeurs, le stockage et le réseau), sous la forme d'un environnement d'exploitation transparent, polyvalent et dynamique. Contrairement aux systèmes d'exploitation traditionnels qui gèrent une machine individuelle, VMware vSphere agrège l'infrastructure d'un data Center dans son ensemble pour créer une seule puissance avec des ressources qui peuvent être allouées rapidement et dynamiquement à n'importe quelle application, selon les besoins.

Pour plus d'informations sur VMware vSphere, veuillez suivre ["ce lien"](#).

VMware vSphere vCenter

VMware vCenter Server assure une gestion unifiée de tous les hôtes et machines virtuelles depuis une console unique et rassemble le contrôle des performances des clusters, des hôtes et des machines virtuelles. VMware vCenter Server offre aux administrateurs des informations détaillées sur l'état et la configuration des clusters de calcul, des hôtes, des VM, du stockage, du système d'exploitation invité, et autres composants essentiels d'une infrastructure virtuelle. VMware vCenter gère la richesse des fonctionnalités disponibles dans un environnement VMware vSphere.

Versions matérielles et logicielles

Cette solution de cloud hybride peut être étendue à tout environnement FlexPod qui exécute des versions logicielles, matérielles et de firmware prises en charge telles que définies dans la matrice d'interopérabilité NetApp et dans la liste de compatibilité matérielle Cisco UCS.

La solution FlexPod utilisée comme plateforme de base dans notre environnement sur site a été déployée selon les instructions et les spécifications décrites ["ici"](#).

Le réseau au sein de cet environnement est basé sur l'ACI. Pour plus d'informations, voir ["ici"](#).

- Consultez les liens suivants pour plus d'informations :
- ["Matrice d'interopérabilité NetApp"](#)
- ["Guide de compatibilité VMware"](#)
- ["Outil d'interopérabilité matérielle et logicielle Cisco UCS"](#)

Le tableau suivant présente les révisions matérielles et logicielles de FlexPod.

Composant	Solution NetApp	Version
Calcul	CISCO UCS X210C-M6	5.0(1b)
	Cisco UCS Fabric Interconnect 6454	4.2(2a)
Le réseau	Cisco Nexus 9332C (Rachis)	14.2(7)
	Cisco Nexus 9336C-FX2 (feuille)	14.2(7)
	ACI Cisco	4.2(7)
Stockage	Avec AFF A220	9.11.1
	Outils NetApp ONTAP pour VMware vSphere	9.10

Composant	Solution NetApp	Version
	Plug-in NetApp NFS pour VMware VAAI	2.0-15
	Active IQ Unified Manager	9.11
Logiciel	VSphere ESXi	7.0(U3)
	Appliance VMware vCenter	7.0.3
	Appliance virtuelle Cisco InterSight Assist	1.0.11-306

L'exécution des configurations Terraform s'effectue sur le compte Terraform Cloud for Business. La configuration Terraform utilise le fournisseur Terraform pour NetApp Cloud Manager.

Le tableau suivant répertorie les fournisseurs, les produits et les versions.

Composant	Solution NetApp	Version
HashiCorp	Terraform	1.2.7

Le tableau suivant présente les versions de Cloud Manager et de Cloud Volumes ONTAP.

Composant	Solution NetApp	Version
NetApp	Cloud Volumes ONTAP	9.11
	Le gestionnaire Cloud	3.9.21

["Suivant : installation et configuration - déployer FlexPod."](#)

Installation et configuration

Déployez FlexPod

["Précédent : composants de la solution."](#)

Pour comprendre les détails de la conception et du déploiement de FlexPod, notamment la configuration de différents éléments de la conception et des meilleures pratiques associées, consultez la section ["Conceptions validées par Cisco pour FlexPod"](#).

FlexPod peut être déployé à la fois en mode géré UCS et en mode géré Cisco InterSight. Si vous déployez FlexPod en mode géré UCS, vous trouverez la dernière conception validée Cisco ["ici"](#).

Cisco Unified Computing System (Cisco UCS) X-Series est un tout nouveau système de calcul modulaire, configuré et géré à partir du cloud. Elle est conçue pour répondre aux besoins des applications modernes et pour améliorer l'efficacité opérationnelle, l'agilité et l'évolutivité au travers d'un design modulaire, adaptable et prêt pour le futur. Vous trouverez des conseils de conception concernant l'intégration de la plateforme UCS X-Series gérée par Cisco Intersight dans l'infrastructure FlexPod ["ici"](#).

FlexPod avec Cisco ACI est disponible ["ici"](#).

["Suivant : configuration Cisco Intersight."](#)

Configuration Cisco Intersight

["Précédent : déployer FlexPod."](#)

Pour configurer Cisco Intersight et Intersight, consultez les conceptions validées par Cisco pour FlexPod trouvées ["ici"](#).

["Suivant : intégration du cloud Terraform avec la condition préalable d'ICO."](#)

Terraform intégration au cloud avec une condition préalable de l'ICO

["Précédent : configuration Cisco Intersight."](#)

Procédure 1 : connecter Cisco Intersight et Terraform Cloud

1. Faites une demande de remboursement ou créez une cible cloud Terraform en fournissant les informations pertinentes sur le compte Terraform Cloud.
2. Créez une cible Terraform Cloud Agent pour les clouds privés afin que les clients puissent installer l'agent dans le data Center et activer la communication avec Terraform Cloud.

Pour plus d'informations, veuillez consulter la section ["ce lien"](#).

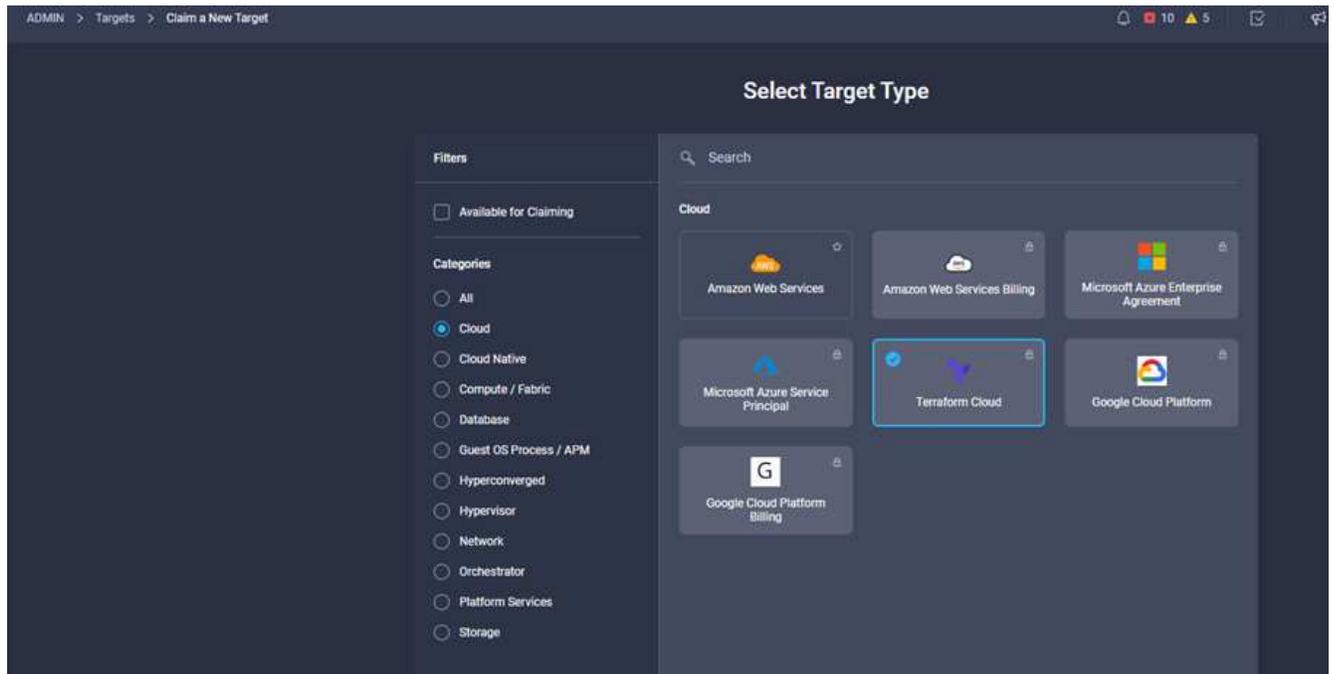
Procédure 2 : générer un jeton utilisateur

Dans le cadre de l'ajout d'une cible pour Terraform Cloud, vous devez fournir le nom d'utilisateur et le jeton d'API à partir de la page des paramètres Terraform Cloud.

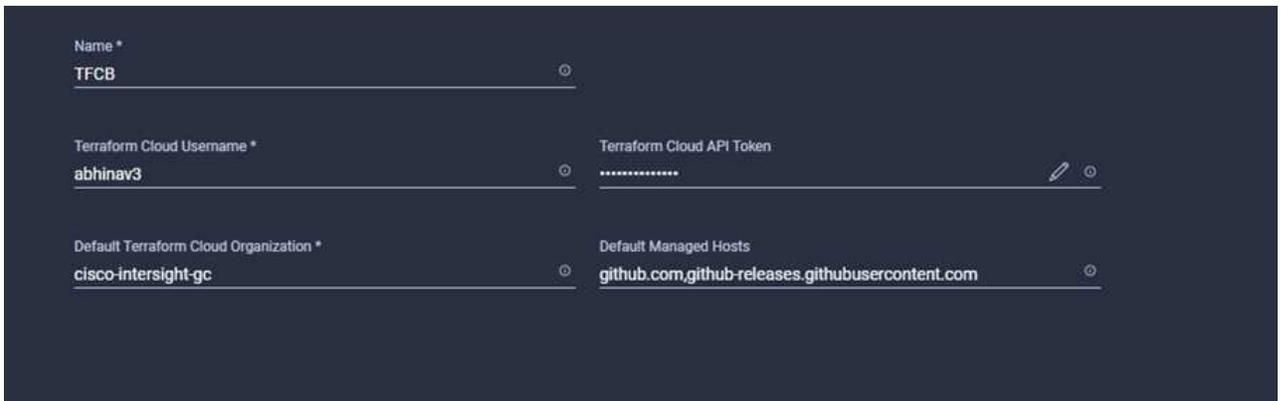
1. Connectez-vous à Terraform Cloud et accédez à **User Tokens** : ["https://app.terraform.io/app/settings/tokens"](https://app.terraform.io/app/settings/tokens).
2. Cliquez sur **Créer un nouveau jeton API**.
3. Attribuez un nom à mémoriser et enregistrez le token dans un endroit sécurisé.

Procédure 3 : cible de cloud de demande Terraform

1. Connectez-vous à Intersight avec les privilèges Administrateur de compte, Administrateur de périphérique ou technicien de périphérique.
2. Accédez à **ADMIN > Targets > Claim a New Target**.
3. Dans **Categories**, cliquez sur **Cloud**.
4. Cliquez sur **Terraform Cloud** et cliquez sur **Start**.



5. Entrez un nom pour la cible, votre nom d'utilisateur pour le Terraform Cloud, le jeton API et une organisation par défaut dans Terraform Cloud comme indiqué dans l'image suivante.
6. Dans le champ **Default Managed Hosts**, assurez-vous d'ajouter les liens suivants avec d'autres hôtes gérés :
 - github.com
 - github-releases.githubusercontent.com



Si tout est correctement saisi, votre cible Terraform Cloud s'affiche dans la section **cibles Intersight**.

Procédure 4 : ajouter des agents Terraform Cloud

Prérequis :

- Cible Terraform Cloud.
- Demande d'assistance Intersight dans Intersight avant de déployer l'agent Cloud Terraform.



Vous ne pouvez demander que cinq agents pour chaque assistance.



Après avoir créé la connexion à Terraform, vous devez faire tourner un agent Terraform pour exécuter le code Terraform.

1. Cliquez sur **Claim Terraform Cloud Agent** dans la liste déroulante de votre cible Terraform Cloud.
2. Entrez les détails de l'agent Terraform Cloud. La capture d'écran suivante montre les détails de configuration de l'agent Terraform.

Terraform Cloud target

Name *
flexpod-solution-terraform-agent

Intersight Assist *
g13-intersight-appliance.fpmc.sa

Terraform Cloud Organization *
cisco-intersight-gc

Terraform Cloud Agent Pool Name *
flexpod-solution-agent-pool

Managed Hosts

Hostname / IP Address / Subnets *
github.com
github-releases.githubusercontent.com



Vous pouvez mettre à jour n'importe quelle propriété Terraform Agent. Si la cible est à l'état **non connecté** et n'a jamais été à l'état **connecté**, alors aucun jeton n'a été généré pour l'agent Terraform.

Une fois la validation de l'agent réussie et qu'un jeton d'agent est généré, vous ne pouvez pas reconfigurer l'organisation et/ou le pool d'agents. Le déploiement réussi d'un agent Terraform est indiqué par l'état **Connected**.

Après avoir activé et demandé l'intégration Terraform Cloud, vous pouvez déployer un ou plusieurs agents Terraform Cloud dans Cisco InterSight Assist. L'agent Terraform Cloud est modélisé comme cible enfant de la cible Terraform Cloud. Lorsque vous demandez la cible de l'agent, un message s'affiche pour indiquer que la demande cible est en cours.

Au bout de quelques secondes, la cible est déplacée à l'état **Connected** et la plateforme Intersight achemine les paquets HTTPS de l'agent vers la passerelle Terraform Cloud.

Votre agent Terraform doit être correctement réclamé et s'afficher sous cibles comme **connecté**.

["Configuration du fournisseur de services clouds publics"](#)

Configurez le fournisseur de services clouds publics

["Précédent : intégration du cloud Terraform avec la condition préalable d'ICO."](#)

Procédure 1 : accéder à NetApp Cloud Manager

Pour accéder à NetApp Cloud Manager et aux autres services cloud, vous devez vous inscrire ["NetApp Cloud Central"](#).



Pour configurer des espaces de travail et des utilisateurs sur le compte Cloud Central, cliquez sur ["ici"](#).

Procédure 2 : déployer le connecteur

Pour déployer Connector dans Google Cloud, rendez-vous ici ["lien"](#).

["Ensuite, déploiement automatisé du stockage NetApp dans le cloud hybride."](#)

Déploiement automatisé du stockage de cloud hybride NetApp

["Précédent : configuration du fournisseur de services clouds publics."](#)

Google Cloud

Vous devez d'abord activer des API et créer un compte de service qui fournit à Cloud Manager des autorisations pour déployer et gérer des systèmes Cloud Volumes ONTAP dans le même projet que celui du connecteur ou dans des projets différents.

Avant de déployer un connecteur dans un projet Google Cloud, vérifiez que ce connecteur ne s'exécute pas sur vos sites ou dans un autre fournisseur cloud.

Deux ensembles d'autorisations doivent être en place avant de déployer un connecteur directement depuis Cloud Manager :

- Vous devez déployer Connector à l'aide d'un compte Google qui dispose d'autorisations pour lancer l'instance de VM Connector à partir de Cloud Manager.
- Lors du déploiement de Connector, vous êtes invité à sélectionner l'instance de VM. Cloud Manager obtient les autorisations du compte de service pour créer et gérer les systèmes Cloud Volumes ONTAP en votre nom. Les autorisations sont fournies en ajoutant un rôle personnalisé au compte de service. vous devez configurer deux fichiers YAML qui incluent les autorisations requises pour l'utilisateur et le compte de service. Découvrez comment utiliser ["Les fichiers YAML pour configurer les autorisations"](#) ici.

Voir ["cette vidéo détaillée"](#) pour tous les prérequis requis.

Architecture et modes de déploiement Cloud Volumes ONTAP

Cloud Volumes ONTAP est disponible dans Google Cloud sous forme de système à un seul nœud et en tant que paire de nœuds à haute disponibilité. En fonction de ces exigences, nous pouvons choisir le mode de déploiement Cloud Volumes ONTAP. La mise à niveau d'un système à un seul nœud vers une paire haute disponibilité n'est pas prise en charge. Si vous souhaitez passer d'un système à un seul nœud à une paire HA, vous devez déployer un nouveau système et répliquer les données du système existant vers le nouveau.

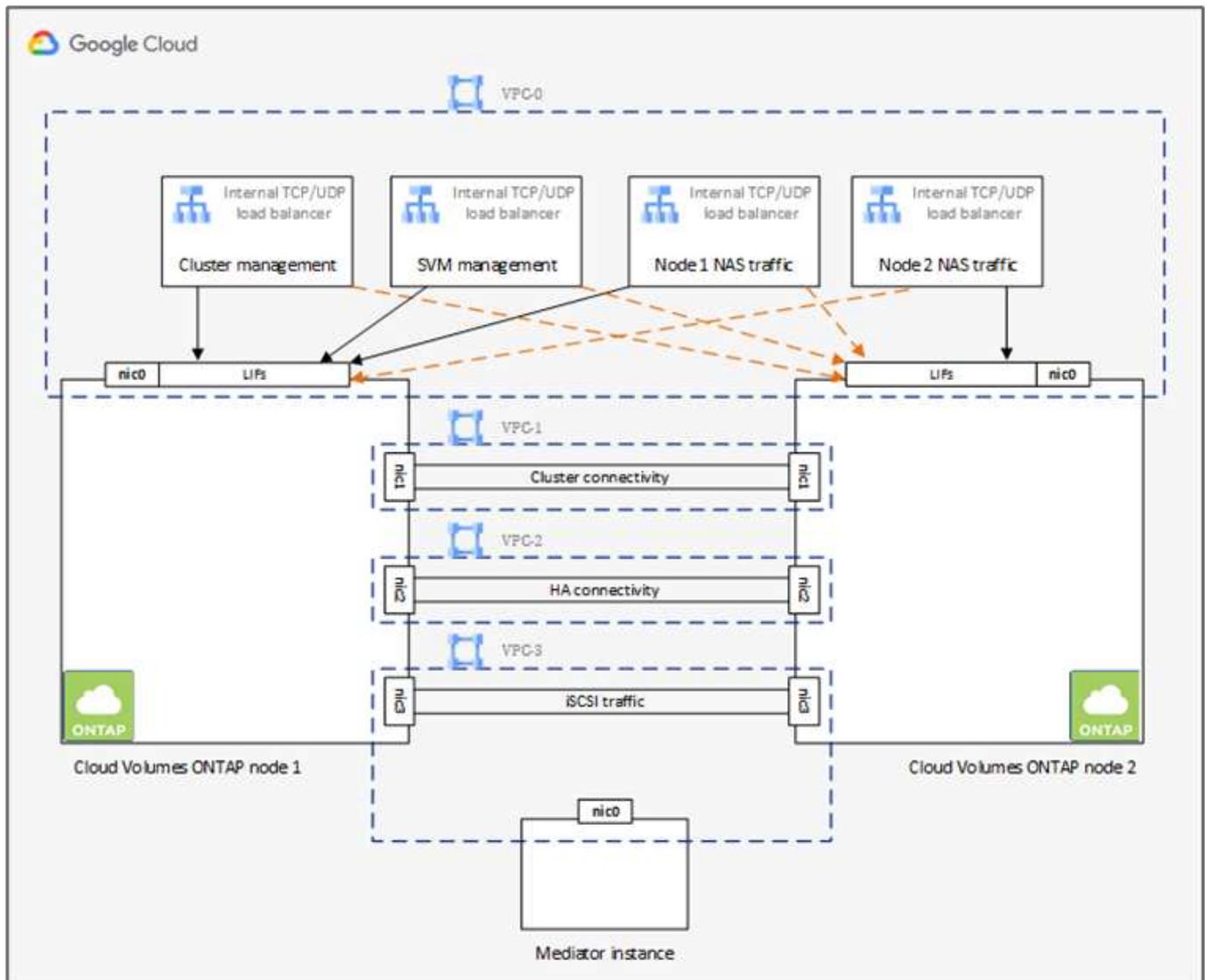
Haute disponibilité de Cloud Volumes ONTAP dans Google Cloud

Google Cloud prend en charge le déploiement de ressources dans plusieurs régions géographiques et zones géographiques. Le déploiement HA comprend deux nœuds ONTAP qui utilisent de puissants types de machines standard n1 ou n2 disponibles dans Google Cloud. Les données sont répliquées de manière synchrone entre les deux nœuds Cloud Volumes ONTAP afin d'assurer la disponibilité en cas de défaillance. Le déploiement HAUTE DISPONIBILITÉ de Cloud Volumes ONTAP requiert quatre VPC et un sous-réseau privé dans chaque VPC. Les sous-réseaux des quatre VPC doivent être configurés avec des plages CIDR non chevauchantes.

Les quatre VPC sont utilisés à des fins suivantes :

- VPC 0 permet la communication entrante aux nœuds de données et Cloud Volumes ONTAP.
- VPC 1 assure la connectivité du cluster entre les nœuds Cloud Volumes ONTAP.
- VPC 2 permet la répllication des RAM non volatiles (NVRAM) entre les nœuds.
- VPC 3 est utilisé pour la connectivité à l'instance de médiateur HA et au trafic de réplication de disque pour les reconstructions de nœuds.

L'image suivante montre un Cloud Volumes ONTAP hautement disponible dans Goggle Cloud.



Pour plus de détails, voir ["ce lien"](#).

Pour connaître les exigences de mise en réseau pour Cloud Volumes ONTAP dans Google Cloud, consultez ["ce lien"](#).

Pour plus d'informations sur le Tiering des données, voir ["ce lien"](#).

Configurez les conditions préalables à l'environnement

La création automatisée de clusters Cloud Volumes ONTAP, la configuration SnapMirror entre un volume sur site et un volume cloud, la création d'un volume cloud, etc., s'effectue à l'aide de la configuration Terraform. Ces configurations Terraform sont hébergées sur un compte Terraform Cloud for Business. Avec Intersight Cloud Orchestrator, vous orchestrez des tâches telles que la création d'un espace de travail dans un compte Terraform Cloud for Business, l'ajout de toutes les variables requises à l'espace de travail, l'exécution d'un plan Terraform, etc.

Pour ces tâches d'automatisation et d'orchestration, quelques exigences et données sont nécessaires, comme décrit dans les sections suivantes.

Référentiel GitHub

Vous avez besoin d'un compte GitHub pour héberger votre code Terraform. Intersight Orchestrator crée un nouvel espace de travail dans le compte Terraform Cloud for Business. Cet espace de travail est configuré avec un workflow de contrôle de version. À cette fin, vous devez conserver la configuration Terraform dans un référentiel GitHub et la fournir comme entrée lors de la création de l'espace de travail.

["Lien GitHub"](#) Fournit la configuration Terraform avec diverses ressources. Vous pouvez forer ce référentiel et en faire une copie dans votre compte GitHub.

Dans ce référentiel, `provider.tf` A la définition du fournisseur Terraform requis. Le fournisseur Terraform pour NetApp Cloud Manager est utilisé.

`variables.tf` dispose de toutes les déclarations de variables. La valeur de ces variables est entrée en tant qu'entrée de workflow d'Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à un espace de travail et d'exécuter la configuration Terraform.

`resources.tf` Définit les diverses ressources nécessaires pour ajouter un système ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à nœud unique sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Dans ce référentiel :

- `provider.tf` Définit NetApp Cloud Manager comme fournisseur Terraform requis.
- `variables.tf` Dispose des déclarations de variables utilisées comme entrée pour le workflow Intersight Cloud Orchestrator. Cela permet de transmettre des valeurs à l'espace de travail et d'exécuter la configuration Terraform.
- `resources.tf` Définit diverses ressources pour ajouter une ONTAP sur site à l'environnement de travail, créer un cluster Cloud Volumes ONTAP à un seul nœud sur Google Cloud, établir une relation SnapMirror entre l'infrastructure sur site et Cloud Volumes ONTAP, créer un volume cloud sur Cloud Volumes ONTAP, etc.

Vous pouvez ajouter un bloc de ressources supplémentaire pour créer plusieurs volumes sur Cloud Volumes ONTAP, ou utiliser `count` ou `for_each` Constructions Terraform.

Pour connecter des espaces de travail Terraform, des modules et des jeux de règles aux référentiels git contenant des configurations Terraform, Terraform Cloud doit accéder à votre GitHub repo.

Ajoutez un client et l'ID Token OAuth du client est utilisé comme l'une des entrées de workflow d'InterSight Cloud Orchestrator.

1. Connectez-vous à votre compte Terraform Cloud for Business. Accédez à **Paramètres > fournisseurs**.
2. Cliquez sur **Ajouter un fournisseur VCS**.
3. Sélectionnez votre version.
4. Suivez les étapes de la section **configurer fournisseur**.
5. Vous voyez le client ajouté dans **VCS Providers**. Notez l'ID du token OAuth.

Jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager

En plus de l'interface du navigateur Web, Cloud Manager dispose d'une API REST qui permet aux développeurs de logiciels d'accéder directement à la fonctionnalité Cloud Manager via l'interface SaaS. Le service Cloud Manager comprend plusieurs composants distincts qui forment collectivement une plateforme de développement extensible. Le jeton d'actualisation vous permet de générer des jetons d'accès que vous ajoutez à l'en-tête autorisation pour chaque appel d'API.

Sans appeler directement une API, le fournisseur netapp-cloudManager utilise un jeton d'actualisation et convertit les ressources Terraform en appels d'API correspondants. Vous devez générer un jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager à partir de "[NetApp Cloud Central](#)".

Vous devez disposer de l'ID client du connecteur Cloud Manager pour créer des ressources dans Cloud Manager, par exemple pour créer un cluster Cloud Volumes ONTAP, configurer SnapMirror, etc.

1. Connectez-vous à Cloud Manager : "<https://cloudmanager.netapp.com/>".
2. Cliquez sur **connecteur**.
3. Cliquez sur **gérer les connecteurs**.
4. Cliquez sur les points de suspension et copiez l'ID du connecteur.

Développez le workflow Cisco Intersight Cloud Orchestrator

Cisco Intersight Cloud Orchestrator est disponible dans Cisco Intersight si :

- Vous avez installé la licence InterSight Premier.
- Vous êtes administrateur de compte, administrateur de stockage, administrateur de virtualisation ou administrateur de serveurs et avez au moins un serveur qui vous est attribué.

Concepteur de flux de travail

Le concepteur de flux de travail vous aide à créer de nouveaux flux de travail (ainsi que des tâches et des types de données) et à modifier des flux de travail existants pour gérer des cibles dans Cisco Intersight.

Pour lancer Workflow Designer, accédez à **orchestration > workflows**. Un tableau de bord affiche les détails suivants sous les onglets **Mes workflows**, **modèles de flux de travail** et **tous les workflows** :

- État de validation
- Statut de la dernière exécution

- Flux de travail par nombre d'exécution
- Principales catégories de flux de travail
- Nombre de flux de travail définis par le système
- Principaux flux de travail par cible

Le tableau de bord vous permet de créer, modifier, cloner ou supprimer un onglet. Pour créer votre propre onglet de vue personnalisée, cliquez sur **+**, spécifiez un nom, puis sélectionnez les paramètres requis à afficher dans les colonnes, les colonnes de balises et les widgets. Vous pouvez renommer un onglet s'il ne possède pas d'icône **Lock**.

Sous le tableau de bord, vous trouverez une liste tabulaire des flux de production affichant les informations suivantes :

- Afficher le nom
- Description
- Défini par le système
- Version par défaut
- Exécutions
- Statut de la dernière exécution
- État de validation
- Dernière mise à jour
- Entreprise

La colonne actions vous permet d'effectuer les actions suivantes :

- **Exécuter.** exécute le flux de travail.
- **Historique.** affiche l'historique d'exécution du flux de travail.
- **Gérer les versions.** Créer et gérer des versions pour les flux de travail.
- **Supprimer.** Supprimer un flux de travail.
- **Réessayer.** Réessayer un flux de travail échoué.

Flux de travail

Créer un flux de travail composé des étapes suivantes :

- **Définition d'un flux de travail.** spécifier le nom d'affichage, la description et d'autres attributs importants.
- **Définir les entrées de flux de travail et les sorties de flux de travail.** spécifier les paramètres d'entrée obligatoires pour l'exécution du flux de travail et les sorties générées lors de l'exécution réussie
- **Ajouter des tâches de flux de travail.** Ajouter une ou plusieurs tâches de flux de travail dans le concepteur de flux de travail qui sont nécessaires pour que le flux de travail puisse exécuter sa fonction.
- *Valider le flux de travail. *Valider un flux de travail pour s'assurer qu'il n'y a pas d'erreurs dans la connexion des entrées et sorties de tâche.

Créez des workflows de stockage FlexPod sur site

Pour configurer un workflow pour le stockage FlexPod sur site, reportez-vous à la section "[ce lien](#)".

"Suivant : [workflow de reprise après incident.](#)"

Workflow de reprise d'activité

"Précédent : [déploiement automatisé du stockage NetApp dans le cloud hybride.](#)"

Les étapes sont les suivantes :

1. Définir le flux de travail.
 - Créez un nom court et convivial pour le flux de travail, tel que Disaster Recovery Workflow.
2. Définissez l'entrée du flux de travail. Nous utilisons les données d'entrée suivantes pour ce flux de travail :
 - Options de volume (nom du volume, chemin de montage)
 - Capacité du volume
 - Data Center associé au nouveau datastore
 - Cluster sur lequel le datastore est hébergé
 - Nom du nouveau datastore à créer dans vCenter
 - Type et version du nouveau datastore
 - Nom de l'organisation Terraform
 - Espace de travail Terraform
 - Description de l'espace de travail Terraform
 - Variables (sensibles et non sensibles) requises pour exécuter la configuration Terraform
 - Motif du démarrage du plan
3. Ajoutez les tâches du flux de travail.

Les tâches liées aux opérations dans FlexPod incluent les tâches suivantes :

- Création de volumes dans FlexPod.
- Ajout de l'export policy de stockage au volume créé
- Mappez le nouveau volume sur un datastore dans VMware vCenter.

Tâches liées à la création d'un cluster Cloud Volumes ONTAP :

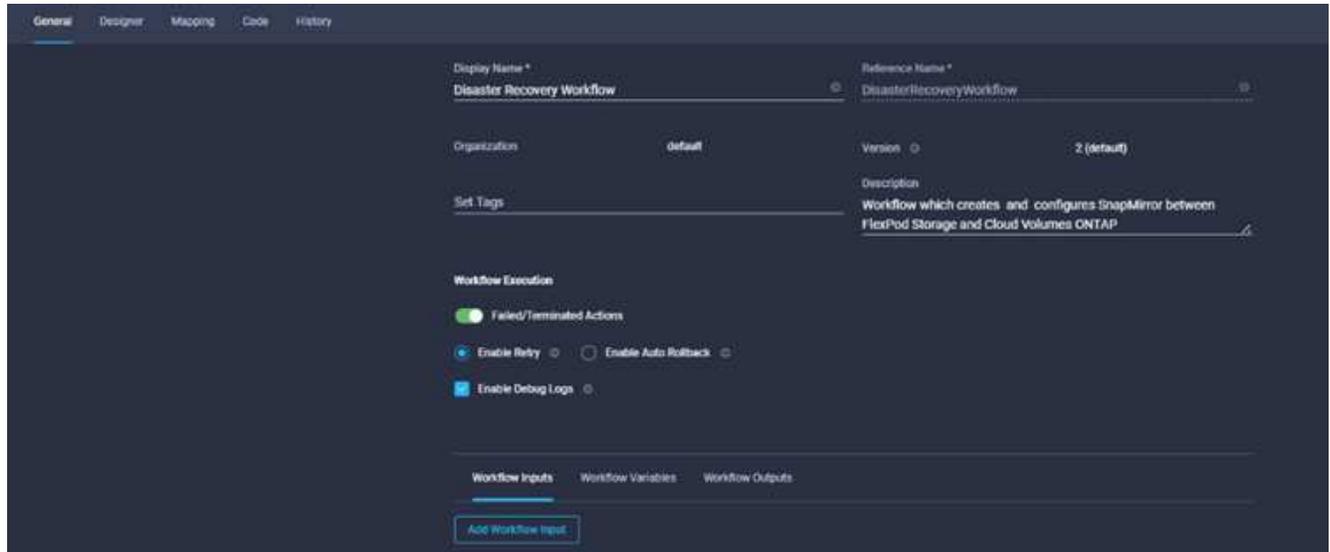
- Ajouter un espace de travail Terraform
- Ajouter des variables Terraform
- Ajoutez des variables sensibles à Terraform
- Démarrez un nouveau plan Terraform
- Confirmez l'exécution de Terraform

4. Validation du flux de travail

Procédure 1 : créez le flux de travail

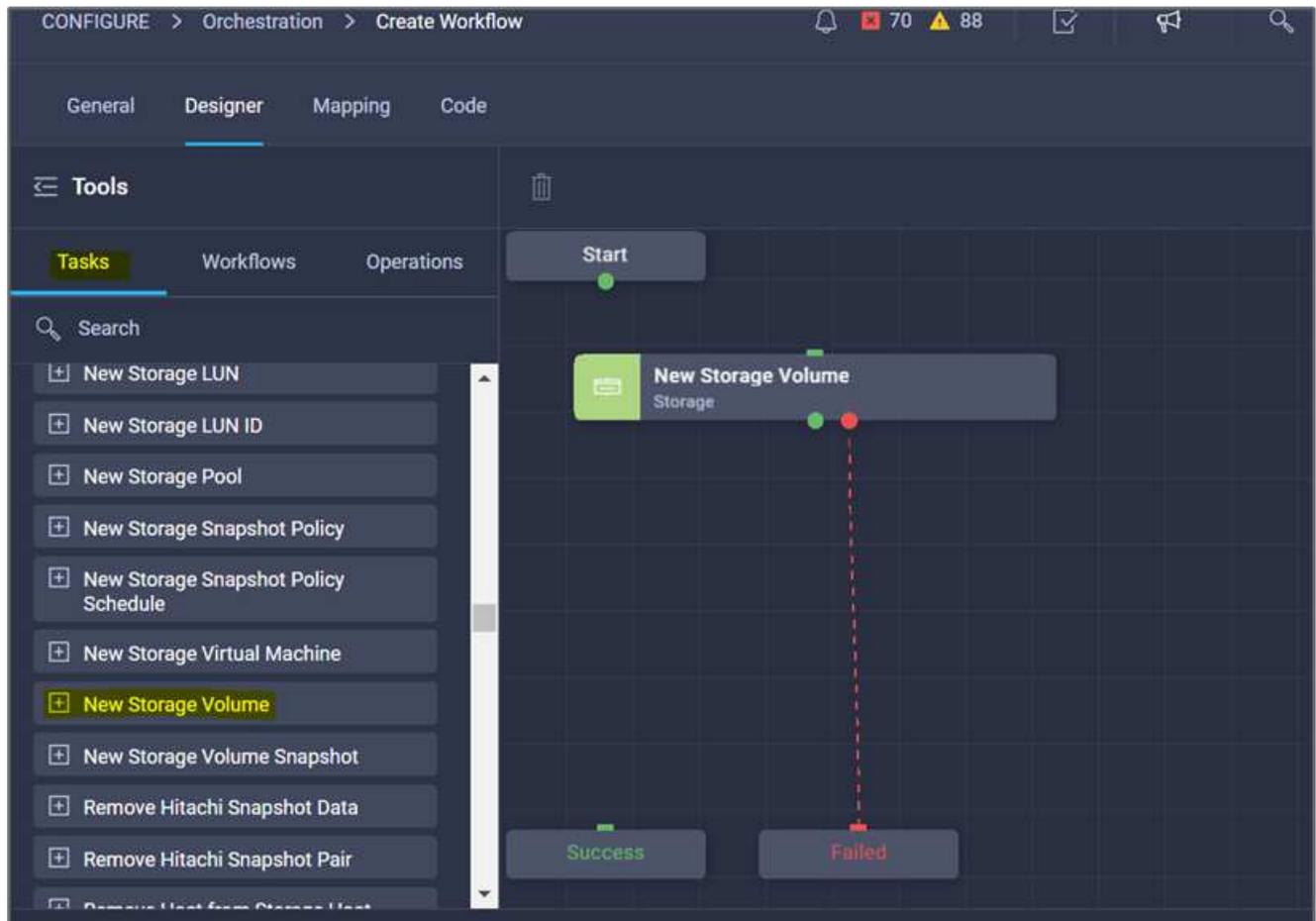
1. Cliquez sur **orchestration** dans le volet de navigation de gauche et cliquez sur **Créer un flux de travail**.
2. Dans l'onglet **général** :
 - a. Indiquez le nom d'affichage (flux de travail de reprise après sinistre).

- b. Sélectionnez l'organisation, définissez les balises et fournissez une description.
3. Cliquez sur Enregistrer.

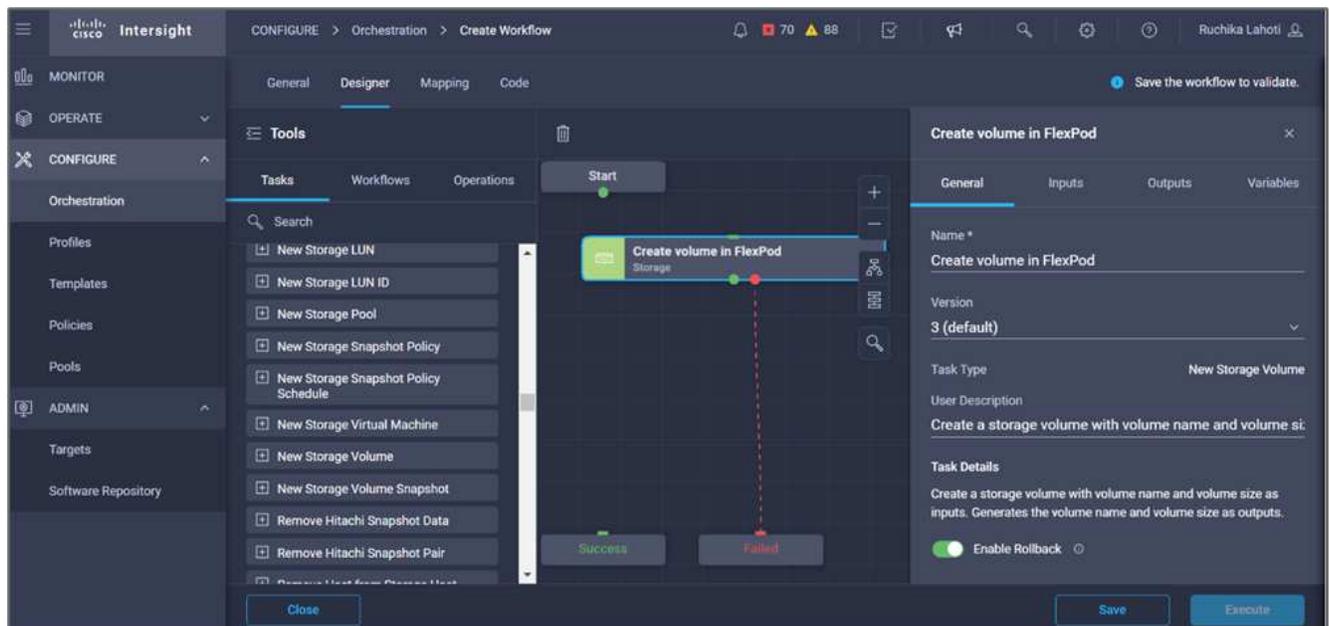


Procédure 2. Créer un nouveau volume dans FlexPod

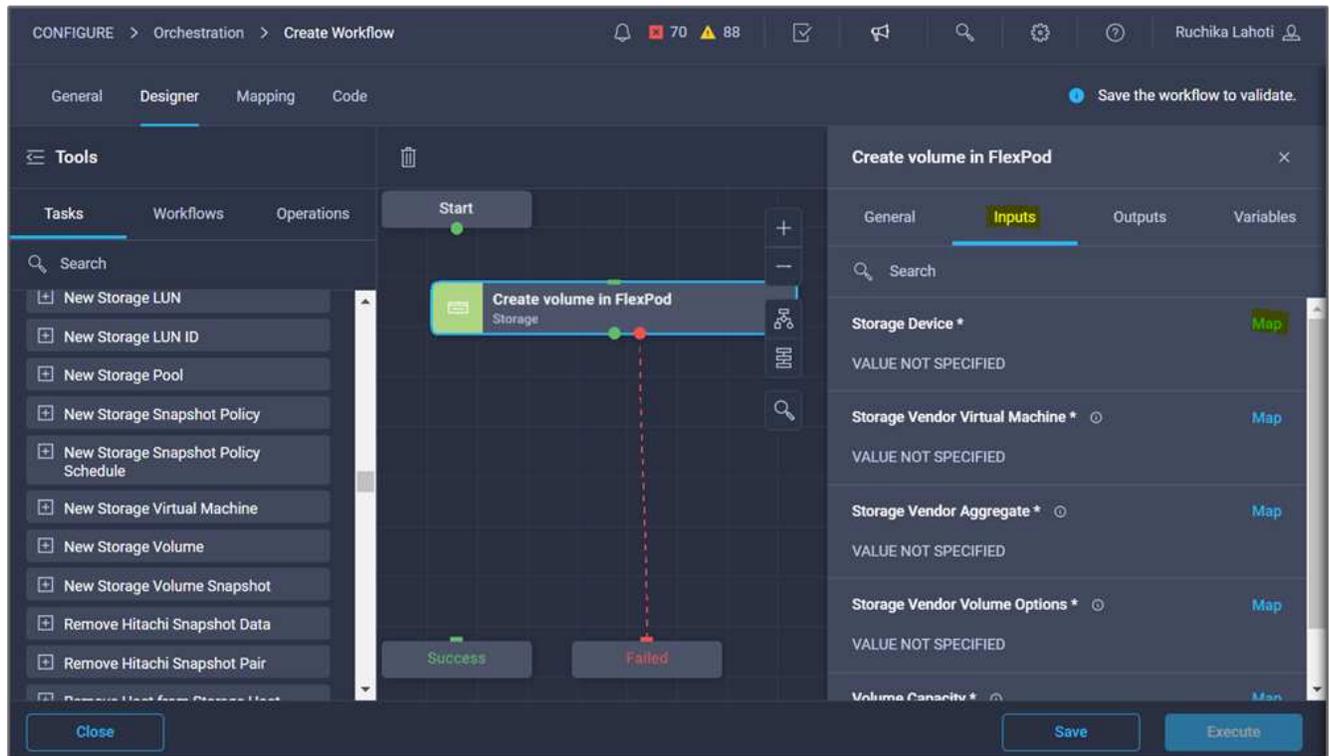
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Nouveau volume de stockage** de la section **Outils** dans la zone **Design**.
3. Cliquez sur **Nouveau volume de stockage**.



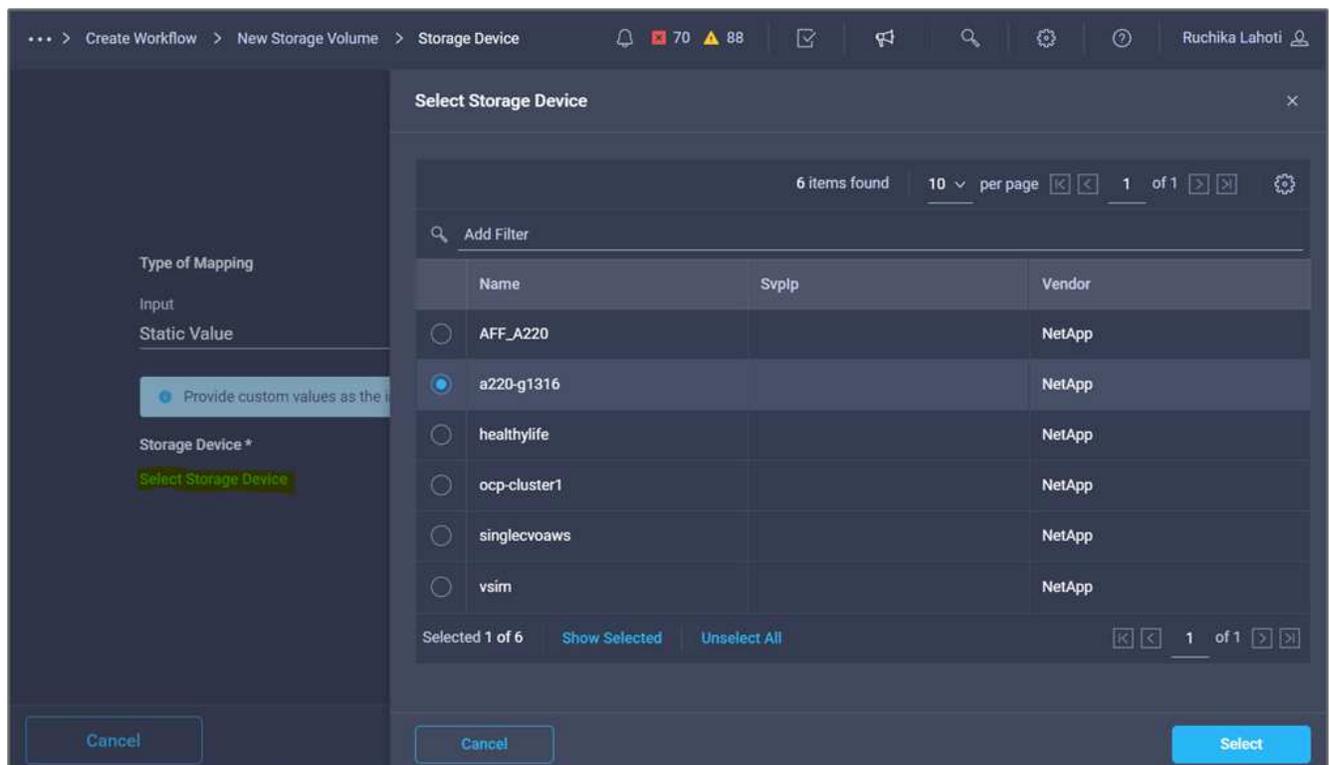
4. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Créer un volume dans FlexPod**.



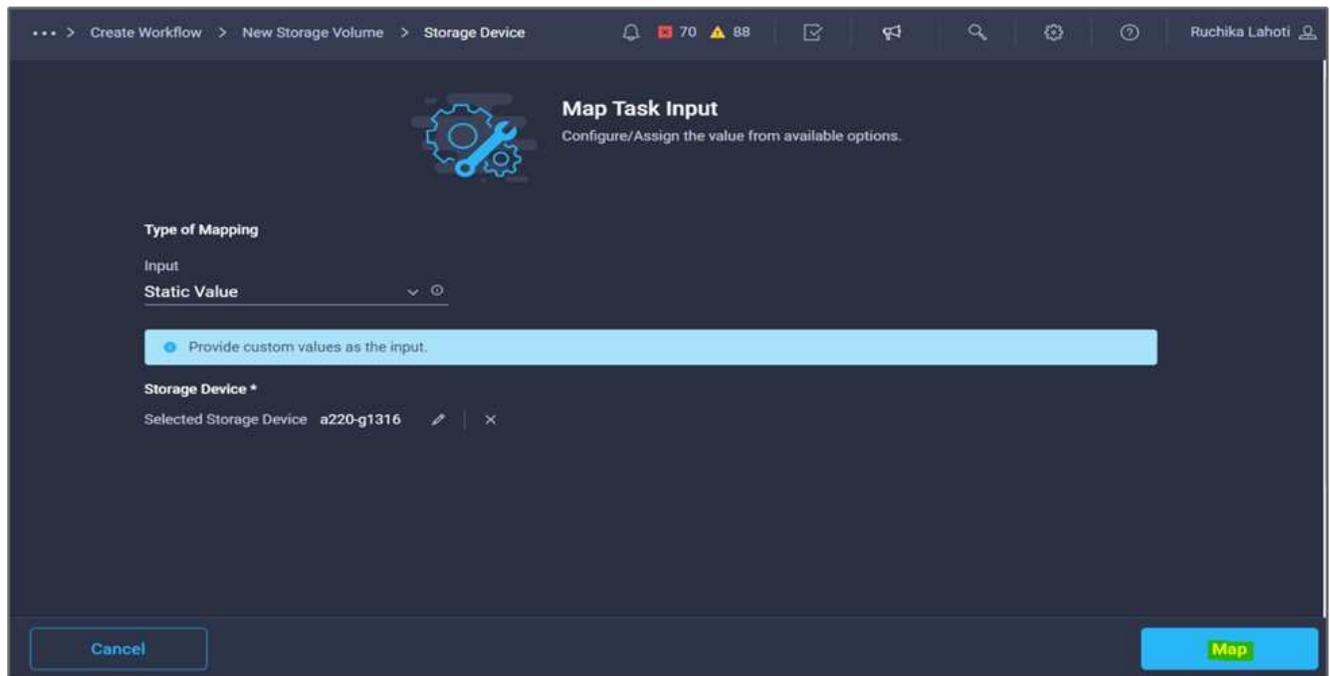
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



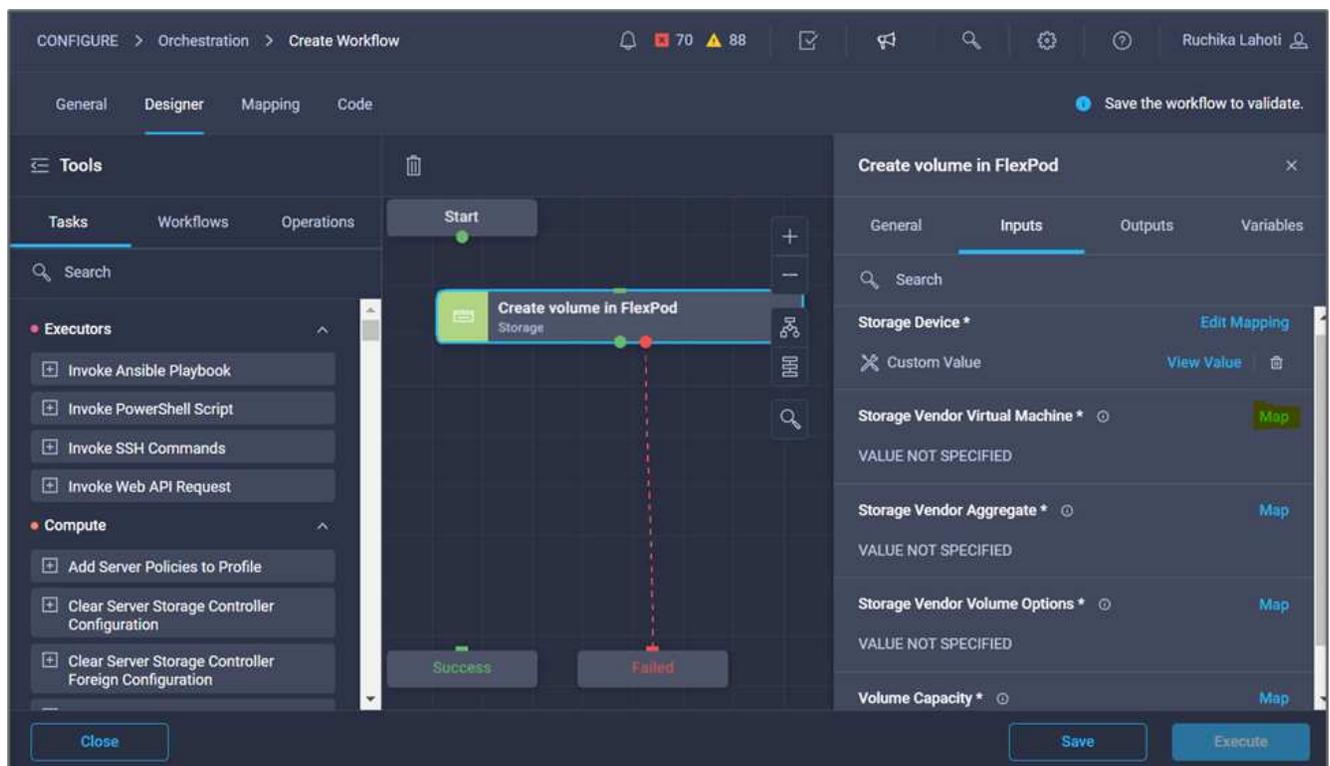
7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**.
8. Cliquez sur la cible de stockage ajoutée et cliquez sur **Sélectionner**.



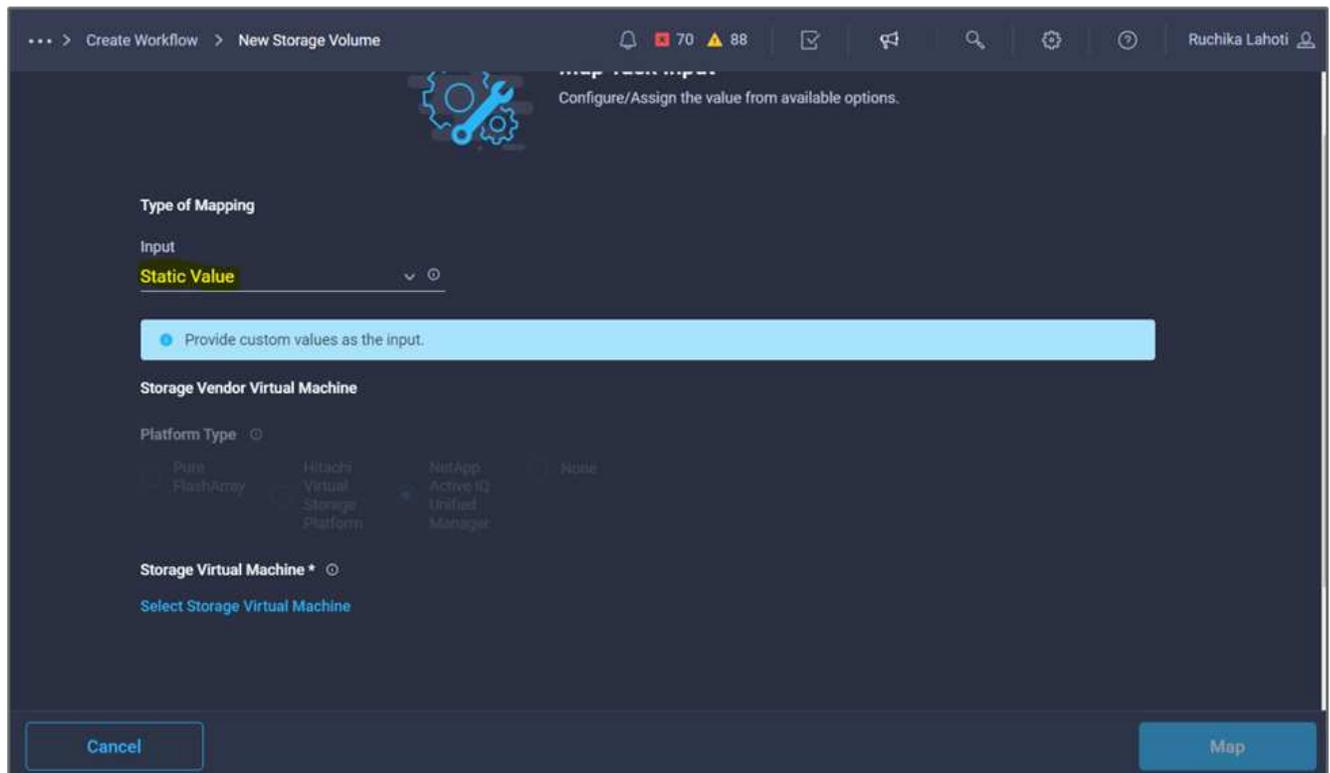
9. Cliquez sur **carte**.



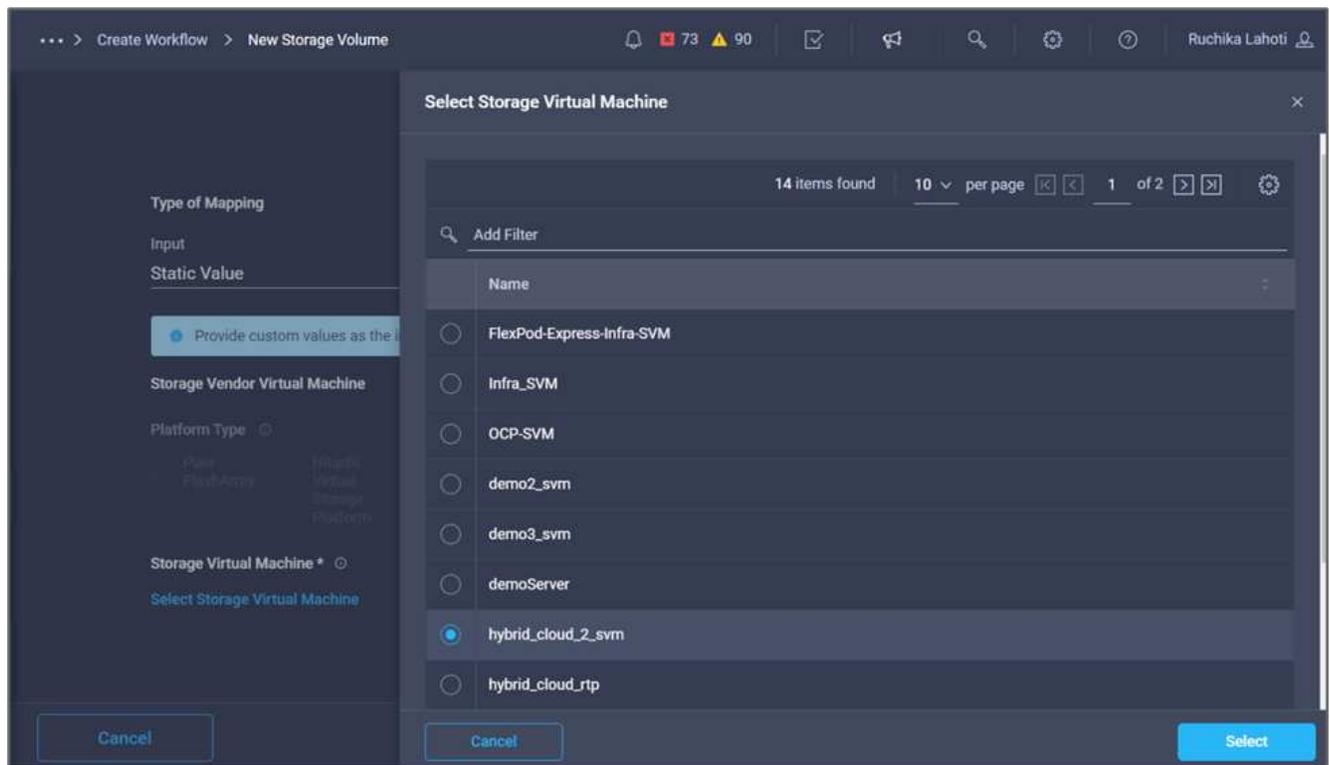
10. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.



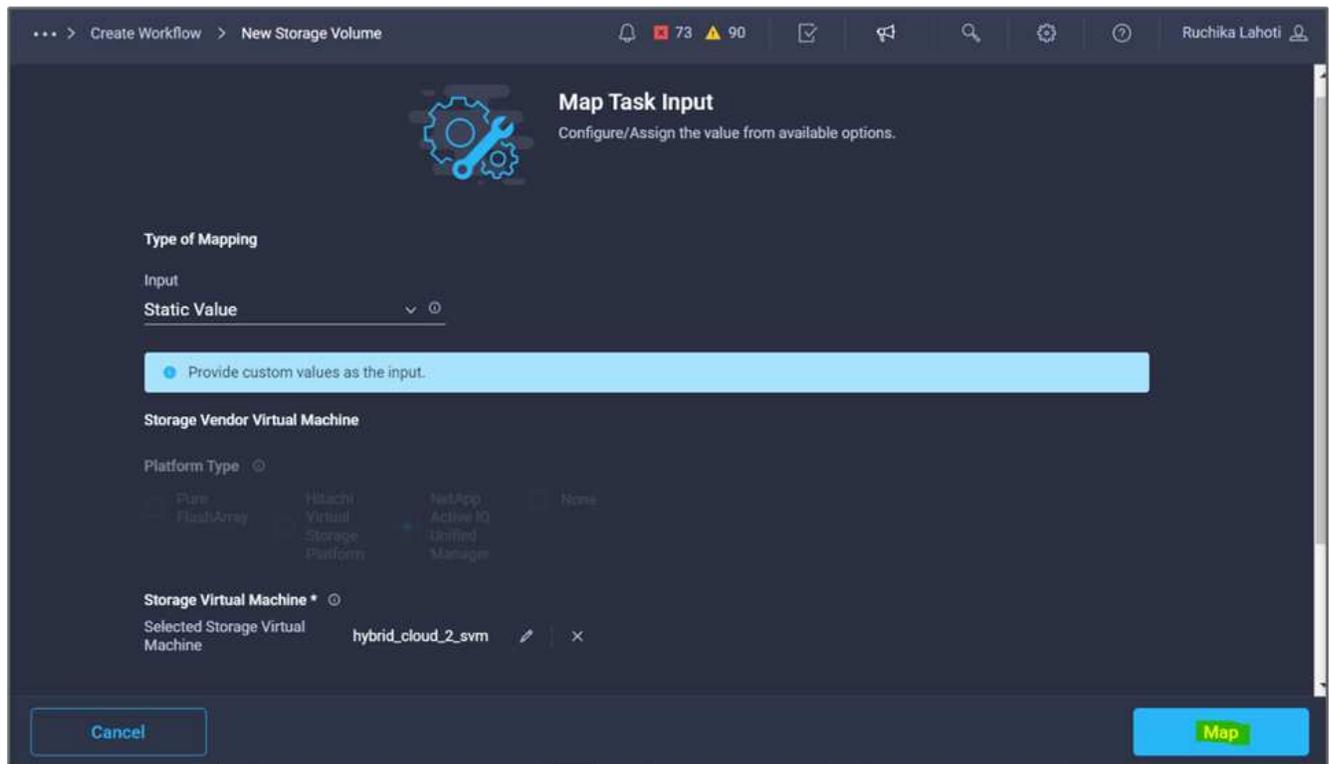
11. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**.



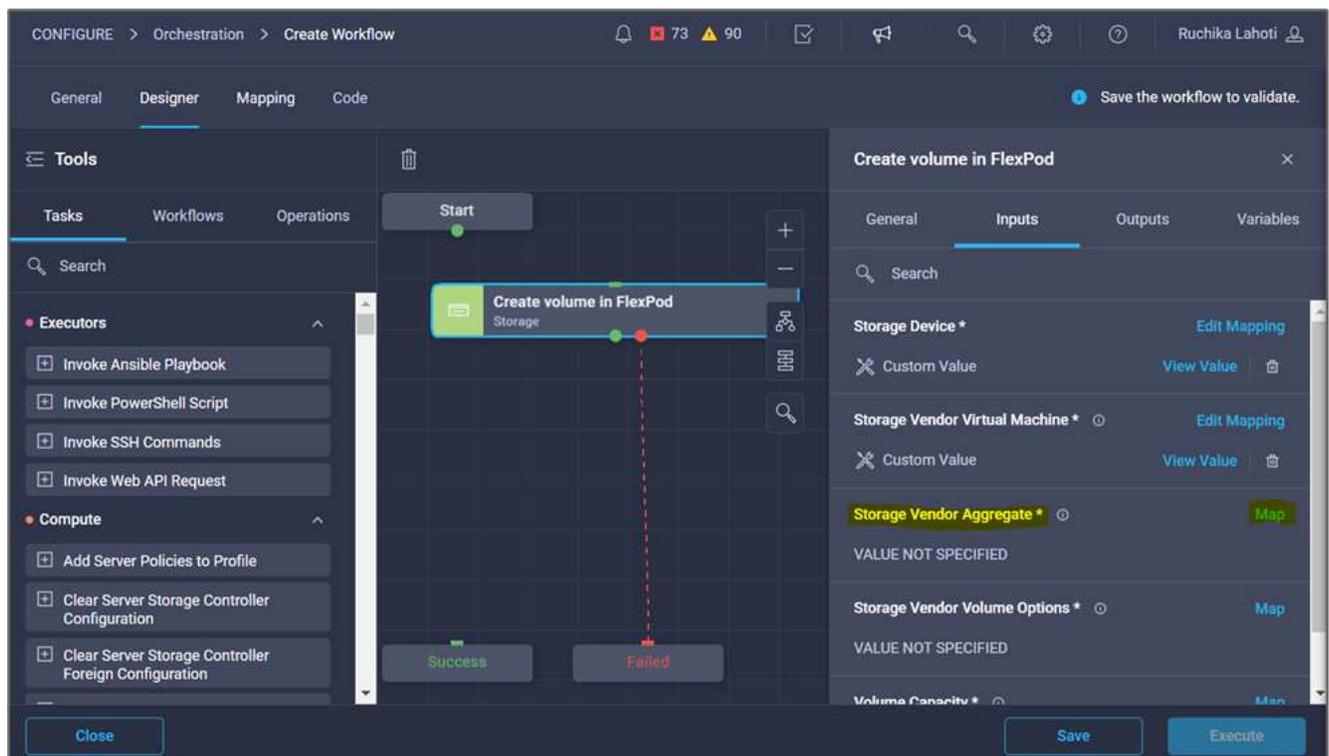
12. Sélectionnez la machine virtuelle de stockage sur laquelle le volume doit être créé et cliquez sur **Sélectionner**.



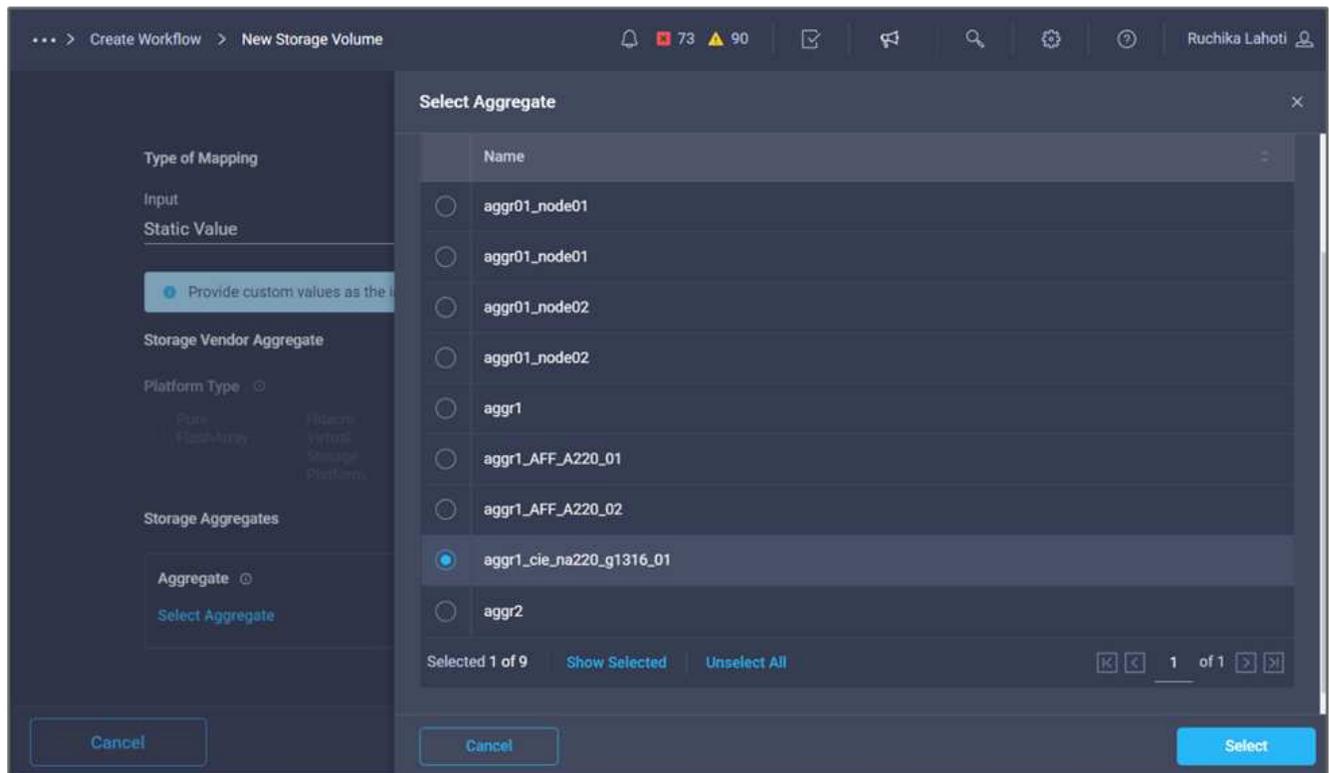
13. Cliquez sur **carte**.



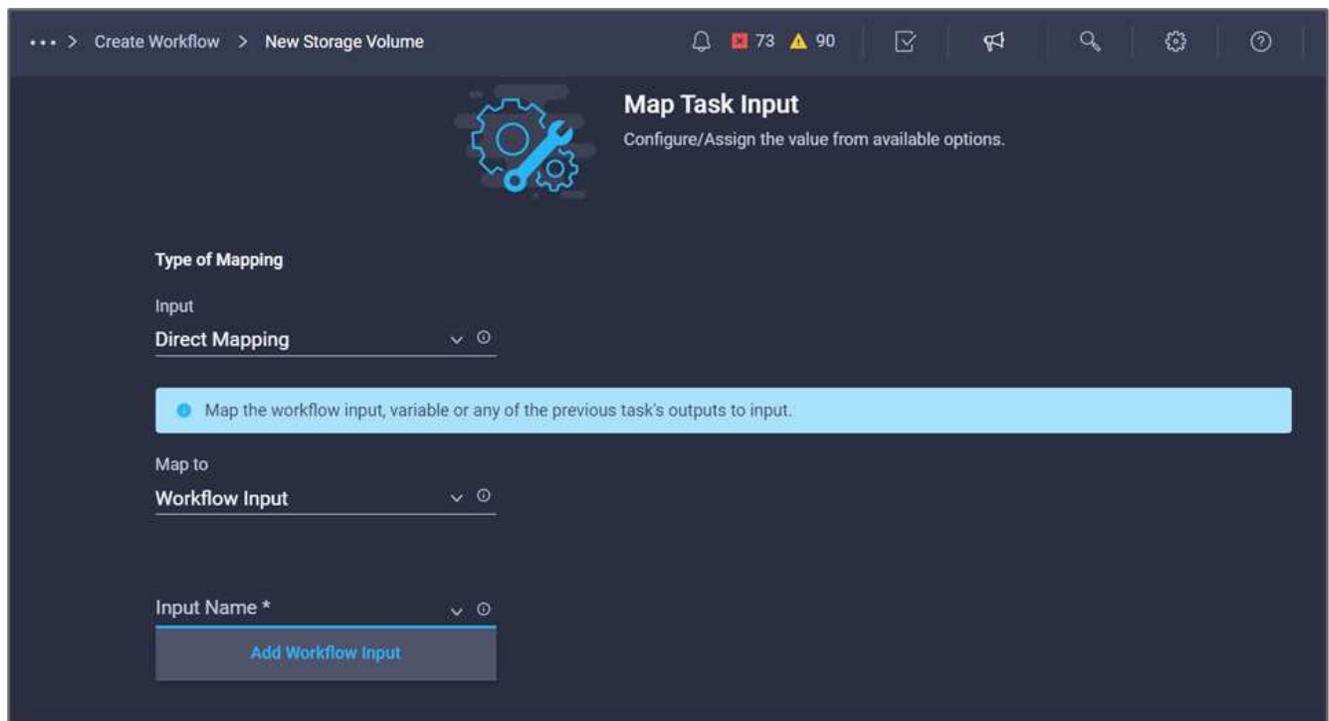
14. Cliquez sur **Map** dans le champ **Storage Vendor Aggregate**.



15. Choisissez **valeur statique** et cliquez sur **Sélectionner l'agrégat de stockage**. Choisissez l'agrégat et cliquez sur **Select**.



16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Storage Vendor Volume Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.



19. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Assurez-vous que **Storage Vendor Volume Options** est sélectionné pour **Type**.

- c. Cliquez sur **définir la valeur par défaut et remplacer**.
- d. Cliquez sur **requis**.
- e. Définissez **Type de plateforme** sur **NetApp Active IQ Unified Manager**.
- f. Indiquez une valeur par défaut pour le volume créé sous **Volume**.
- g. Cliquez sur **NFS**. Si NFS est défini, un volume NFS est créé. Si cette valeur est définie sur FALSE, un volume SAN est créé.
- h. Indiquez un chemin de montage et cliquez sur **Ajouter**.

Add Workflow Input

Set Default Value ⓘ

Allow User Override ⓘ

Default Values *

Storage Vendor Volume Options

Platform Type ⓘ

Pure FlashArray Hitachi Virtual Storage Platform NetApp Active IQ Unified Manager None

Volume *

mssql_data_vol ⓘ

NFS Volume Option

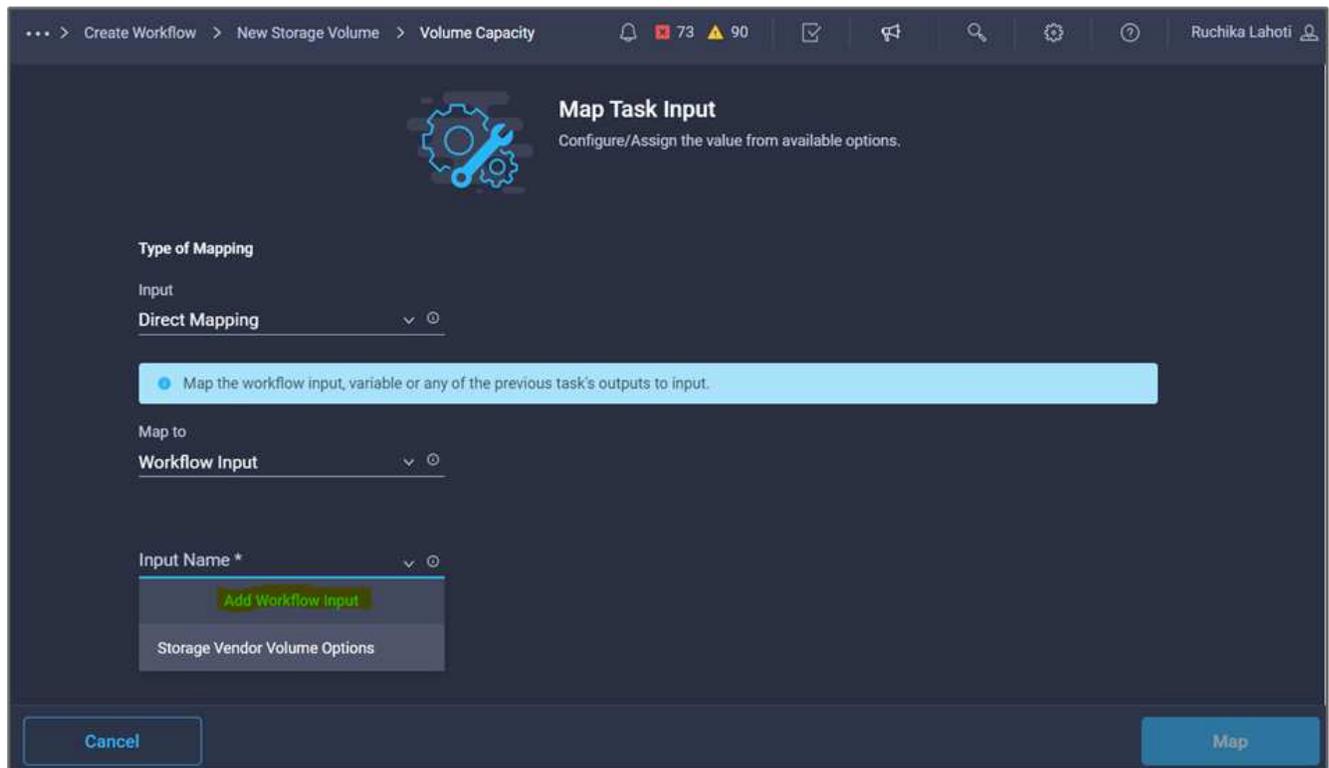
NFS ⓘ

Mount Path

/mssql_data_vol ⓘ

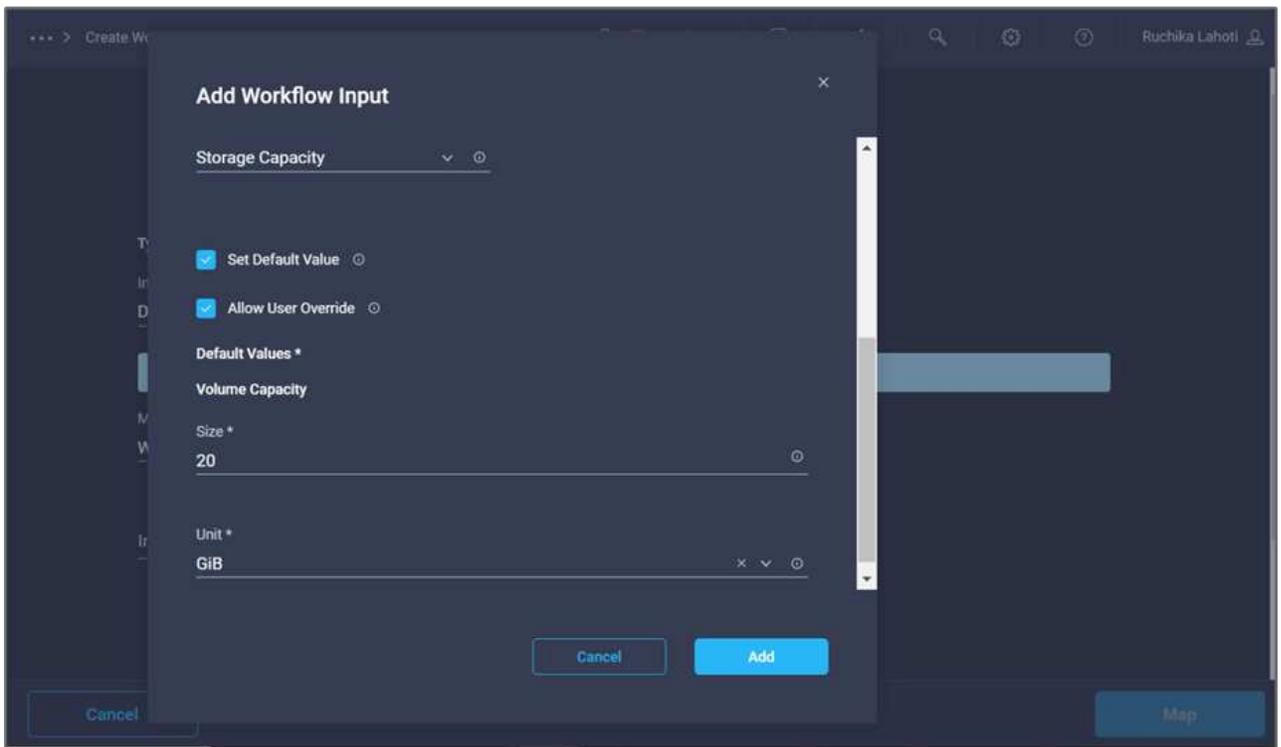
Cancel Add

20. Cliquez sur **carte**.
21. Cliquez sur **Map** dans le champ **Volume Capacity**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



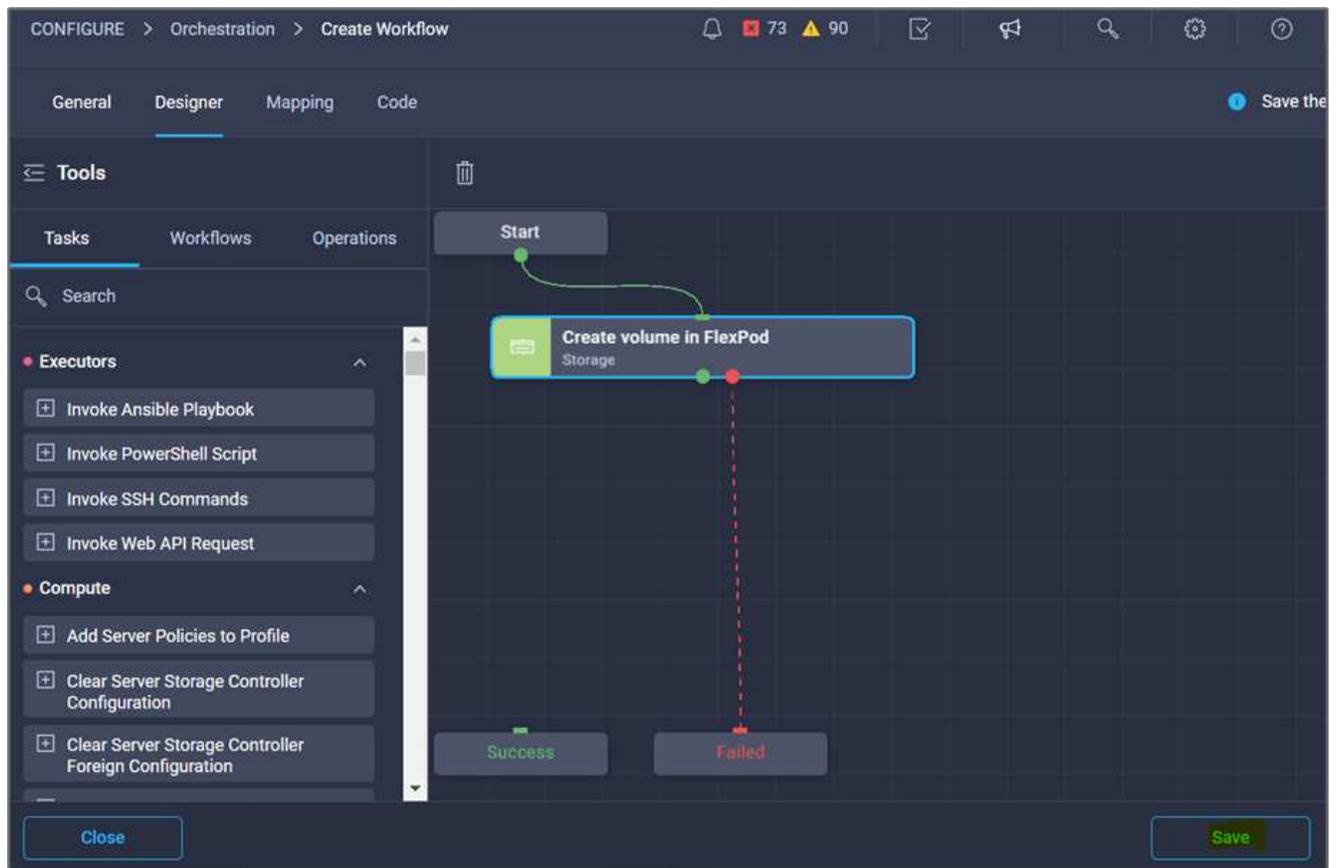
24. Dans l'assistant Ajouter une entrée :

- a. Indiquez un nom d'affichage et un nom de référence (facultatif).
- b. Cliquez sur **requis**.
- c. Pour **Type**, sélectionnez **capacité de stockage**.
- d. Cliquez sur **définir la valeur par défaut et remplacer**.
- e. Indiquez une valeur par défaut pour la taille du volume et l'unité.
- f. Cliquez sur **Ajouter**.



25. Cliquez sur **carte**.

26. Avec Connector, créez une connexion entre les tâches **Démarrer** et **Créer un volume dans FlexPod**, puis cliquez sur **Enregistrer**.





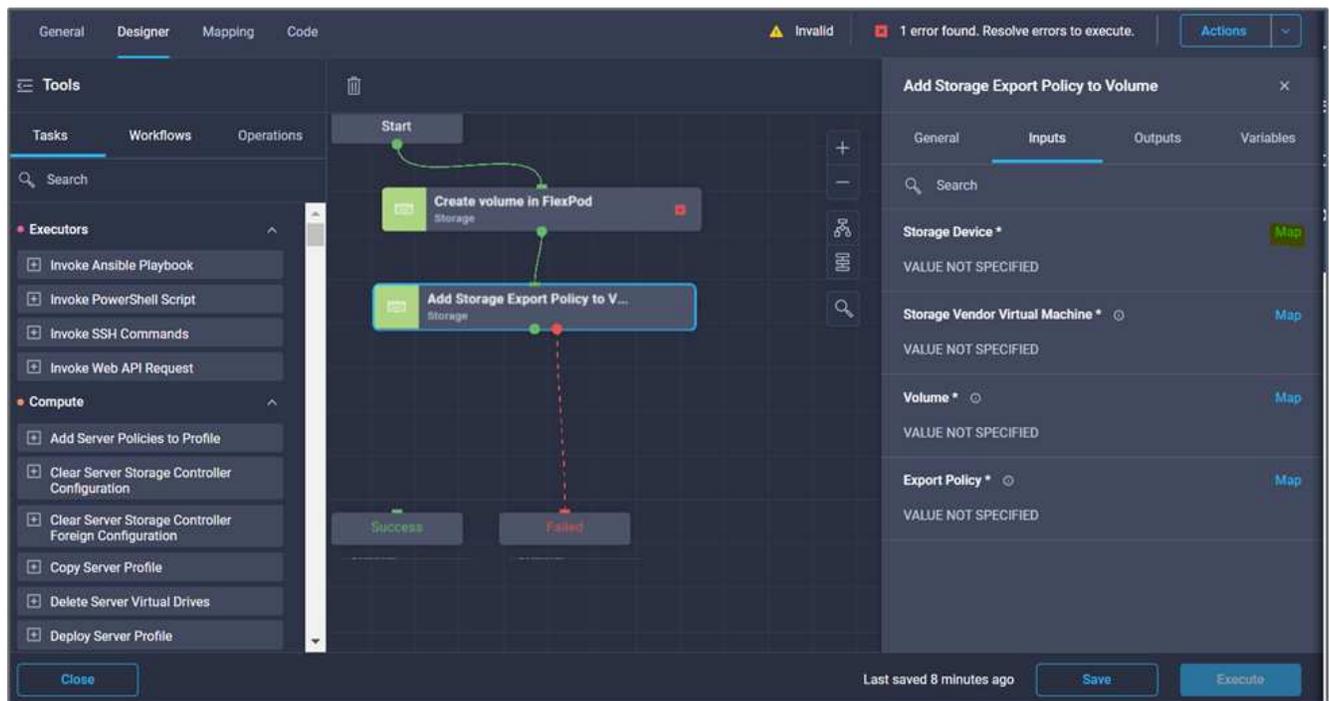
Ignorer l'erreur pour l'instant. Cette erreur s'affiche car il n'y a pas de connectivité entre les tâches **Créer un volume dans FlexPod** et **succès** qui est nécessaire pour spécifier la transition réussie.

Procédure 3 : ajout d'une règle d'exportation de stockage

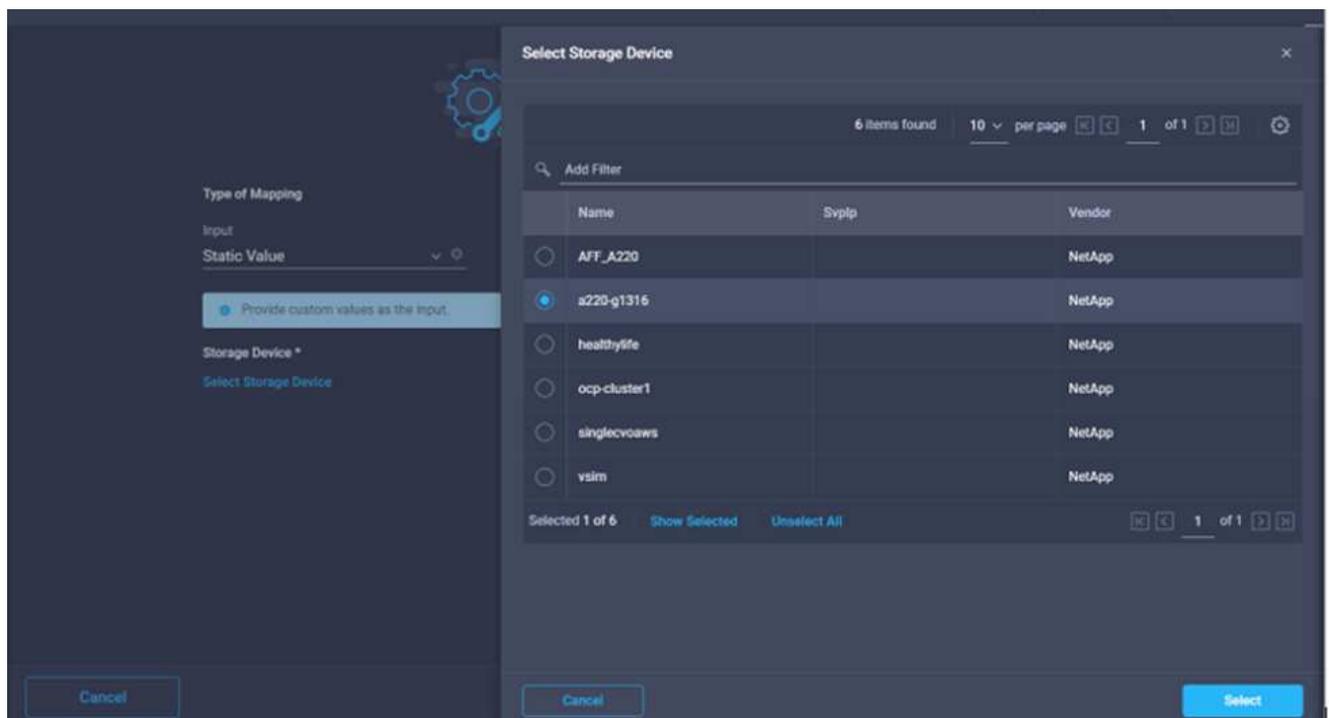
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **stockage > Ajouter une stratégie d'exportation de stockage au volume** à partir de la section **Outils** de la zone **Design**.
3. Cliquez sur **Ajouter une stratégie d'exportation de stockage au volume**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Ajouter une stratégie d'exportation de stockage**.
4. Utilisez Connector pour établir une connexion entre les tâches **Créer un volume dans FlexPod** et **Ajouter une stratégie d'exportation de stockage**. Cliquez sur **Enregistrer**.

The screenshot shows the workflow designer interface. On the left, a 'Tools' panel lists various storage tasks, including 'New Storage Export Policy'. The main workspace shows a workflow starting with 'Start', followed by 'Create volume in FlexPod' (Storage), and then 'Add Storage Export Policy to V...' (Storage). A red dashed line indicates a connection between the 'Add Storage Export Policy to V...' task and a 'Failed' terminal. The right-hand panel is titled 'Add Storage Export Policy to Volume' and shows the 'General' tab with fields for Name, Version, Task Type, and User Description. The 'Task Details' section provides instructions on how to use the task.

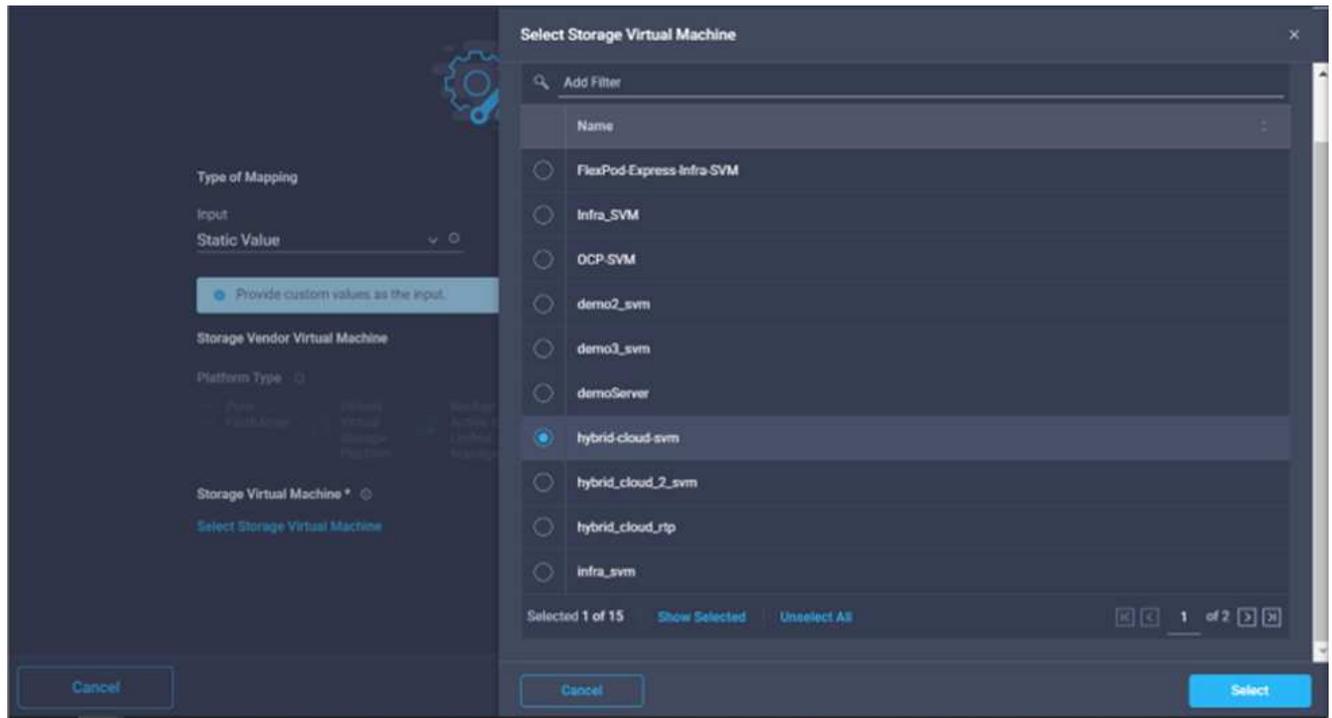
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Storage Device**.



7. Choisissez **valeur statique** et cliquez sur **Sélectionner le périphérique de stockage**. Sélectionnez la même cible de stockage ajoutée lors de la création de la tâche précédente de création d'un volume de stockage.
8. Cliquez sur **carte**.



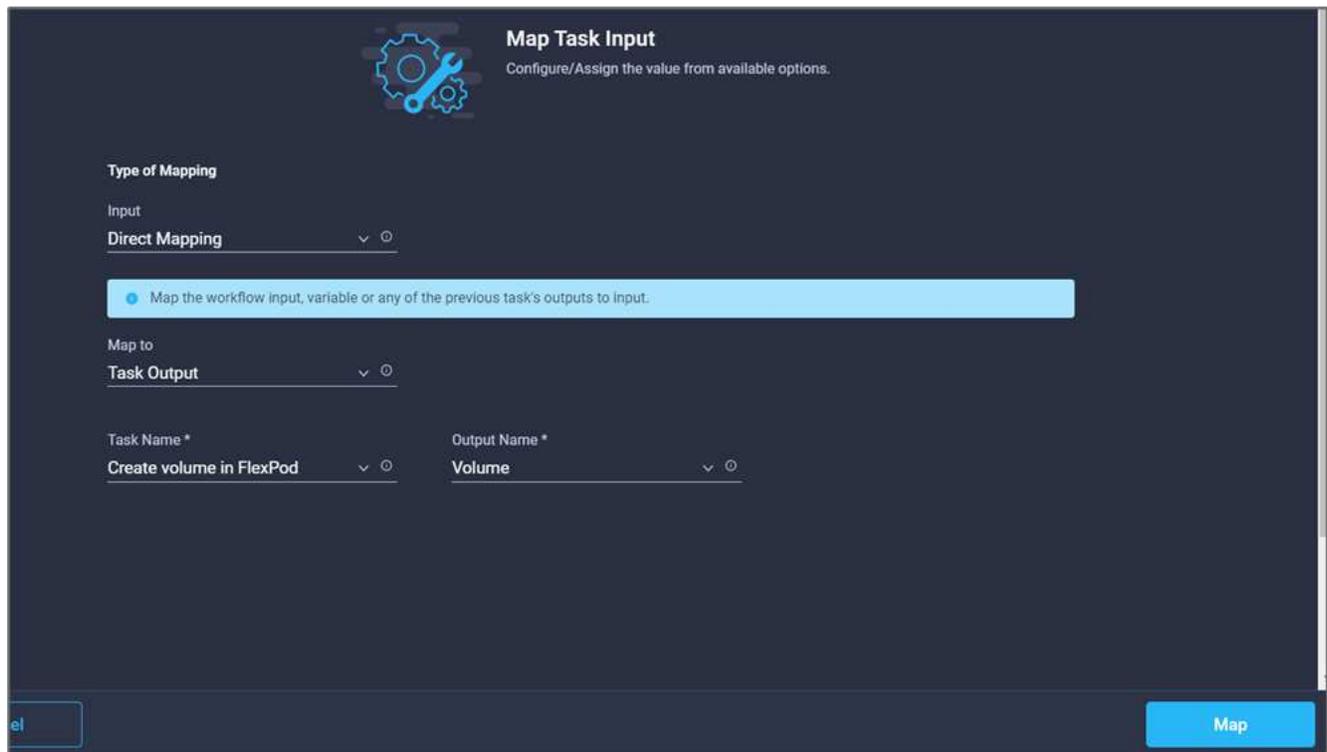
9. Cliquez sur **Map** dans le champ **Storage Vendor Virtual machine**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner Storage Virtual machine**. Sélectionnez la même machine virtuelle de stockage ajoutée lors de la création de la précédente tâche de création d'un volume de stockage.



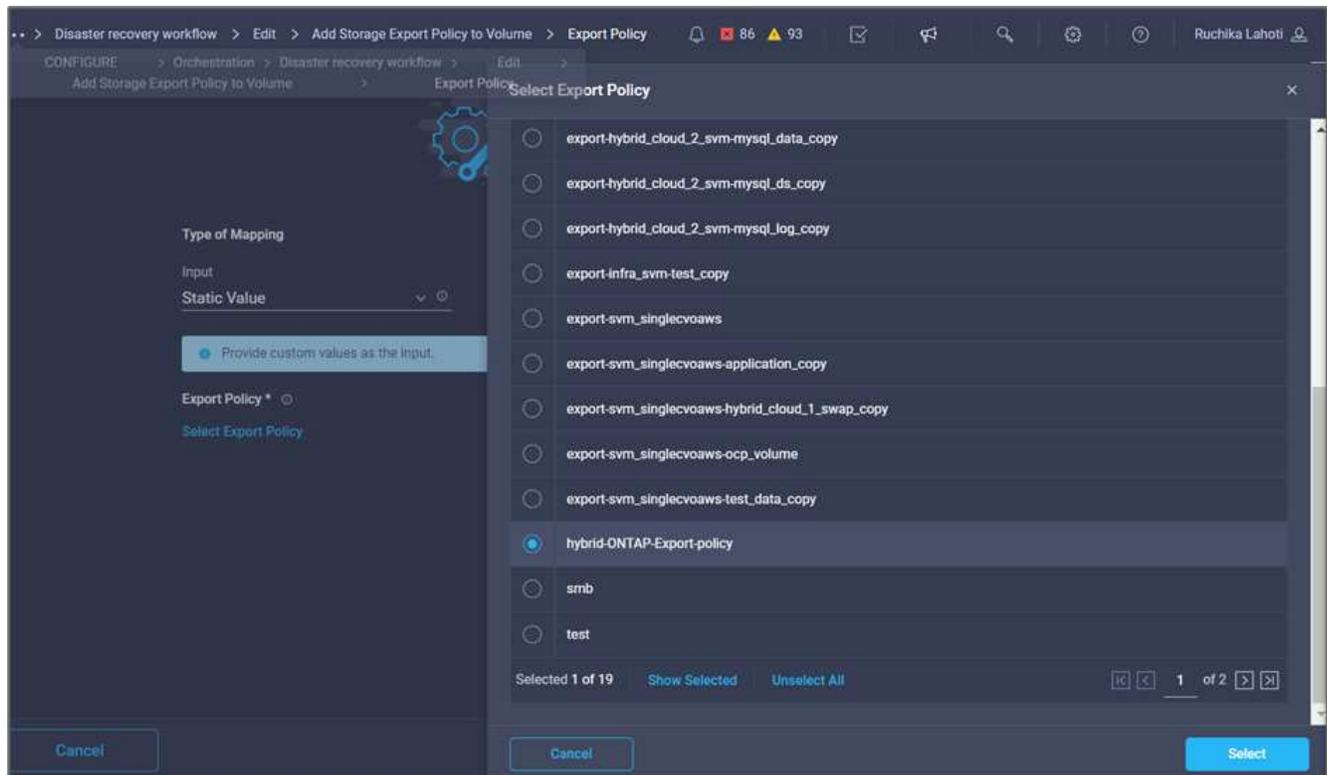
11. Cliquez sur **carte**.
12. Cliquez sur **Map** dans le champ **Volume**.
13. Cliquez sur **Nom de la tâche**, puis sur **Créer un volume dans FlexPod**. Cliquez sur **Nom de sortie**, puis sur **Volume**.



Dans Cisco Intersight Cloud Orchestrator, vous pouvez fournir la sortie d'une tâche précédente comme entrée pour une nouvelle tâche. Dans cet exemple, les détails **Volume** ont été fournis à partir de la tâche **Créer un volume dans FlexPod** sous forme d'entrée pour la tâche **Ajouter une stratégie d'exportation de stockage**.



14. Cliquez sur **carte**.
15. Cliquez sur **carte** dans le champ **politique d'exportation**.
16. Choisissez **valeur statique** et cliquez sur **Sélectionner stratégie d'exportation**. Sélectionner la export policy créée.



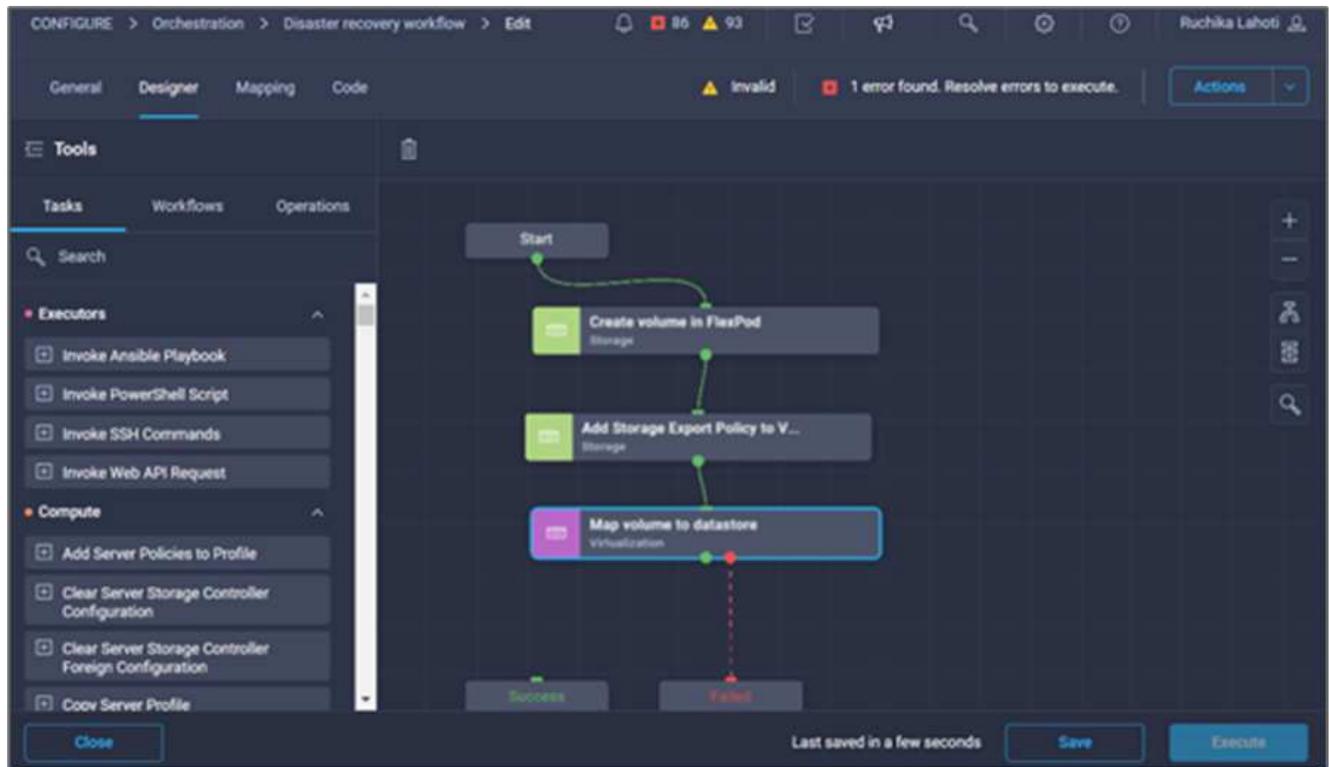
17. Cliquez sur **carte**, puis sur **Enregistrer**.



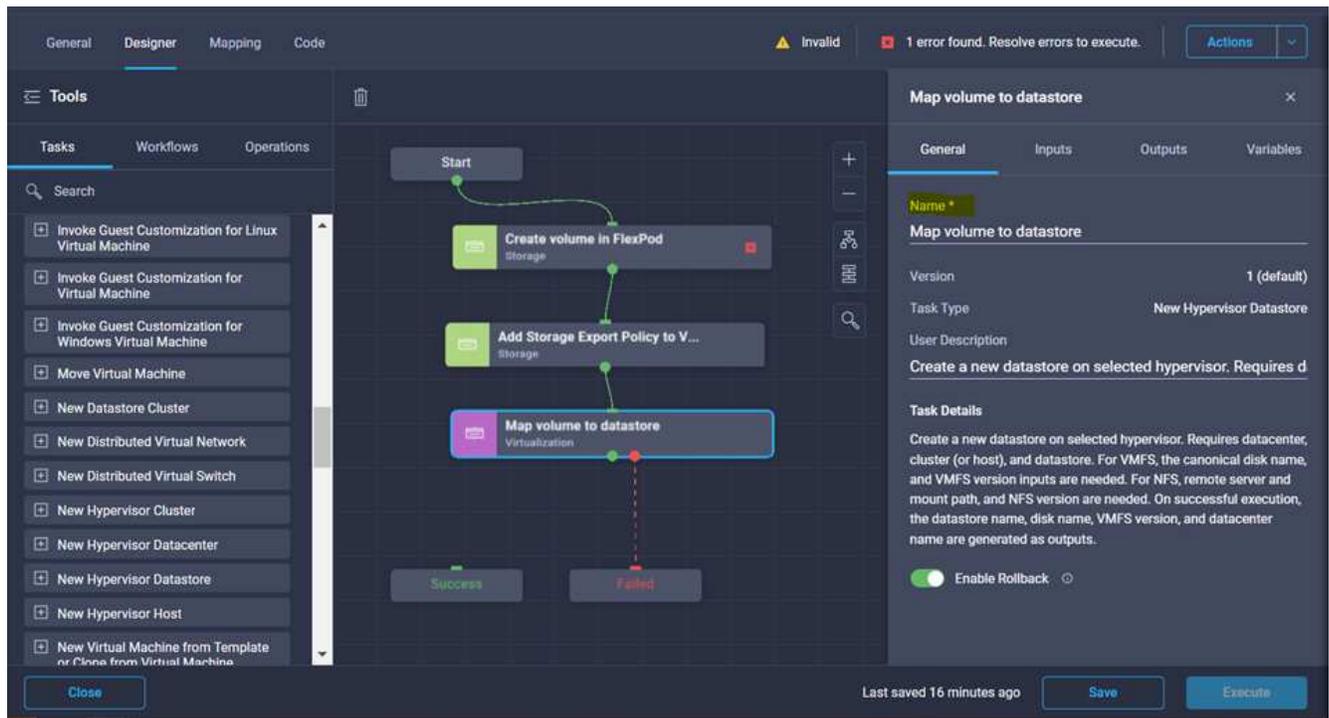
L'ajout d'une export-policy au volume est maintenant terminé. Ensuite, vous créez un nouveau datastore mappant le volume créé.

Procédure 4 : mappe de volumes FlexPod sur le datastore

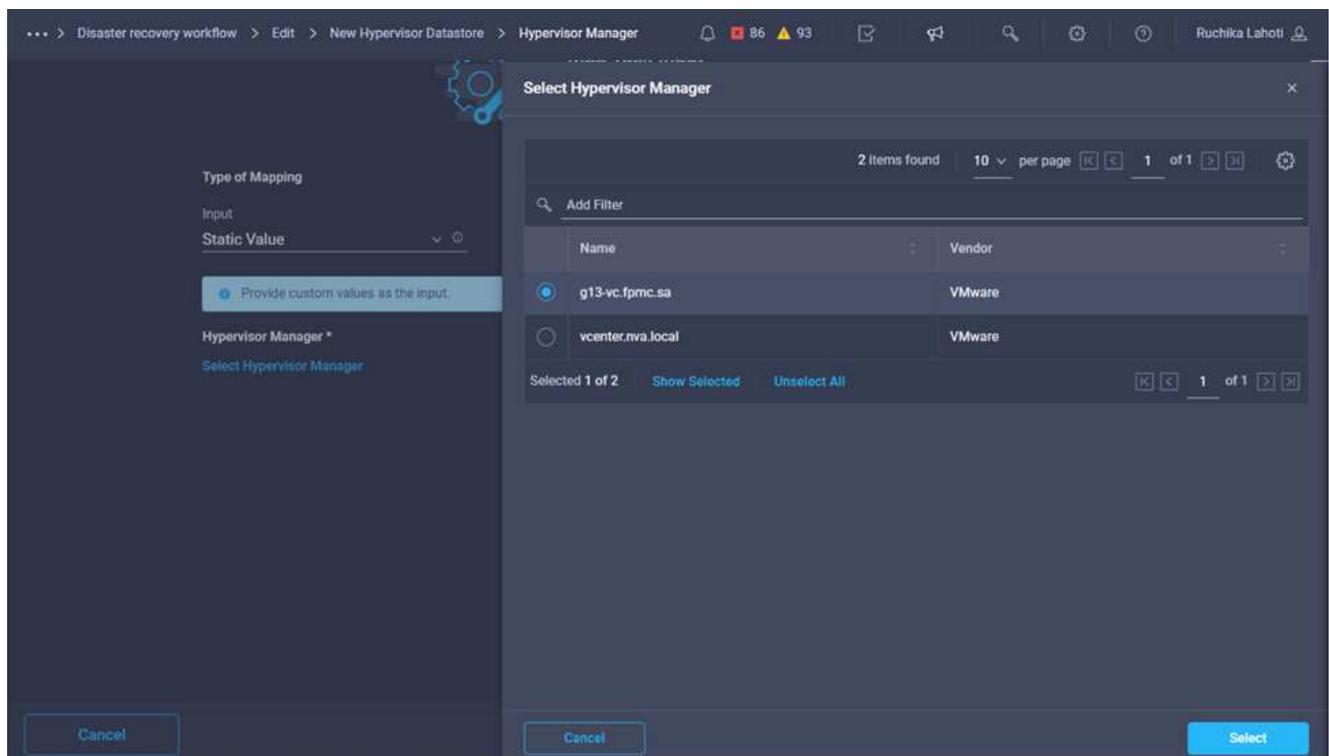
1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **virtualisation** > **Nouveau datastore d'hyperviseur** de la section **Outils** de la zone **Design**.
3. Utilisez Connector pour établir une connexion entre les tâches **Ajouter stratégie d'exportation de stockage** et **Nouveau datastore d'hyperviseur**. Cliquez sur **Enregistrer**.



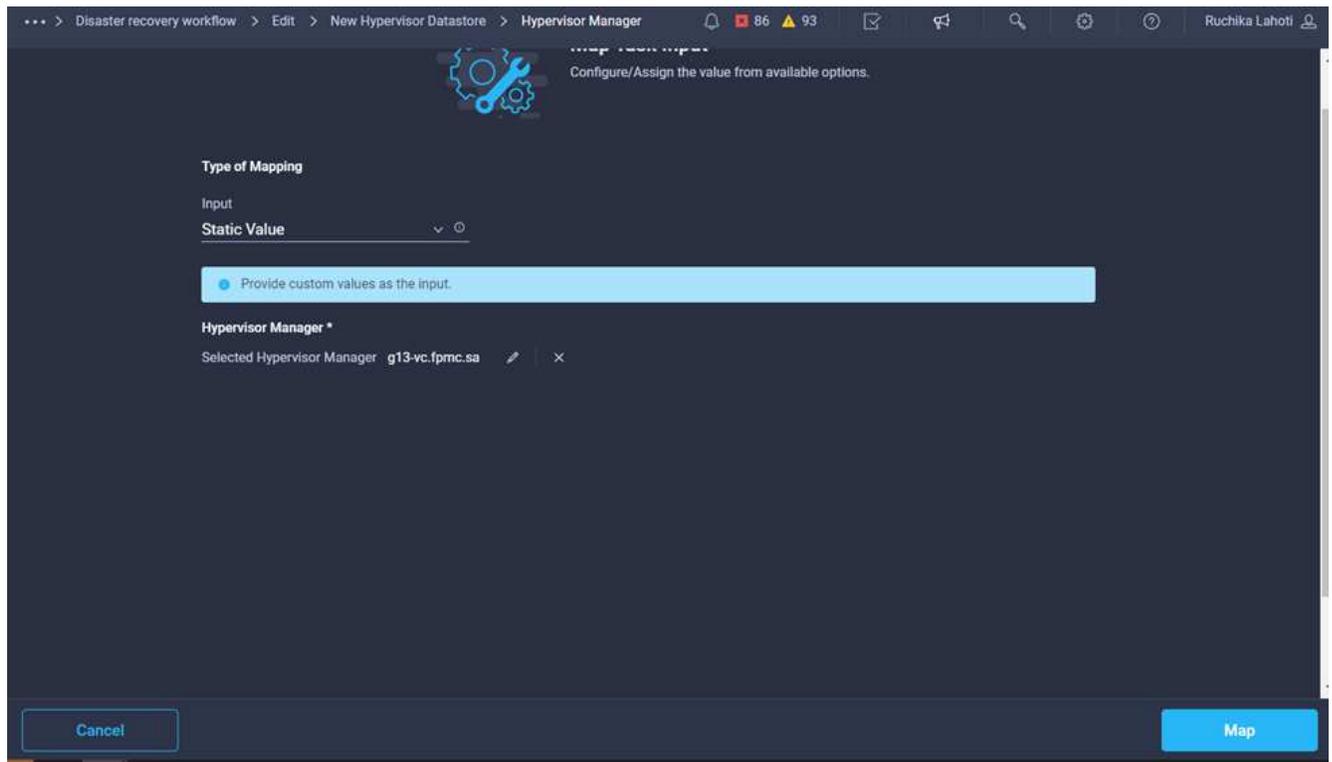
4. Cliquez sur **Nouveau datastore d'hyperviseur**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **mapper le volume sur le datastore**.



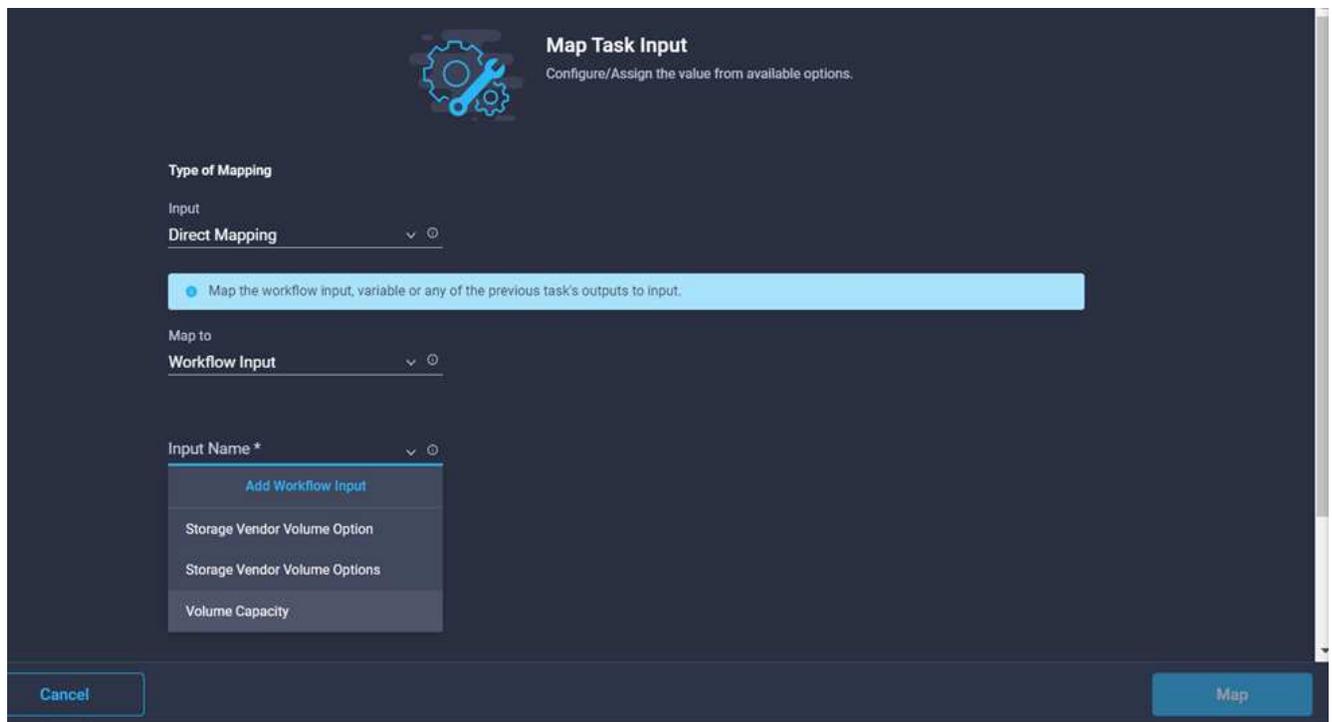
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **Map** dans le champ **Hypervisor Manager**.
7. Choisissez **valeur statique** et cliquez sur **Select Hypervisor Manager**. Cliquez sur la cible VMware vCenter.



8. Cliquez sur **carte**.

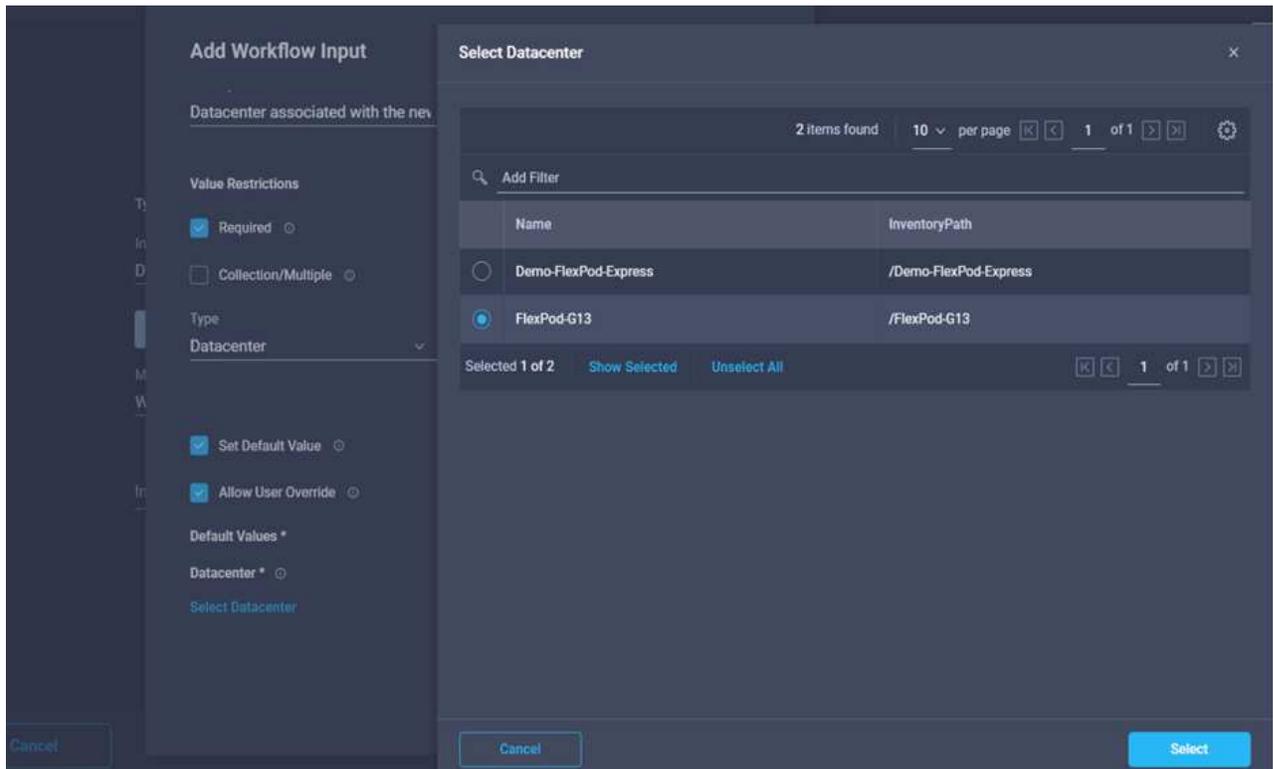


9. Cliquez sur **carte** dans le champ **Data Center**. Il s'agit du data Center associé au nouveau datastore.
10. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
11. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.



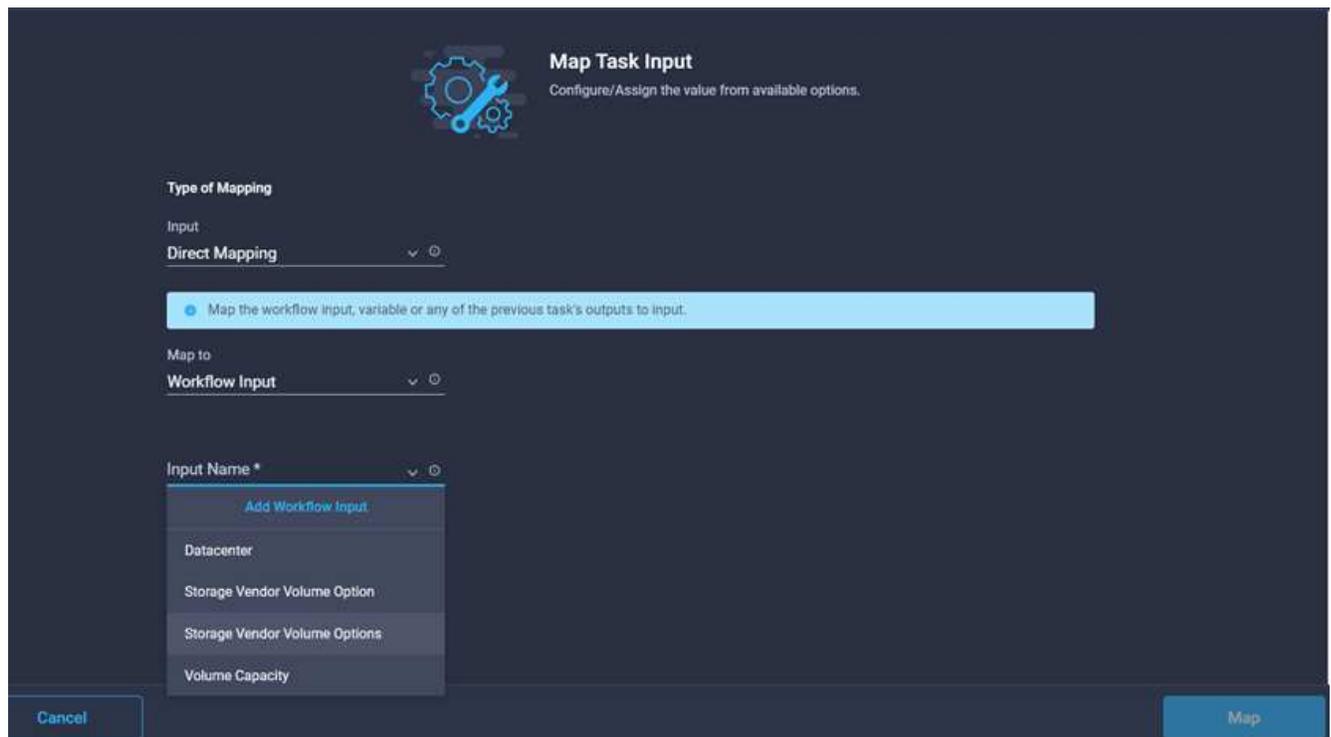
12. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Sélectionnez **Datacenter** comme type.

- c. Cliquez sur **définir la valeur par défaut et remplacer**.
- d. Cliquez sur **Select Datacenter**.
- e. Cliquez sur le centre de données associé au nouveau datastore, puis sur **Select**.

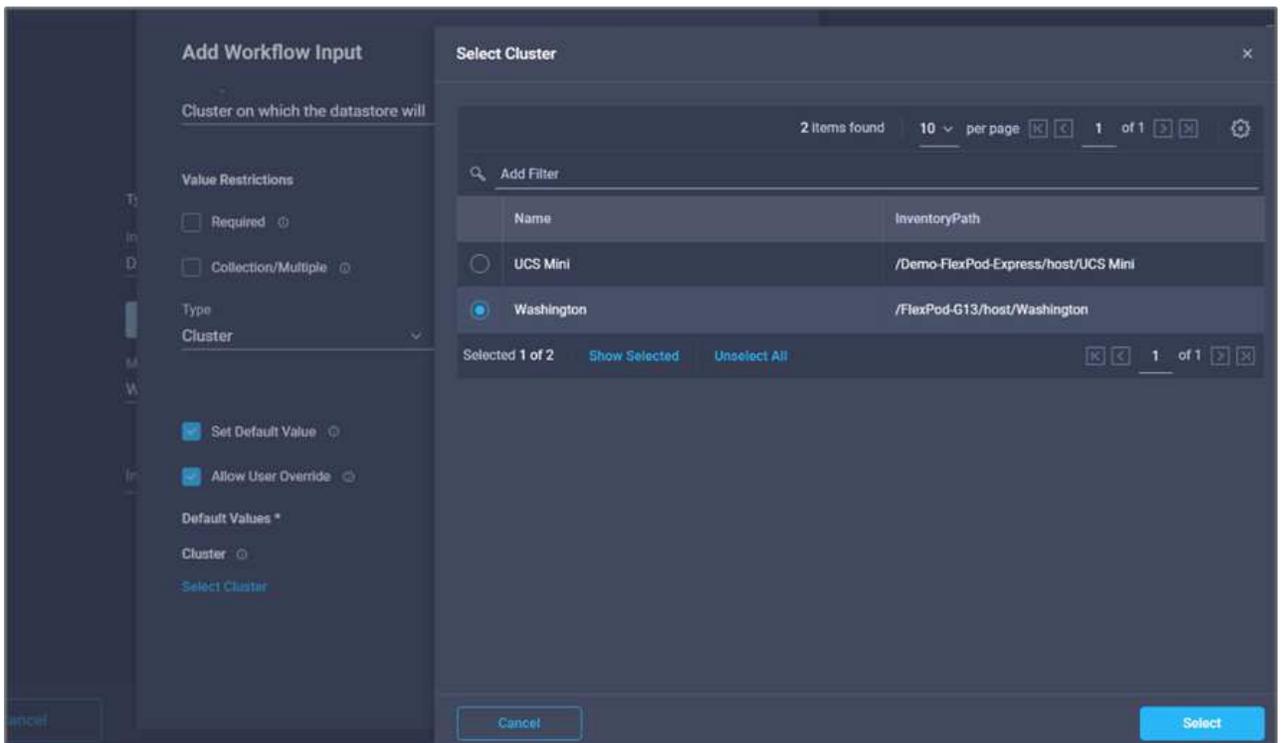


- Cliquez sur **Ajouter**.

13. Cliquez sur **carte**.
14. Cliquez sur **carte** dans le champ **Cluster**.
15. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.



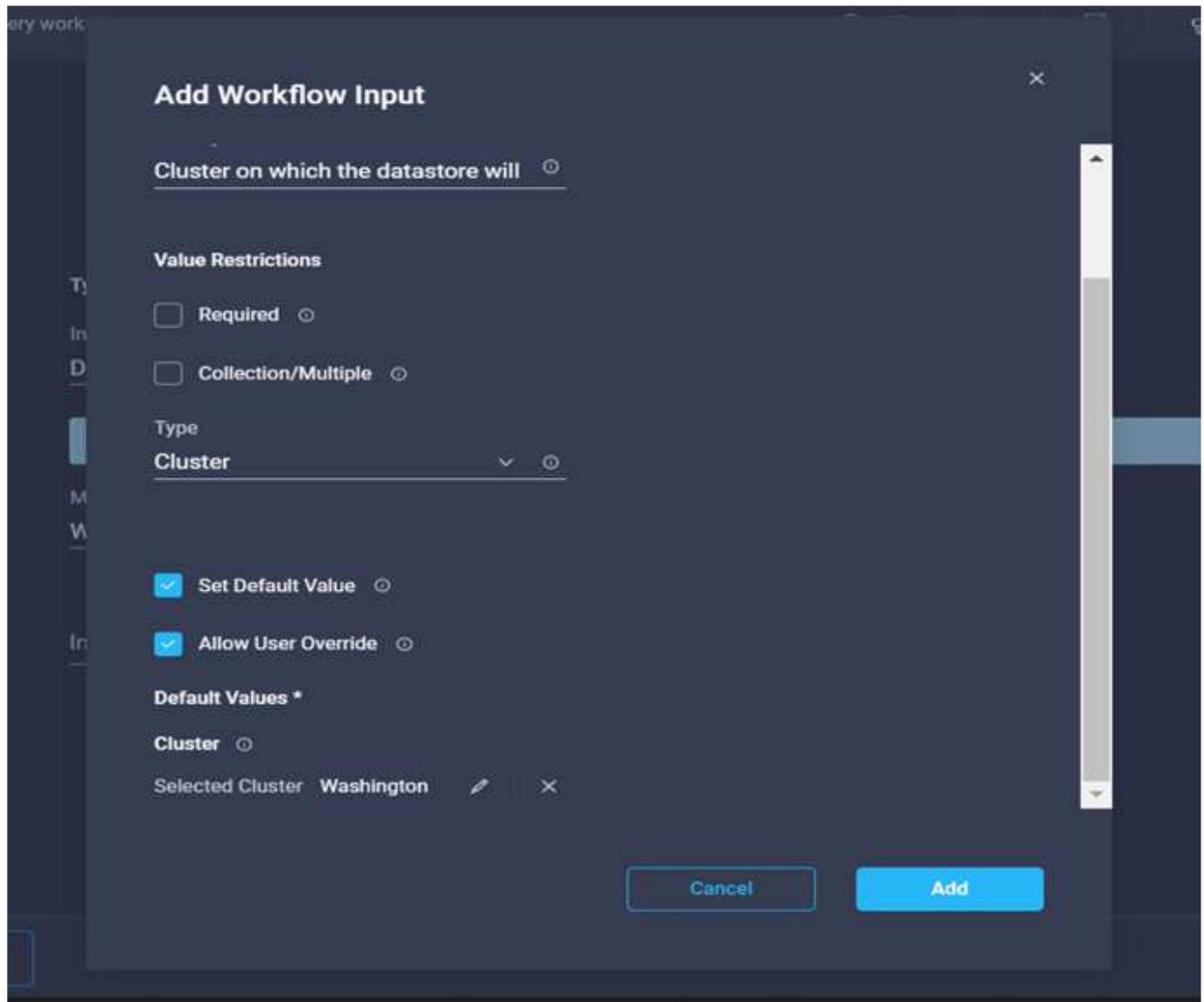
16. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Cliquez sur **requis**.
 - c. Sélectionnez Cluster comme type.
 - d. Cliquez sur **définir la valeur par défaut et remplacer**.
 - e. Cliquez sur **Sélectionner un cluster**.
 - f. Cliquez sur le cluster associé au nouveau datastore.
 - g. Cliquez sur **Sélectionner**.



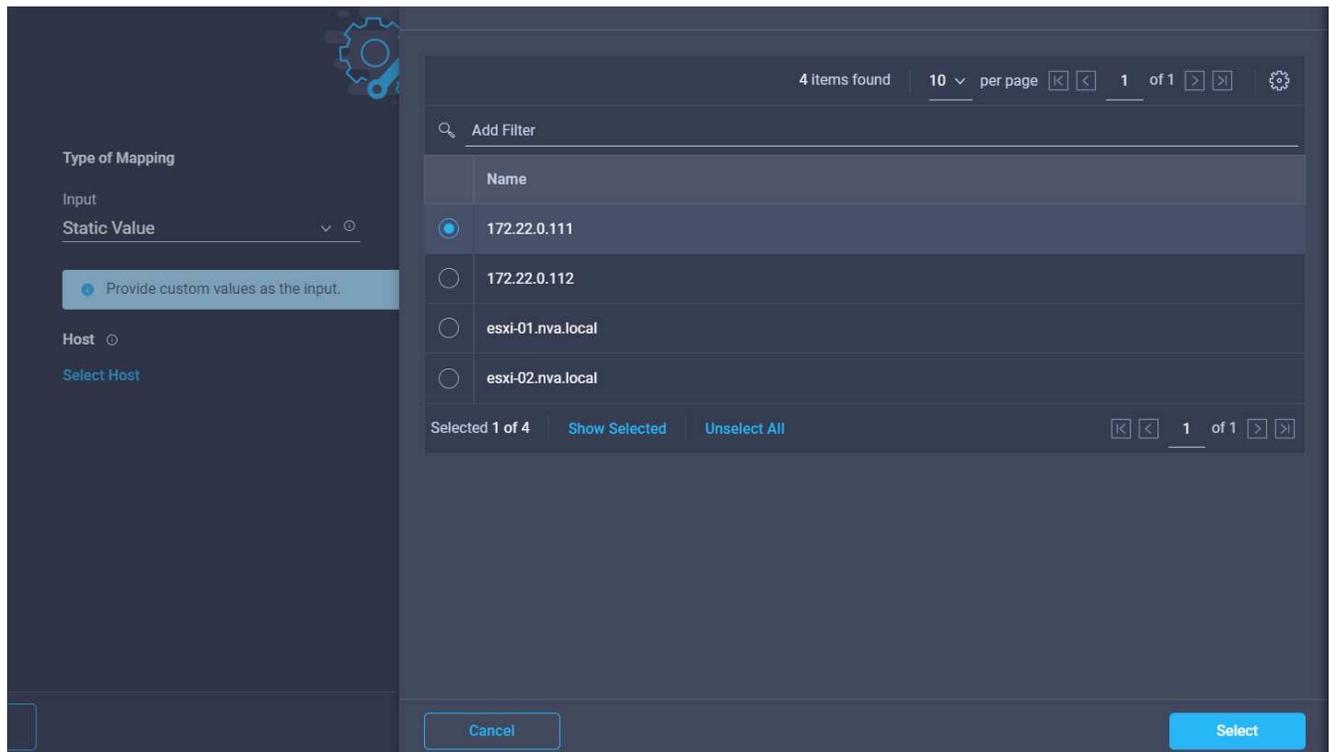
h. Cliquez sur **Ajouter**.

17. Cliquez sur **carte**.

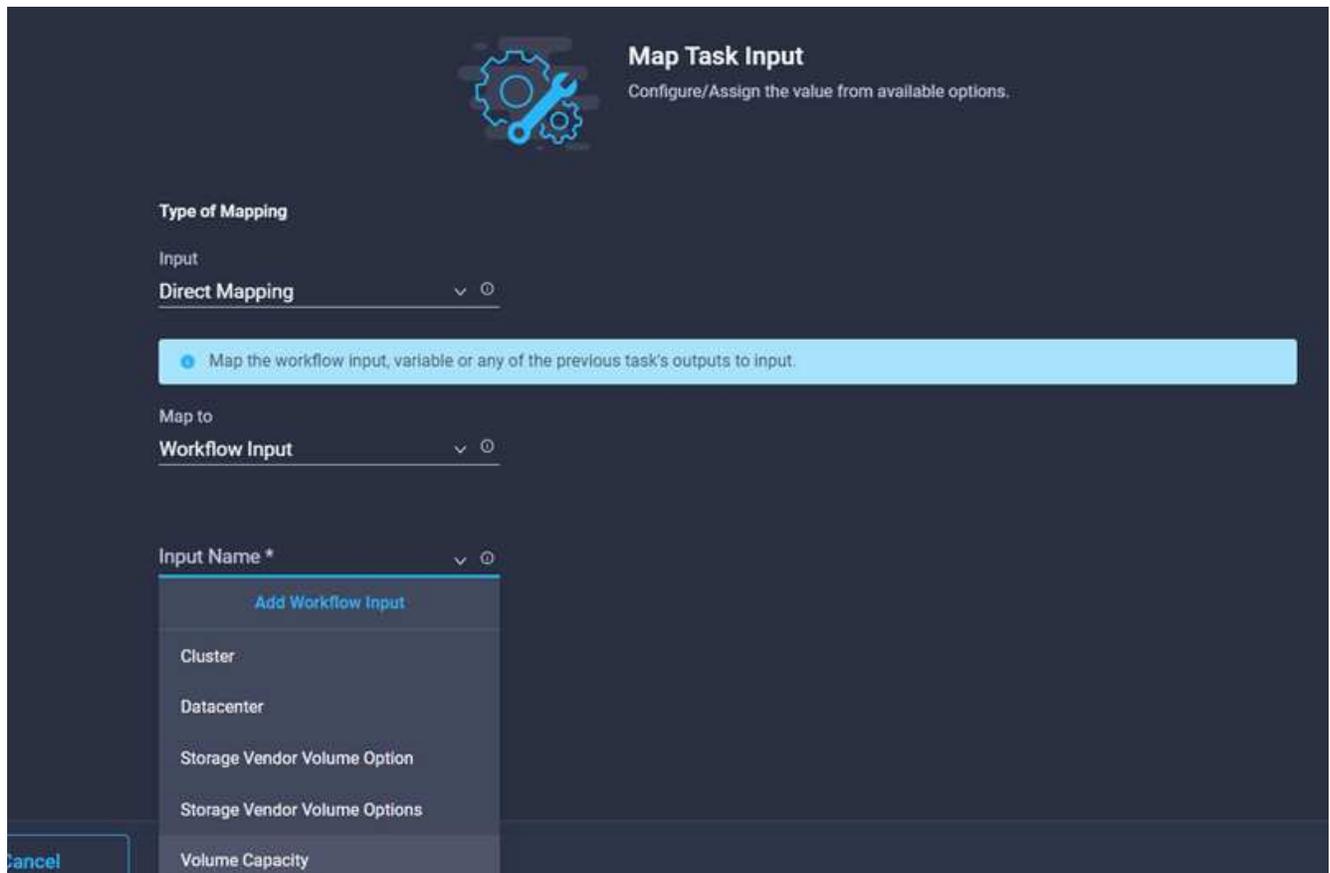
18. Cliquez sur **Map** dans le champ **Host**.



19. Choisissez **valeur statique** et cliquez sur l'hôte sur lequel le datastore sera hébergé. Si un cluster est spécifié, l'hôte est ignoré.



20. Cliquez sur **Sélectionner et carte**.
21. Cliquez sur **Map** dans le champ **datastore**.
22. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
23. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



24. Dans l'assistant Ajouter une entrée :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Cliquez sur **requis**.
 - c. Cliquez sur **définir la valeur par défaut et remplacer**.
 - d. Indiquez une valeur par défaut pour le datastore et cliquez sur **Ajouter**.

Add Workflow Input

Type
String

Min 0 Max 0 Regex ^.{1,42}\$

Secure

Object Selector

Set Default Value

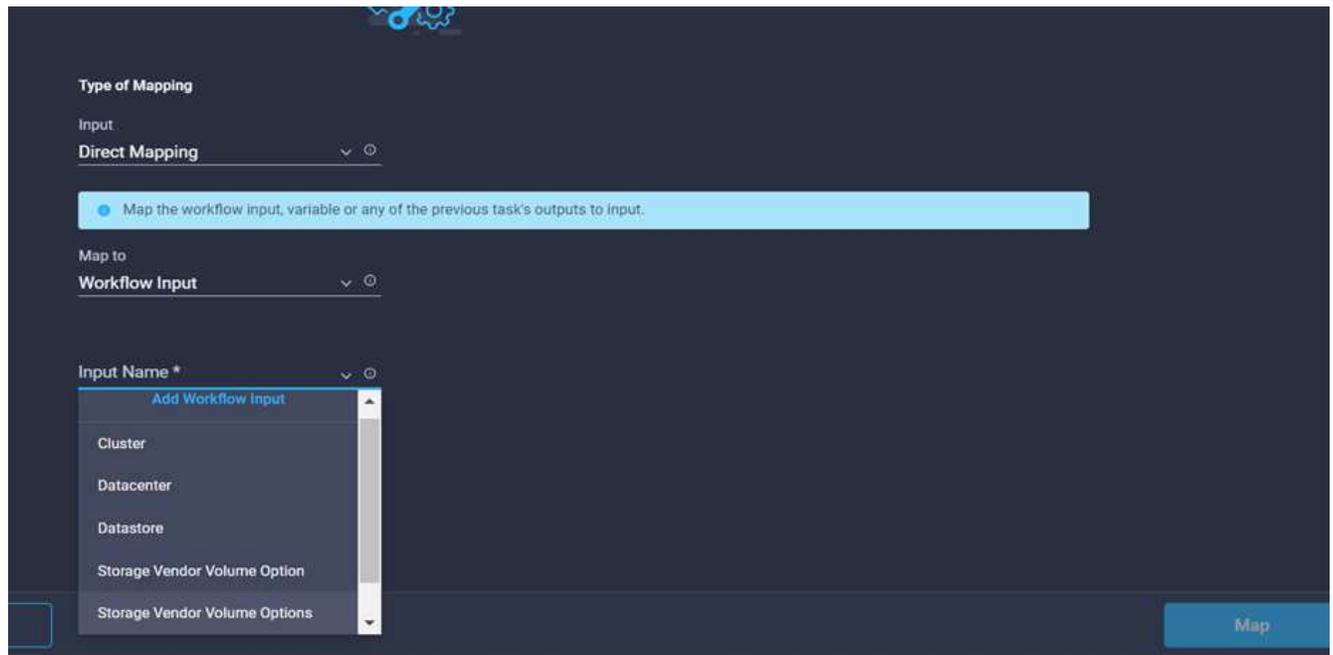
Allow User Override

Default Values *

Datastore *
hybrid-ds

Cancel Add

25. Cliquez sur **carte**.
26. Cliquez sur **carte** dans le champ de saisie **Type de datastore**.
27. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
28. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



29. Dans l'assistant Ajouter une entrée, procédez comme suit :

- a. Indiquez un nom d'affichage et un nom de référence (facultatif) et cliquez sur **requis**.
- b. Assurez-vous de sélectionner le type **types de datastore** et cliquez sur **définir la valeur par défaut et remplacer**.

Add Workflow Input

Display Name *
Type of Datastore

Reference Name *
DatastoreVersion

Description
Type and version of the new dataset

Value Restrictions

Required

Collection/Multiple

Type
Types of Datastore

Set Default Value

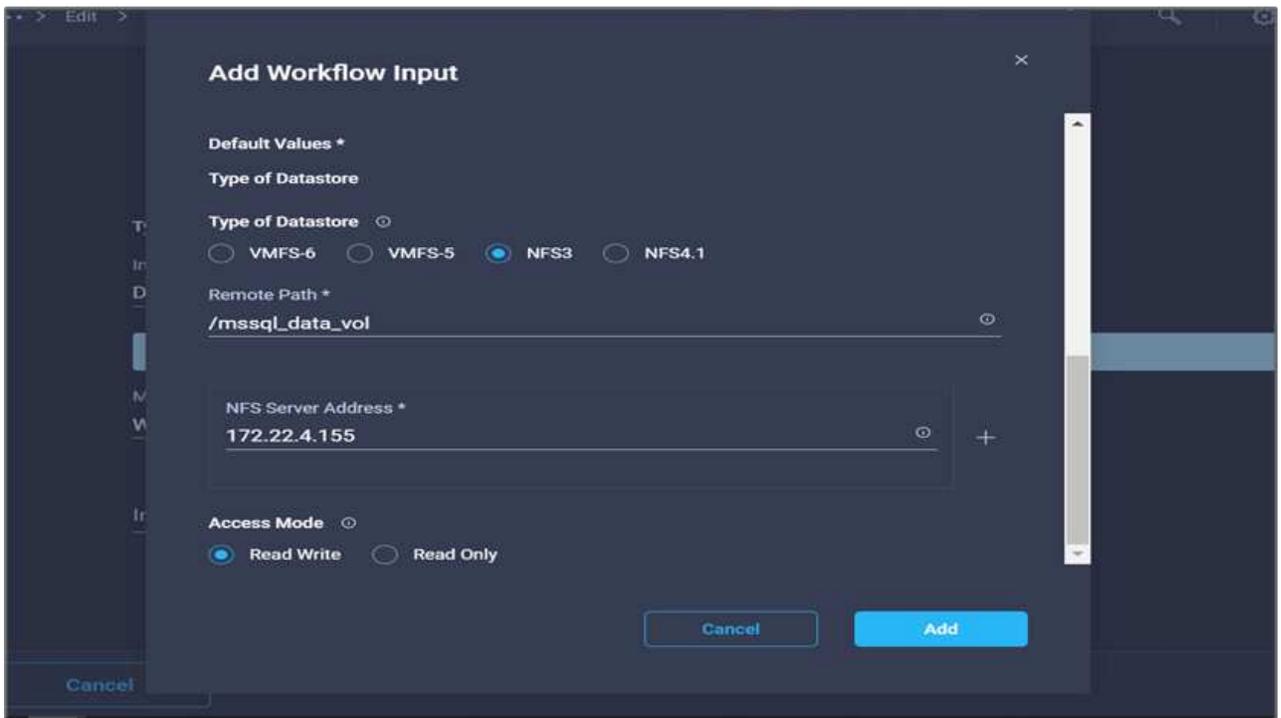
Allow User Override

Default Values *

Type of Datastore

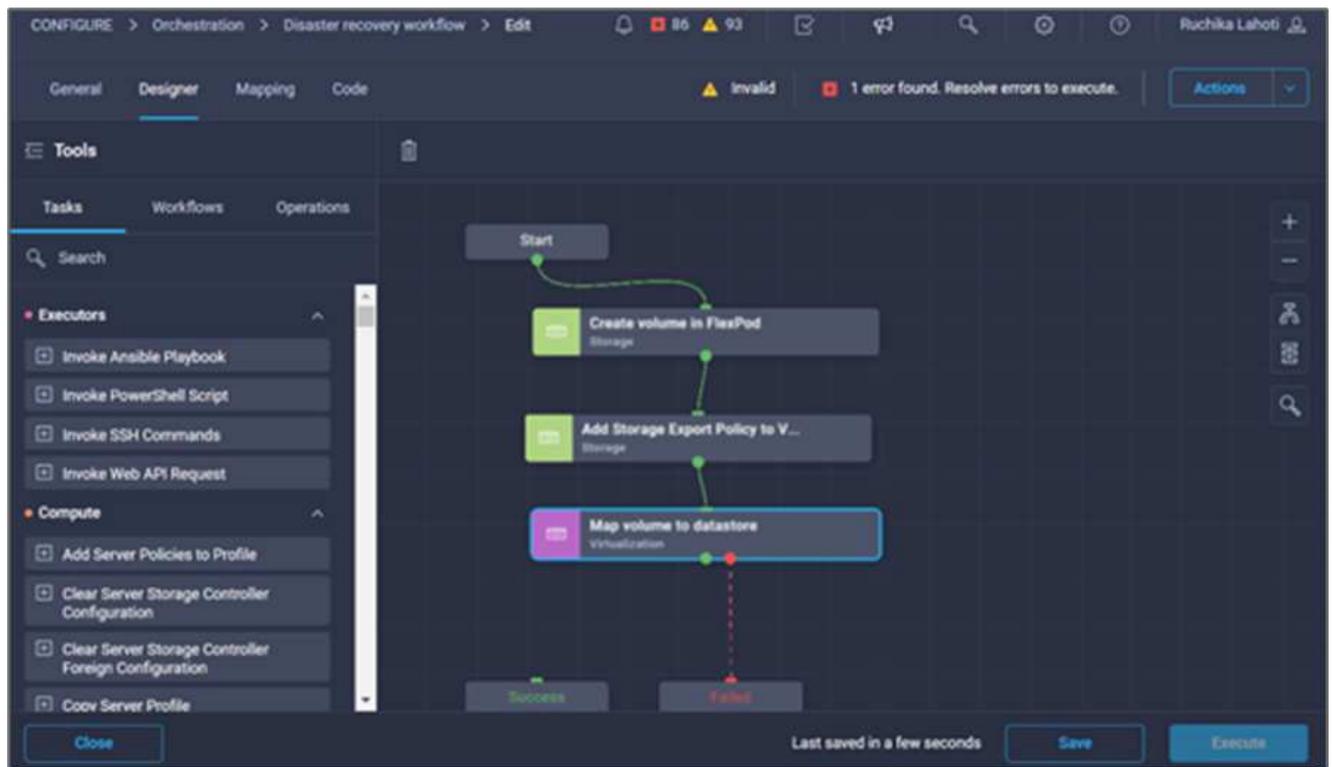
Cancel Add

- c. Indiquez le chemin distant. Il s'agit du chemin d'accès distant du point de montage NFS.
- d. Indiquez les noms d'hôte ou les adresses IP du serveur NFS distant dans l'adresse du serveur NFS.
- e. Cliquez sur le **mode d'accès**. Le mode d'accès est destiné au serveur NFS. Cliquez sur lecture seule si les volumes sont exportés en lecture seule. Cliquez sur **Ajouter**.

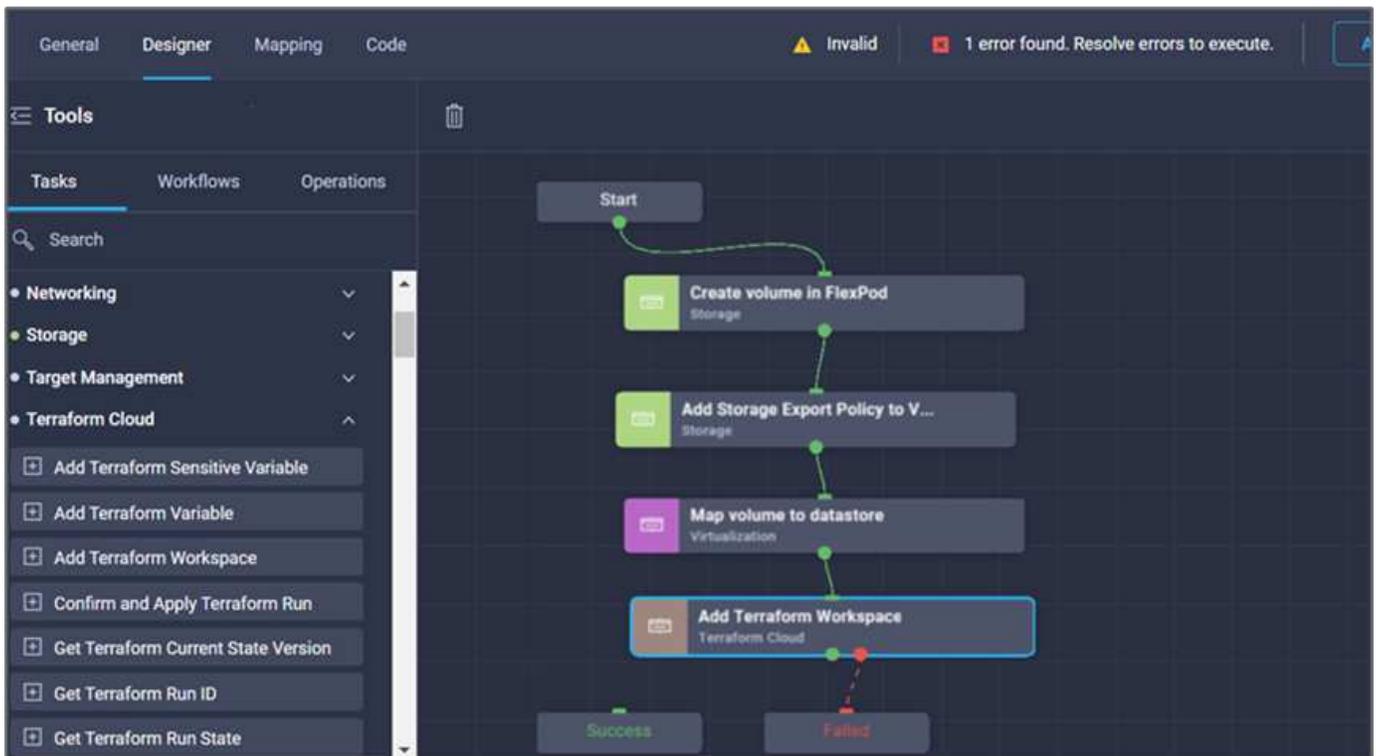


30. Cliquez sur **carte**.

31. Cliquez sur **Enregistrer**.

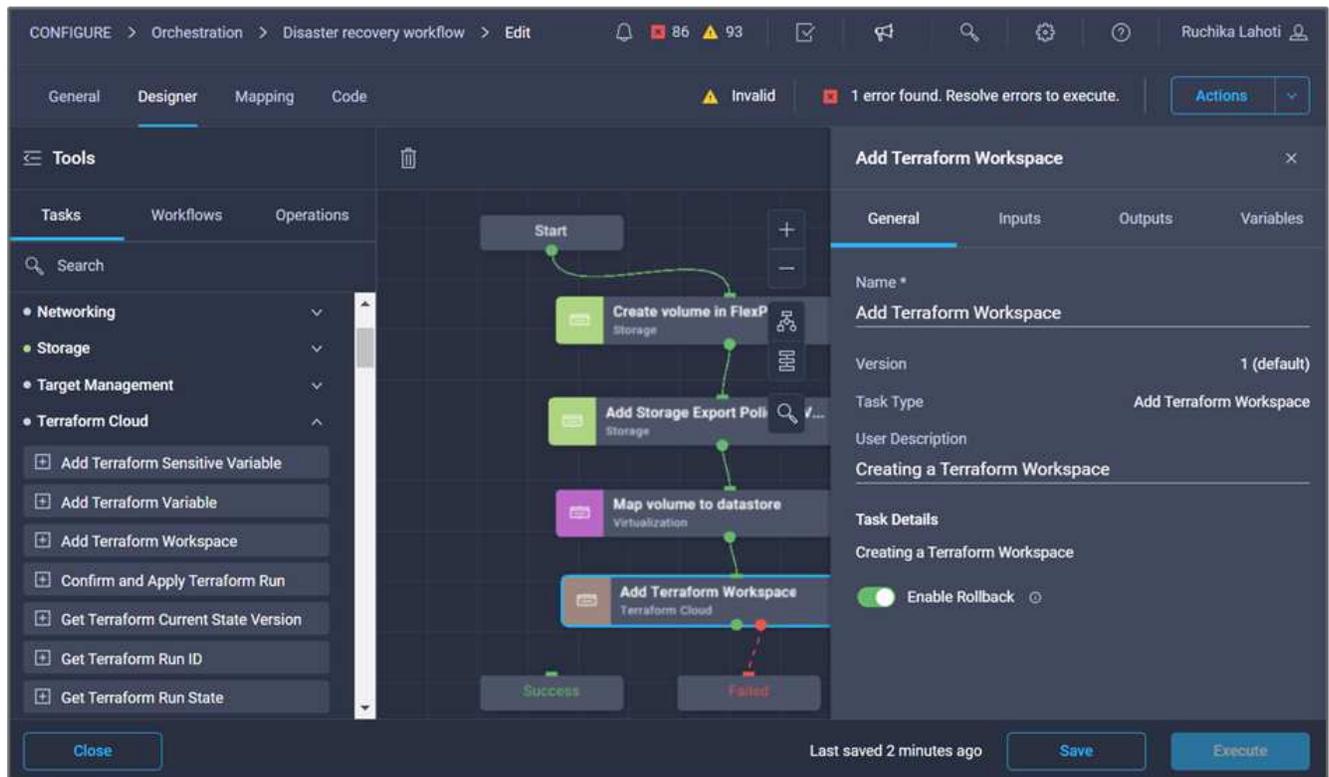


La tâche de création du datastore est terminée. Toutes les tâches effectuées dans le data Center FlexPod sur site sont effectuées.

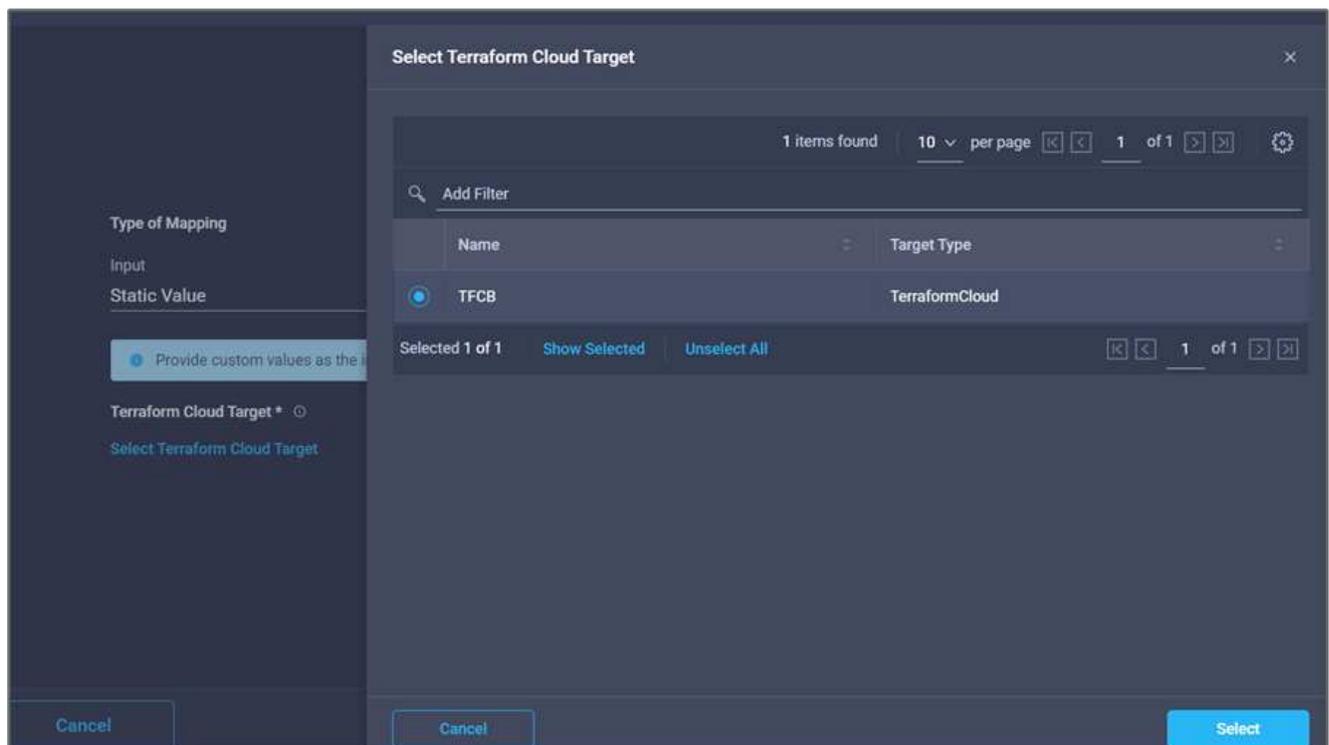


Procédure 5 : Ajout d'un nouvel espace de travail Terraform

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Ajouter un espace de travail Terraform** dans la section Outils de la zone conception.
3. Utilisez Connector pour connecter les tâches **Map volume au datastore** et **Add Terraform Workspace** et cliquez sur **Save**.
4. Cliquez sur **Ajouter un espace de travail Terraform**. Dans la zone Propriétés de la tâche, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.

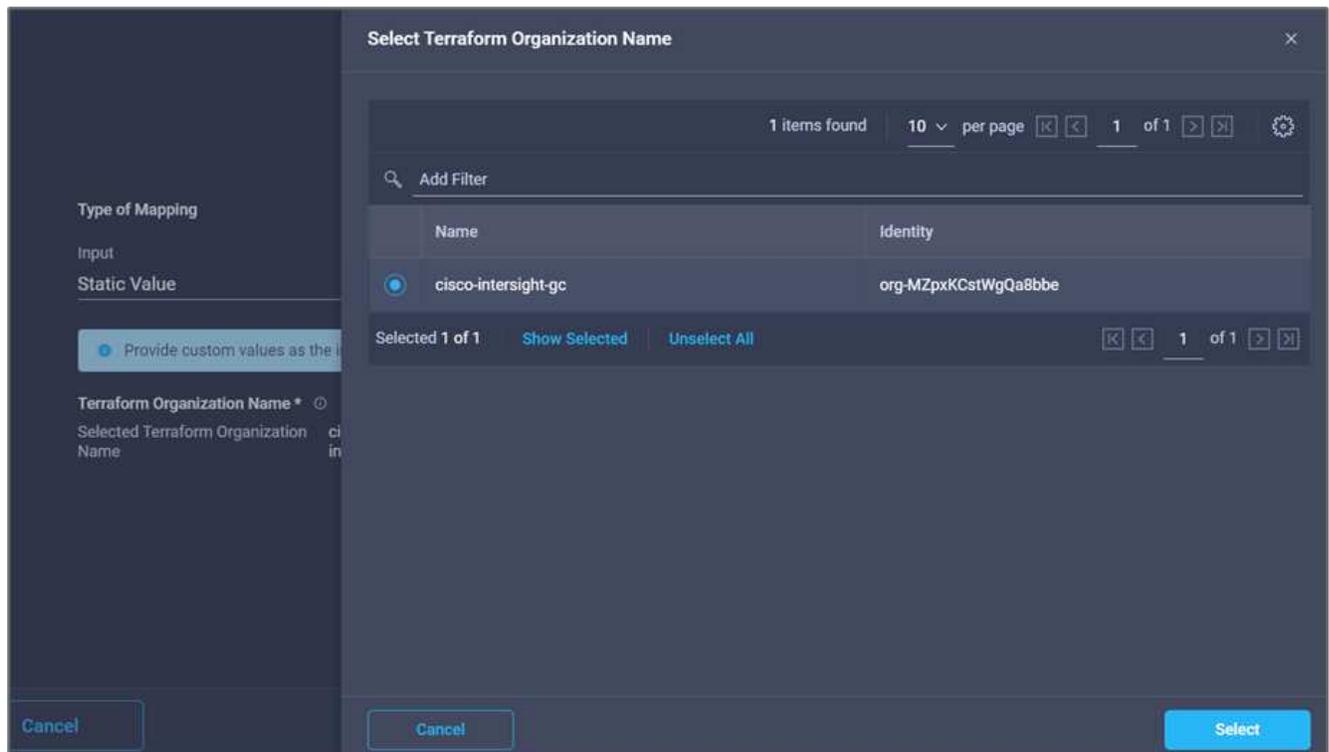


5. Dans la zone Propriétés de la tâche, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ de saisie **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "[Configurez Cisco Intersight Service pour HashiCorp Terraform](#)". ».

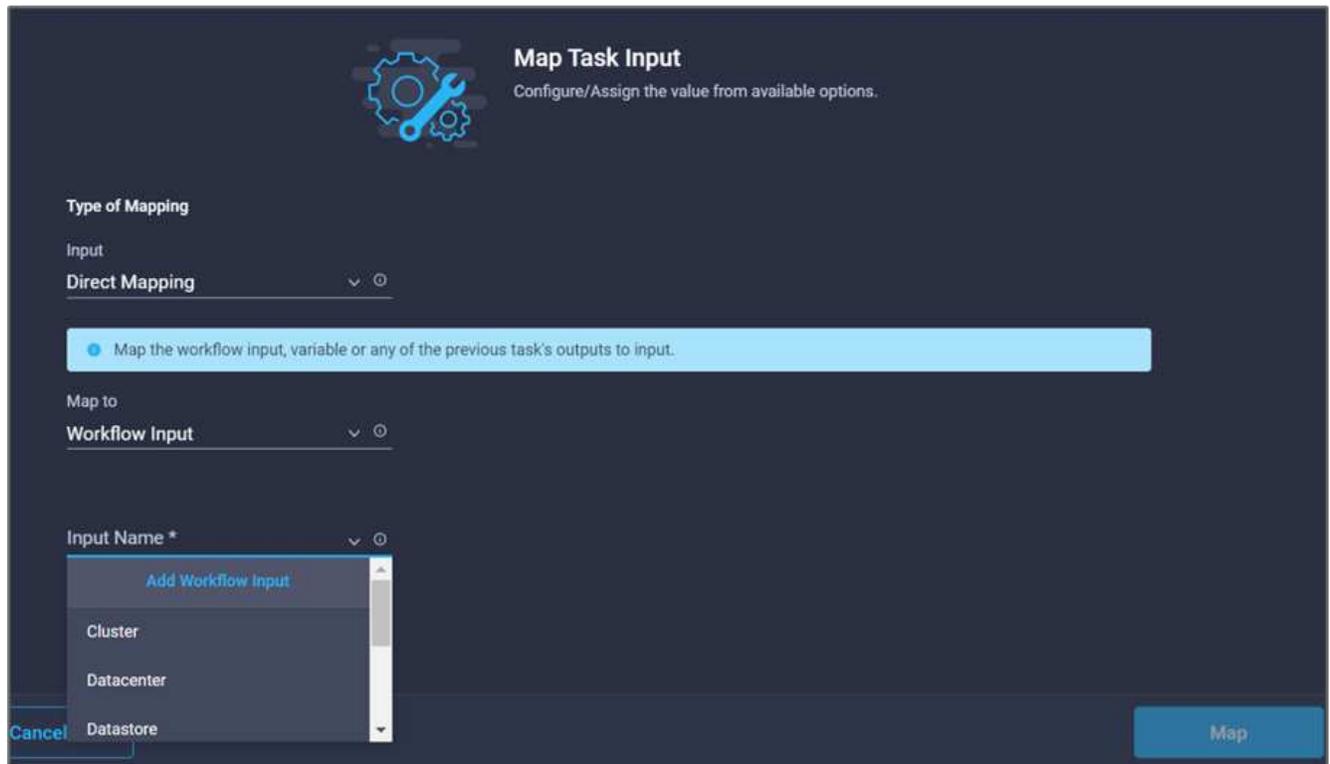


8. Cliquez sur **carte**.

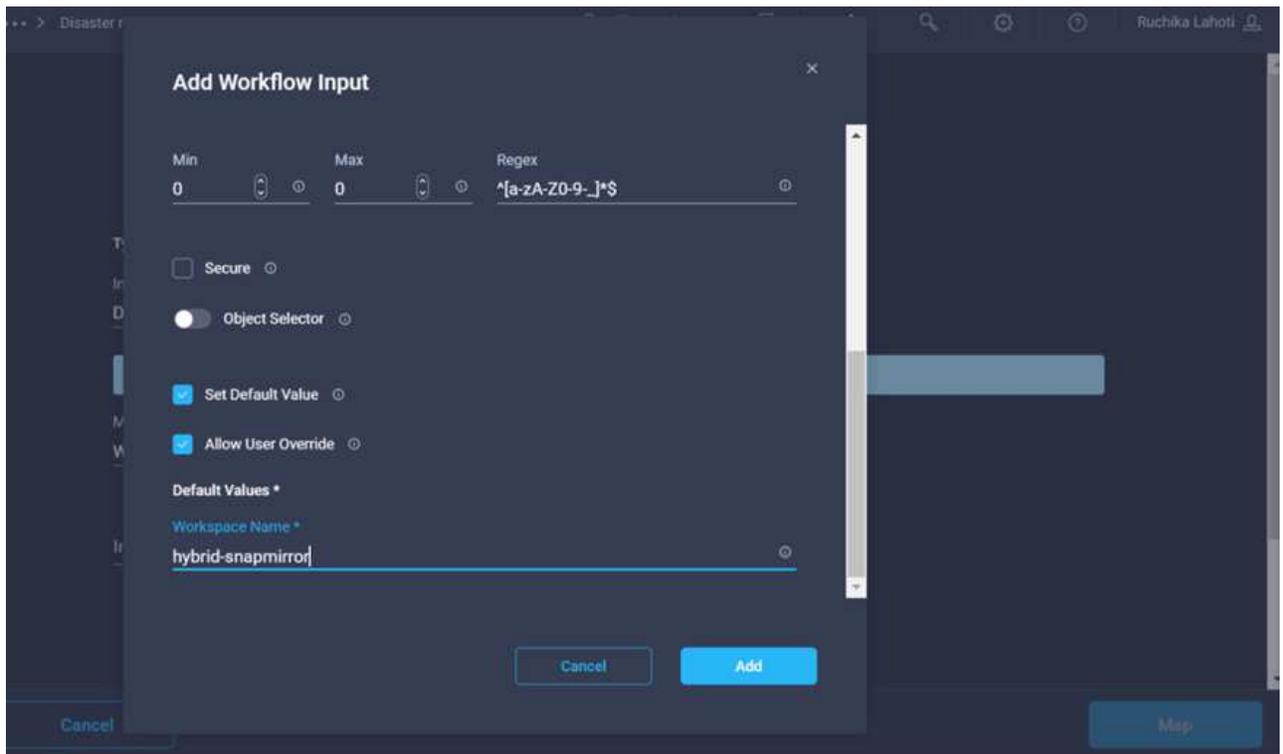
9. Cliquez sur **carte** dans le champ de saisie **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique**, puis cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.



11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**. Il s'agit du nouvel espace de travail dans le compte Terraform Cloud for Business.
13. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
14. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.



15. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Cliquez sur **requis**.
 - c. Assurez-vous de sélectionner **String** pour **Type**.
 - d. Cliquez sur **définir la valeur par défaut et remplacer**.
 - e. Indiquez un nom par défaut pour l'espace de travail.
 - f. Cliquez sur **Ajouter**.



16. Cliquez sur **carte**.
17. Cliquez sur **carte** dans le champ **Description de l'espace de travail**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.

Add Workflow Input ✕

Workspace Description ⓘ WorkspaceDescription ⓘ

Description
Description of the Terraform Work: ⓘ

Value Restrictions

Required ⓘ

Collection/Multiple ⓘ

Type
String ⓘ

Min 0 ⓘ Max 0 ⓘ Regex ⓘ

Secure ⓘ

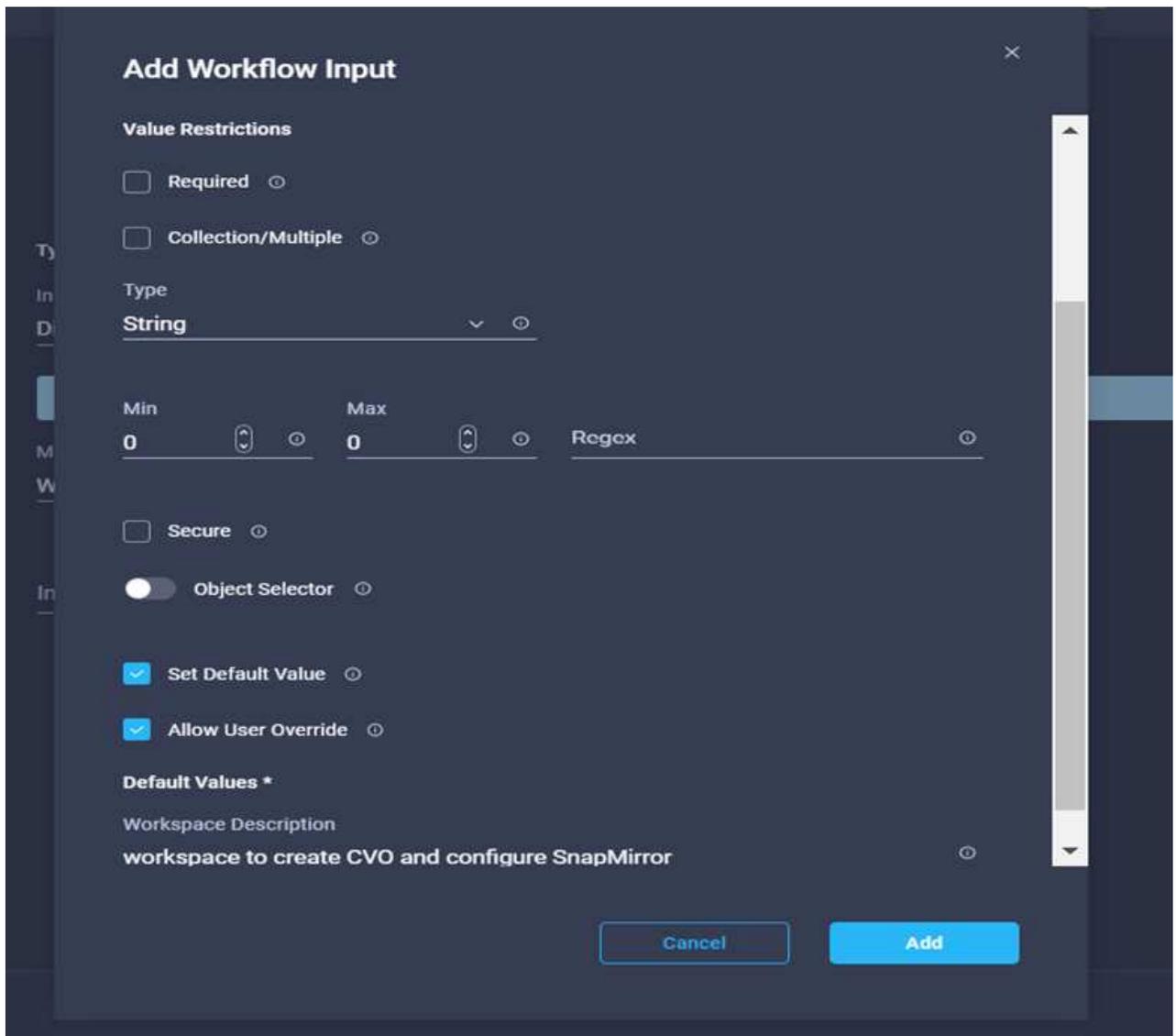
Object Selector ⓘ

Set Default Value ⓘ

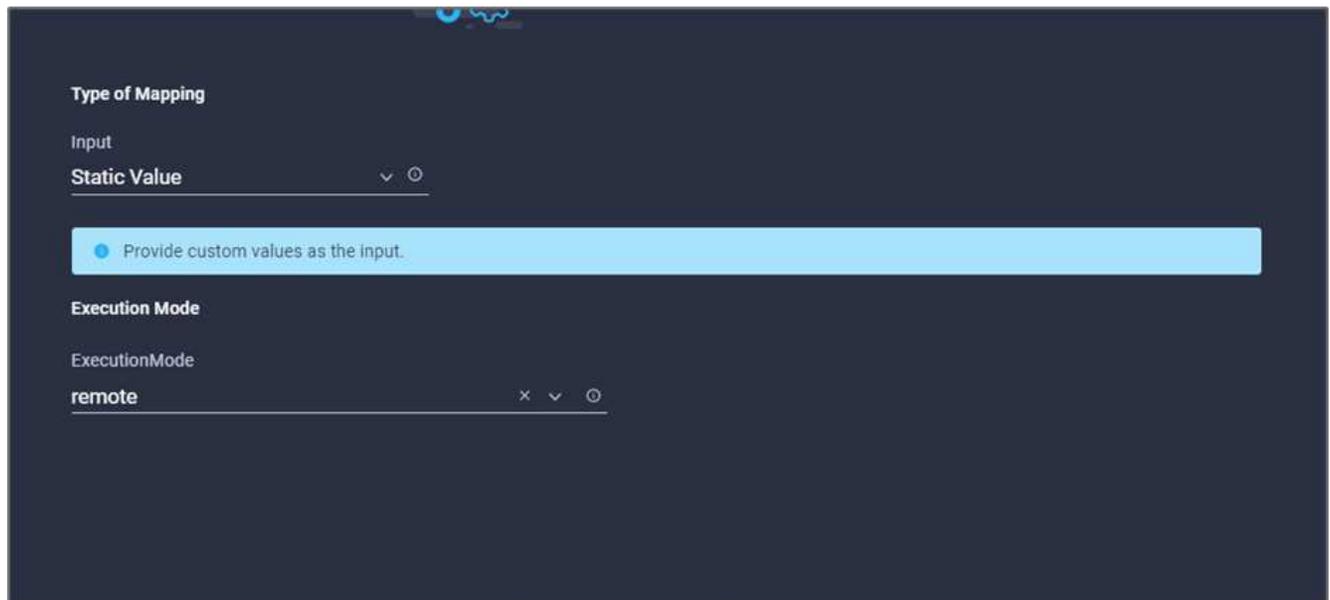
Allow User Override ⓘ

Cancel Add

20. Dans l'assistant Ajouter une entrée, procédez comme suit :
- Indiquez un nom d'affichage et un nom de référence (facultatif).
 - Assurez-vous de sélectionner **String** pour **Type**.
 - Cliquez sur **définir la valeur par défaut et remplacer**.
 - Fournissez une description de l'espace de travail et cliquez sur **Ajouter**.



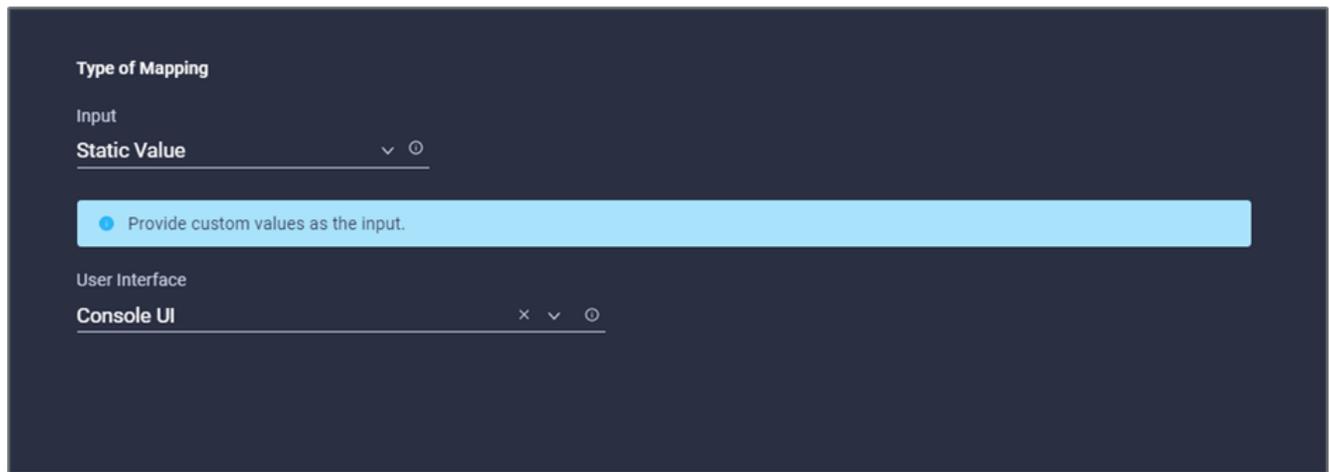
21. Cliquez sur **carte**.
22. Cliquez sur **Map** dans le champ **Execution mode**.
23. Choisissez **valeur statique**, cliquez sur **mode d'exécution**, puis sur **remote**.



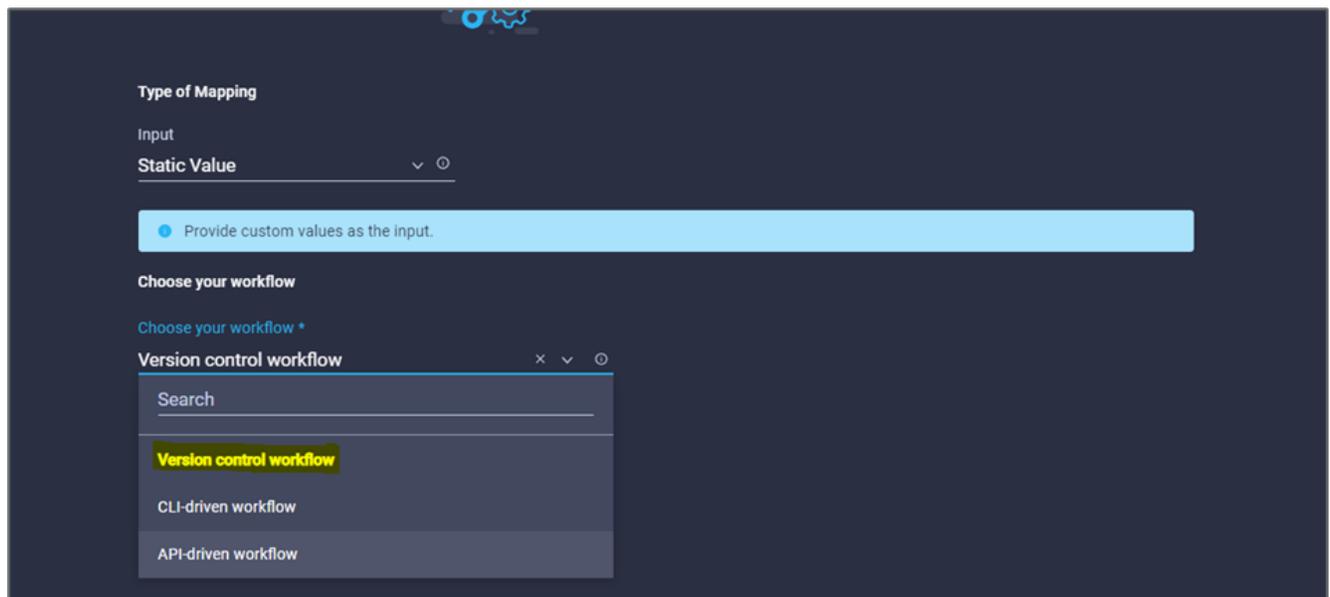
24. Cliquez sur **carte**.
25. Cliquez sur **carte** dans le champ **appliquer méthode**.
26. Choisissez **valeur statique** et cliquez sur **appliquer méthode**. Cliquez sur **application manuelle**.



27. Cliquez sur **carte**.
28. Cliquez sur **Map** dans le champ **User interface**.
29. Choisissez **valeur statique** et cliquez sur **interface utilisateur**. Cliquez sur **interface utilisateur de la console**.



30. Cliquez sur **carte**.
31. Cliquez sur **Map** dans le champ de saisie et sélectionnez votre flux de travail.
32. Sélectionnez **valeur statique**, puis cliquez sur **Choisissez votre flux de travail**. Cliquez sur **version Control Workflow**.



33. Fournissez les informations suivantes sur le référentiel GitHub :
 - a. Dans **Nom du référentiel**, entrez le nom du référentiel détaillé dans la section "[« Configurer les conditions préalables à l'environnement »](#)".
 - b. Indiquez l'ID de token OAuth comme détaillé dans la section "[« Configurer les conditions préalables à l'environnement »](#)".
 - c. Sélectionnez l'option **déclenchement automatique**.

Disaster Recovery Workflow > Edit > Add Terraform Workspace > Choose your workflow

Type of Mapping

Input
Static Value ⌵ ⊙

● Provide custom values as the input.

Choose your workflow

Choose your workflow *
Version control workflow ✕ ⌵ ⊙

Choose repository and configure settings

Repository Name *
NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-wit ⊙

Oauth Token ID *
 ⊙

Terraform Working Directory ⊙

Automatic Run Triggering

Automatic Run Triggering Options
Always Trigger Runs ✕ ⌵ ⊙

34. Cliquez sur **carte**.

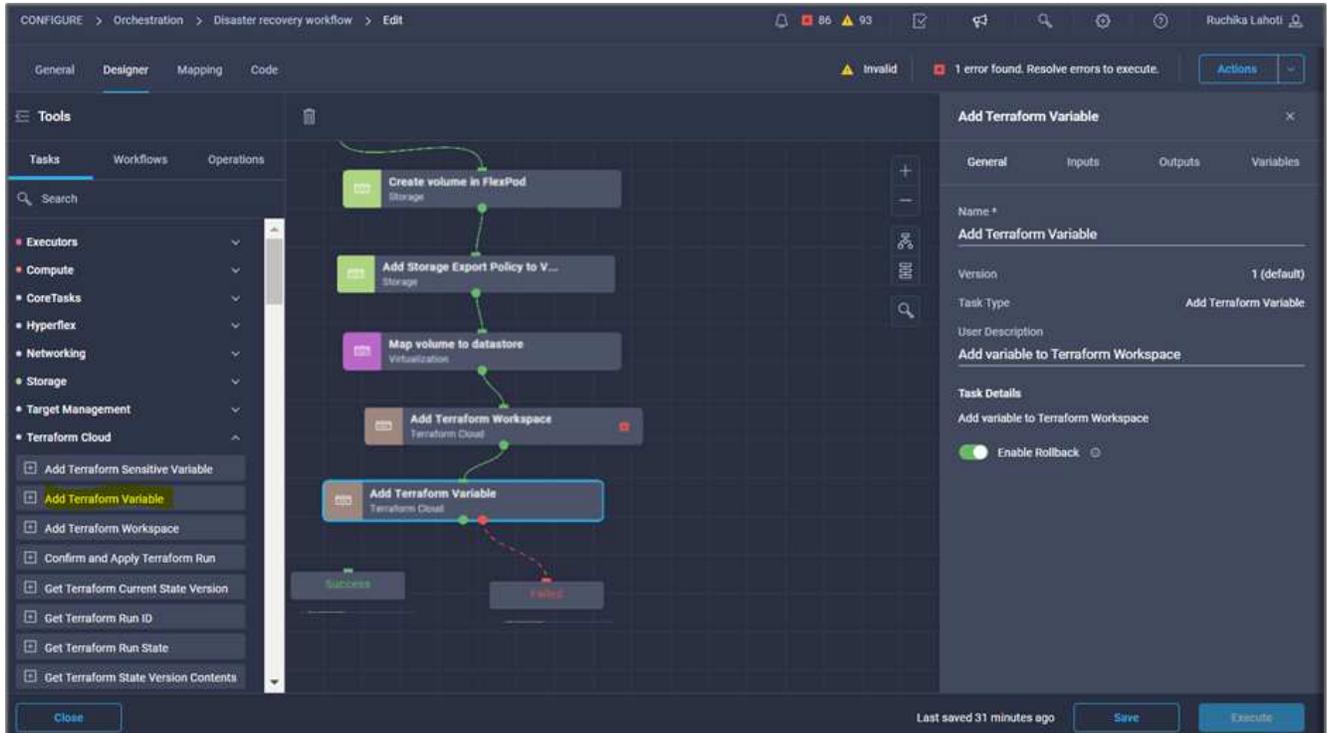
35. Cliquez sur **Enregistrer**.

Cela termine la création d'un espace de travail dans un compte Terraform Cloud for Business.

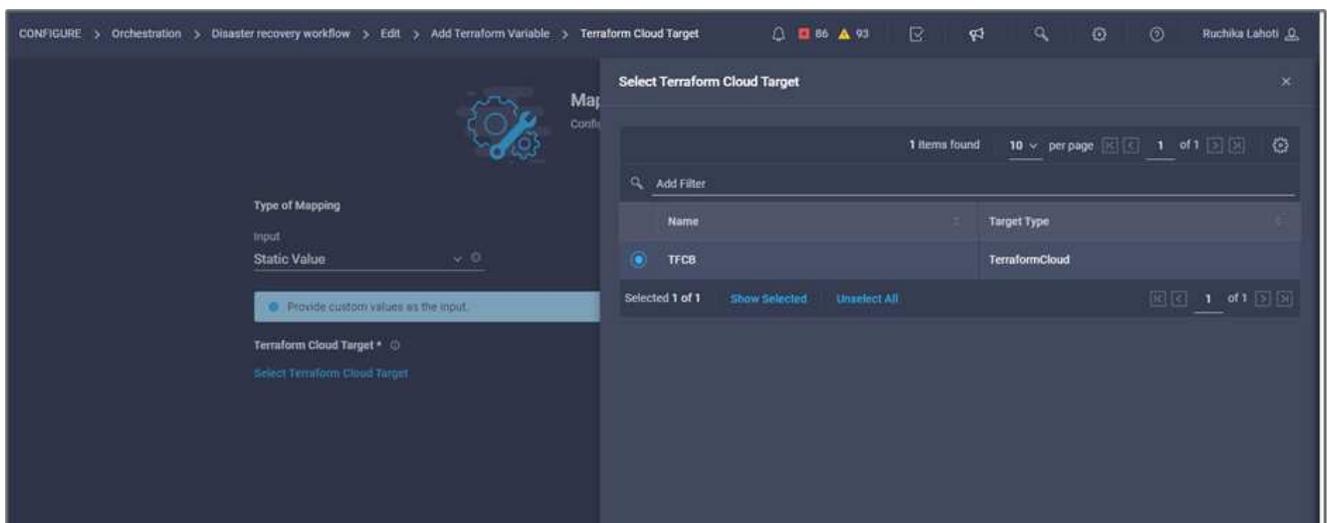
Procédure 6 : ajoutez des variables non sensibles à l'espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur la section **workflows à partir d'Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Add Terraform Workspace** et **Add Terraform variables**. Cliquez sur **Enregistrer**.

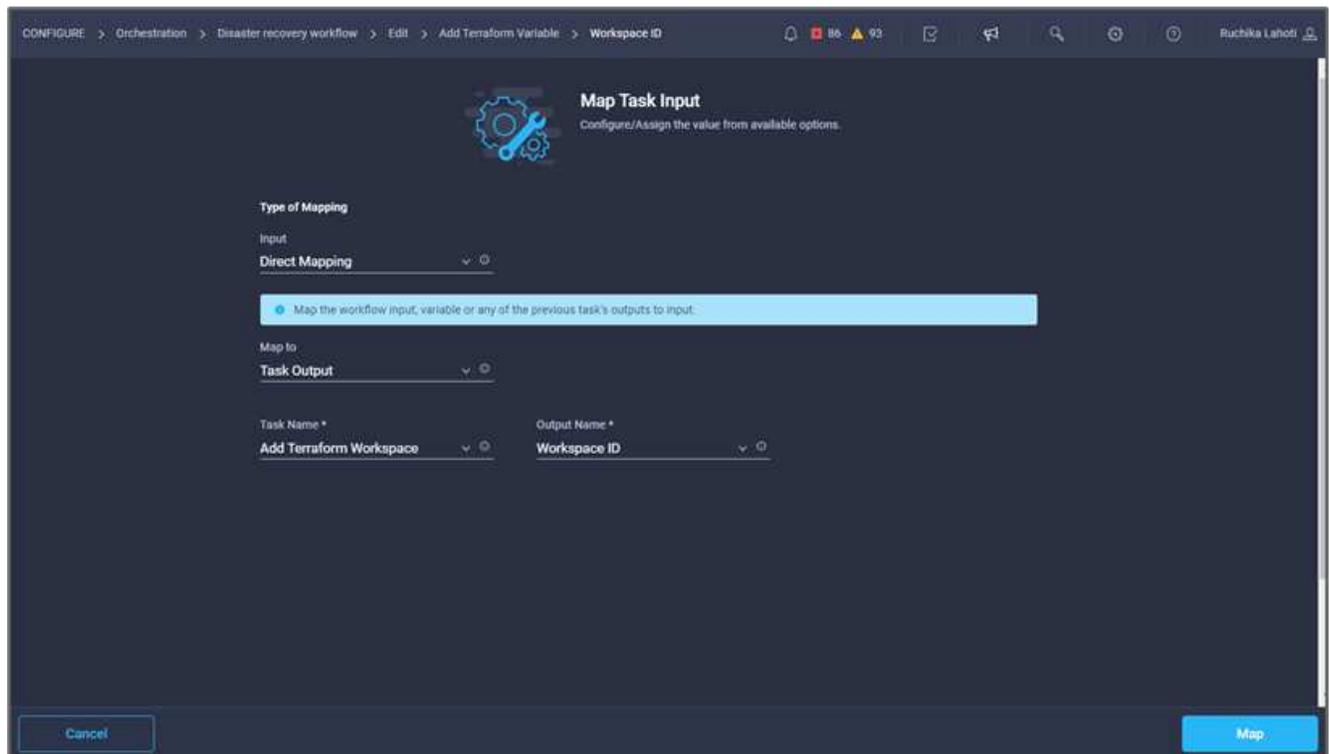
4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



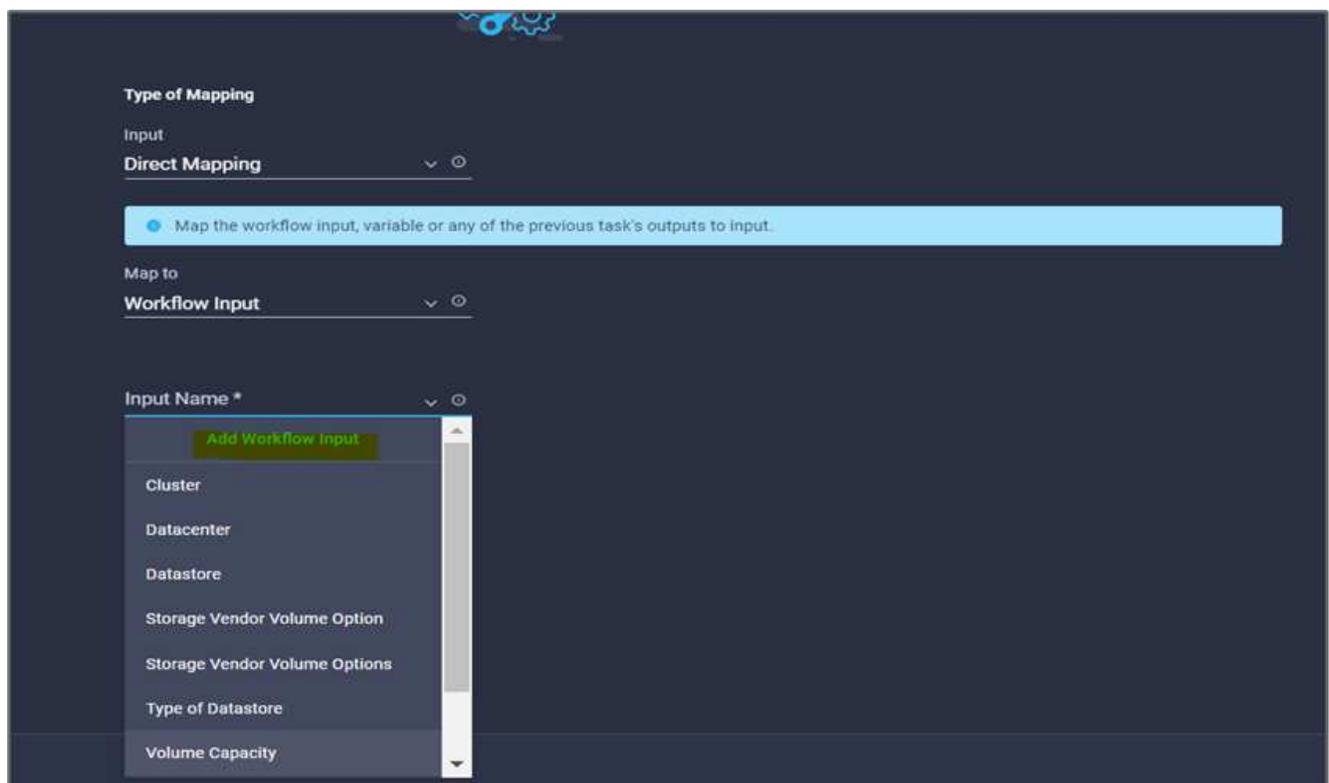
5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté comme expliqué dans "[Configurez Cisco Intersight Service pour HashiCorp Terraform](#)". ».



8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ ***Nom de l'organisation Terraform ***.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.



11. Cliquez sur **carte**.
12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche** et cliquez sur **Ajouter un espace de travail Terraform**.



15. Cliquez sur **Nom de sortie** et cliquez sur **Nom d'espace de travail**.

16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct** et cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.

Add Workflow Input

Display Name *
Terraform Variable

Reference Name *
TerraformAddVariable

Description
Terraform Variable to be added

Value Restrictions

Required

Collection/Multiple

Type
String

Min 0 Max 0 Regex

Secure

Object Selector

Cancel Add

20. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Assurez-vous de sélectionner **String** pour **Type**.
 - c. Cliquez sur **définir la valeur par défaut et remplacer**.
 - d. Cliquez sur **Type de variable**, puis sur **variables non sensibles**.

21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :

- **Clé.** name_of_on-prem-ontap
- **Valeur.** indiquer le nom de ONTAP sur site.
- **Description.** Nom du ONTAP sur place.

22. Cliquez sur + pour ajouter d'autres variables.

Set Default Value ⓘ

Allow User Override ⓘ

Default Values *

Terraform Variable

Key *

name_of_on-prem-ontap ⓘ

Value

Provide the name of On-premise ONTAP added in section Deploying ⓘ

Description

Name of the On-premise ONTAP ⓘ

HCL ⓘ

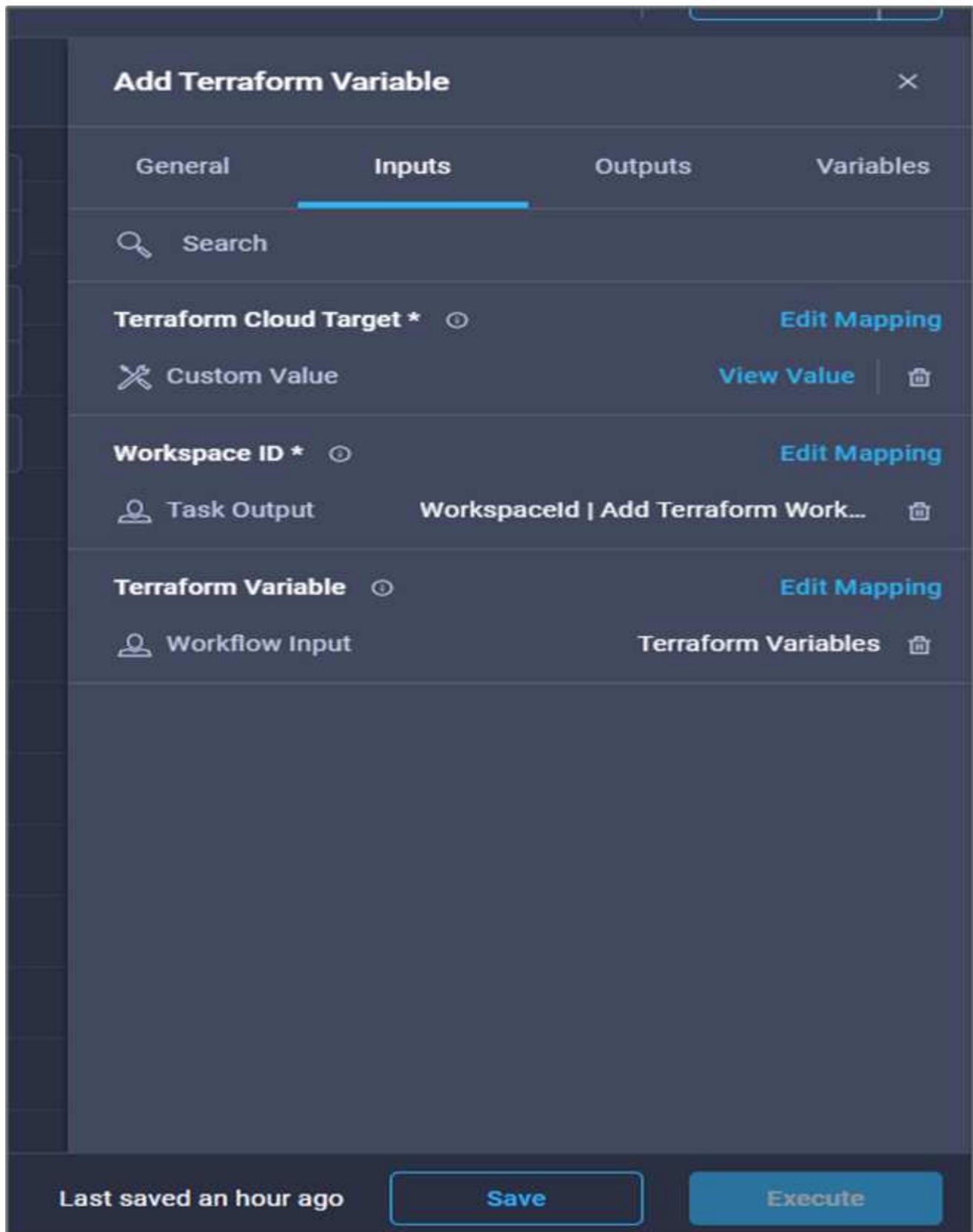
Cancel Add

23. Ajoutez toutes les variables Terraform comme indiqué dans le tableau suivant. Vous pouvez également fournir une valeur par défaut.

Nom de la variable Terraform	Description
nom_of_on-ontap sur site	Nom du ONTAP sur site (FlexPod)

Nom de la variable Terraform	Description
ip_cluster_ontap_sur site	L'adresse IP de l'interface de gestion du cluster de stockage
nom_utilisateur_ontap_sur site	Nom d'utilisateur admin pour le cluster de stockage
Zone	Région GCP dans laquelle l'environnement de travail sera créé
id_sous-réseau	ID de sous-réseau GCP dans lequel l'environnement de travail sera créé
id_vpc	ID VPC dans lequel l'environnement de travail sera créé
capacity_package_name	Type de licence à utiliser
volume_source	Nom du volume source
nom_vm_stockage_source	Nom du SVM source
volume_destination	Nom du volume sur Cloud Volumes ONTAP
schedule_of_replication	La valeur par défaut est 1 heure
nom_du_volume_to_create_on_cvo	Nom du volume cloud
id_espace_de_travail	Espace de travail_ID où l'environnement de travail sera créé
ID_projet	ID_projet où l'environnement de travail sera créé
nom_du_cluster_cvo	Nom de l'environnement de travail Cloud Volumes ONTAP
compte_service_gcp	gcp_service_compte de l'environnement de travail Cloud Volumes ONTAP

24. Cliquez sur **carte**, puis sur **Enregistrer**.



La tâche d'ajout des variables Terraform requises à l'espace de travail est alors terminée. Ajoutez ensuite les variables Terraform sensibles requises à l'espace de travail. Vous pouvez également les combiner en une seule tâche.

Procédure 7 : ajoutez des variables sensibles à un espace de travail

1. Accédez à l'onglet **Designer** et cliquez sur **workflows** dans la section **Outils**.
2. Faites glisser et déposez le flux de travail **Terraform > Ajouter des variables Terraform** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les deux tâches **Ajouter un espace de travail Terraform**. Cliquez sur **Enregistrer**.



Un avertissement s'affiche pour indiquer que les deux tâches ont le même nom. Ignorez l'erreur pour l'instant car vous modifiez le nom de la tâche à l'étape suivante.

4. Cliquez sur **Ajouter variables Terraform**. Dans la zone **Propriétés du flux de travail**, cliquez sur l'onglet **général**. Modifiez le nom en **Ajouter des variables sensibles Terraform**.

The screenshot shows the Terraform Cloud Designer interface. The workflow consists of several tasks: 'Create volume in FilePod', 'Add Storage Export Policy to V...', 'Map volume to datastore', 'Add Terraform Workspace', 'Add Terraform Variable', and 'Add Terraform sensitive Variable'. The 'Add Terraform sensitive Variable' task is highlighted with a red dashed box. The configuration panel on the right shows the 'Inputs' tab for this task, with fields for 'Terraform Cloud Target', 'Workspace ID', and 'Terraform Variable', all of which are currently set to 'VALUE NOT SPECIFIED'.

5. Dans la zone **Propriétés du workflow**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section "[Configurez Cisco Intersight Service pour HashiCorp Terraform](#)". »
8. Cliquez sur **carte**.
9. Cliquez sur **carte** dans le champ **Nom de l'organisation Terraform**.
10. Choisissez **valeur statique** et cliquez sur **Sélectionner l'organisation Terraform**. Sélectionnez le nom de l'organisation Terraform dont vous faites partie dans votre compte Terraform Cloud for Business.
11. Cliquez sur **carte**.

12. Cliquez sur **carte** dans le champ **Nom de l'espace de travail Terraform**.
13. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
14. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.
15. Cliquez sur **Nom de sortie** et cliquez sur sortie **Nom d'espace de travail**.
16. Cliquez sur **carte**.
17. Cliquez sur **Map** dans le champ **Add variables Options**.
18. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
19. Cliquez sur **Nom d'entrée** et **Créer une entrée de flux de travail**.
20. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Assurez-vous de sélectionner **Terraform Ajouter des variables Options** pour le type.
 - c. Cliquez sur **définir la valeur par défaut**.
 - d. Cliquez sur **Type de variable**, puis sur **variables sensibles**.
 - e. Cliquez sur **Ajouter**.

Add Workflow Input

Display Name *
terraform sensitive variable

Reference Name *
terraformsensitivevariable

Description
Add Variables

Value Restrictions

Required

Collection/Multiple

Type
Terraform Add Variables Option

Set Default Value

Allow User Override

Default Values *
terraform sensitive variable

Variable Type *
Sensitive Variables

Cancel Add

21. Dans la section **Ajouter des variables Terraform**, fournissez les informations suivantes :

- **Clé.** `cloudmanager_refresh_token`.
- **Valeur.** saisissez le jeton d'actualisation pour les opérations de l'API NetApp Cloud Manager.
- **Description.** Actualiser jeton.



Pour en savoir plus sur l'obtention d'un jeton de mise à jour pour les opérations de l'API NetApp Cloud Manager, consultez la section "[« Configurer les conditions préalables à l'environnement ».](#)"

Add Workflow Input

Set Default Value ⓘ

Allow User Override ⓘ

Default Values *

terraform sensitive variable

Variable Type *

Sensitive Variables ⓘ

Add Sensitive Terraform Variables

Key *	<input type="text" value="cloudmanager_refresh_token"/>	ⓘ
Value	<input type="text"/>	👁 ⓘ
Description	<input type="text" value="cloudmanager refresh token"/>	ⓘ
<input type="checkbox"/> HCL ⓘ		

+

Cancel Add

22. Ajoutez toutes les variables sensibles à la Terraform comme indiqué dans le tableau ci-dessous. Vous pouvez également fournir une valeur par défaut.

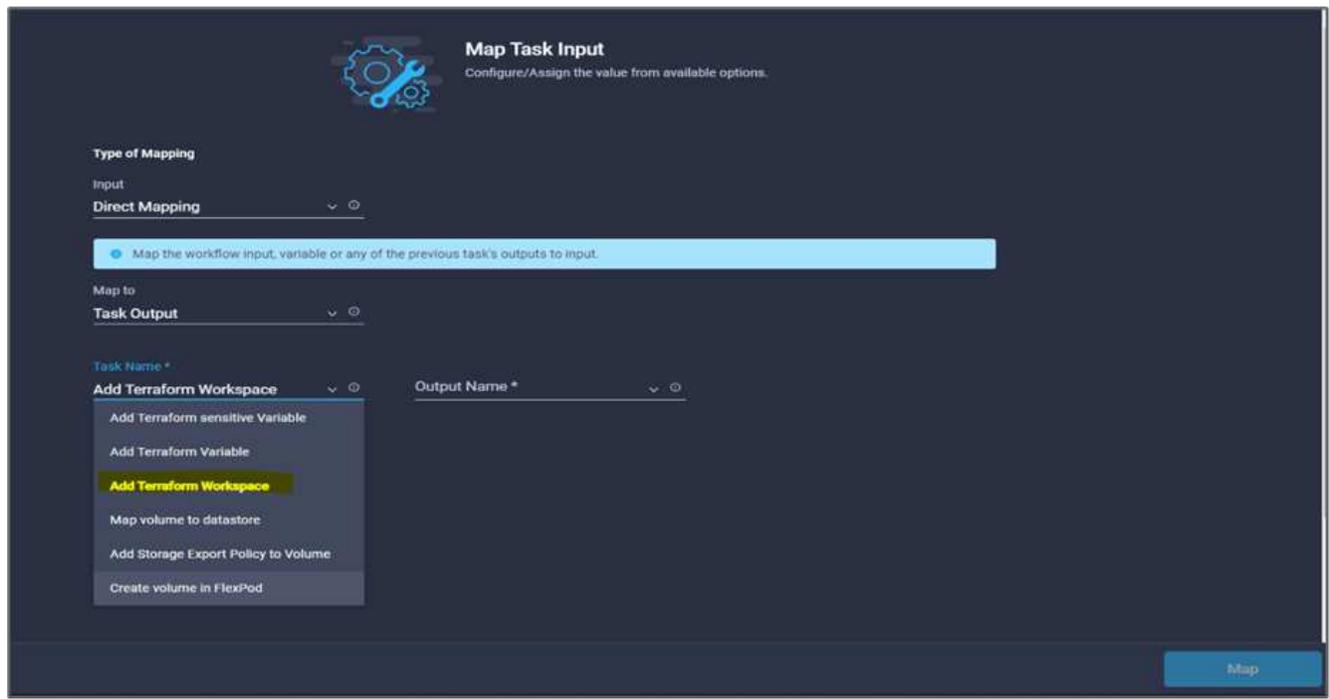
Nom de variable sensible Terraform	Description
cloudmanager_refresh_token	Actualiser le jeton. Vous pouvez l'obtenir auprès de :
id_connecteur	L'ID client du connecteur Cloud Manager. Obtenez-le à partir de
cvo_admin_password	Mot de passe d'administration pour Cloud Volumes ONTAP
mot_de_passe_utilisateur_ontap_sur site	Mot de passe d'administration pour le cluster de stockage

23. Cliquez sur **Map**.cette opération permet d'ajouter les variables sensibles Terraform requises à l'espace de travail. Ensuite, démarrez un nouveau plan Terraform dans l'espace de travail configuré.

Procédure 8 : démarrez un nouveau plan Terraform

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > Start New Terraform Plan** de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour vous connecter entre les tâches **Ajouter des variables sensibles Terraform** et **Démarrer de nouvelles tâches Terraform Plan**. Cliquez sur **Enregistrer**.
4. Cliquez sur **Démarrer Nouveau plan Terraform**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.

5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans la section « Configuration de Cisco InterSight Service for HashiCorp Terraform ».
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Workspace ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche**, puis sur **Ajouter un espace de travail Terraform**.



12. Cliquez sur **Nom de sortie, ID d'espace de travail**, puis sur **carte**.
13. Cliquez sur **carte** dans le champ **motif de démarrage du plan**.
14. Choisissez **mappage direct**, puis cliquez sur **entrée de flux de travail**.
15. Cliquez sur **Nom d'entrée**, puis sur **Créer entrée de flux de travail**.
16. Dans l'assistant Ajouter une entrée, procédez comme suit :
 - a. Indiquez un nom d'affichage et un nom de référence (facultatif).
 - b. Assurez-vous de sélectionner **String** pour **Type**.
 - c. Cliquez sur **définir la valeur par défaut et remplacer**.
 - d. Entrez une valeur par défaut pour **Reason for Starting plan** et cliquez sur **Add**.

Add Workflow Input

Required

Collection/Multiple

Type
String

Min **0** Max **0** Regex

Secure

Object Selector

Set Default Value

Allow User Override

Default Values *

Reason for starting plan *

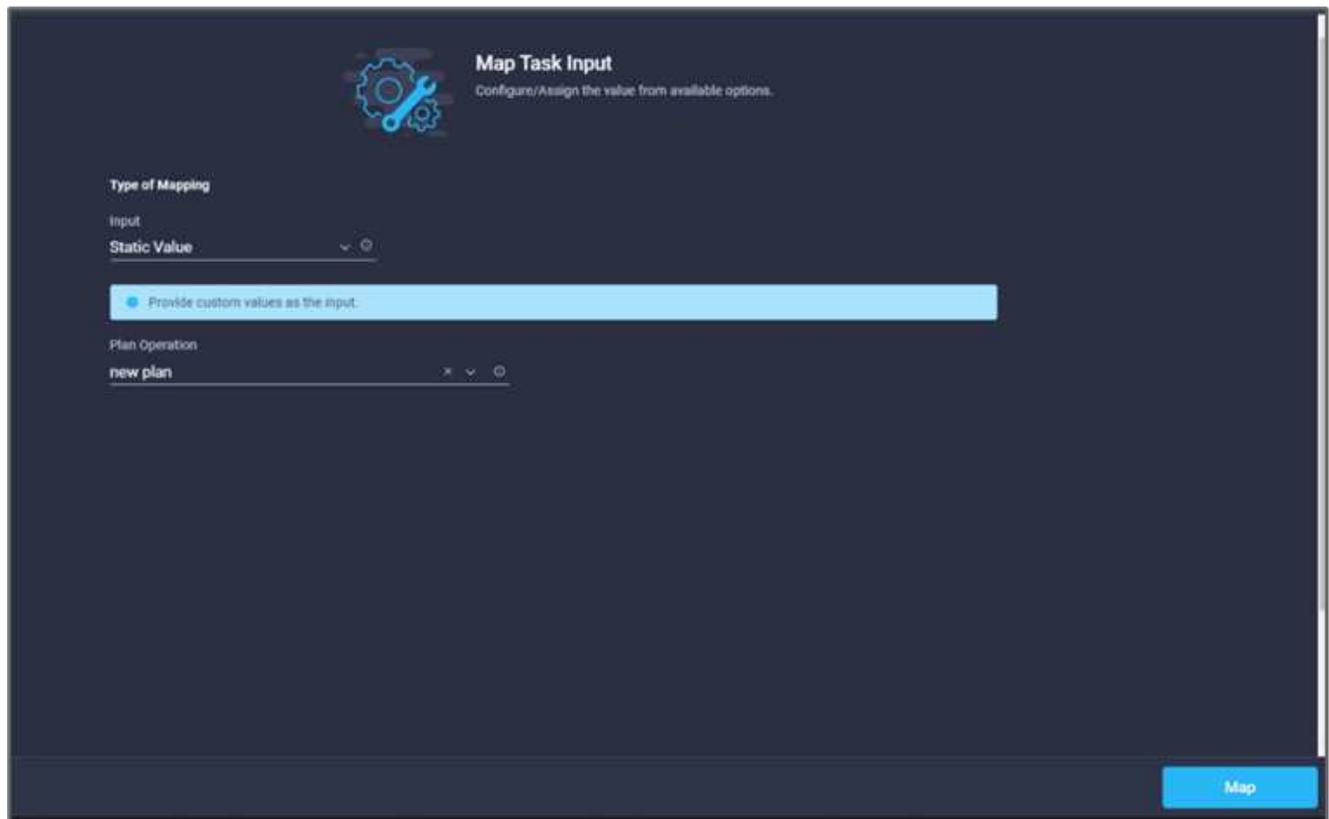
terraform plan for replication between onprem volume and CVO

Cancel Add

17. Cliquez sur **carte**.

18. Cliquez sur **Map** dans le champ **Plan Operation**.

19. Choisissez **valeur statique** et cliquez sur **opération de plan**. Cliquez sur **New plan**.



20. Cliquez sur **carte**.

21. Cliquez sur **Enregistrer**.

Cela complète la tâche d'ajout d'un plan Terraform dans le compte Terraform Cloud for Business. Ensuite, créez une tâche de veille pendant quelques secondes.

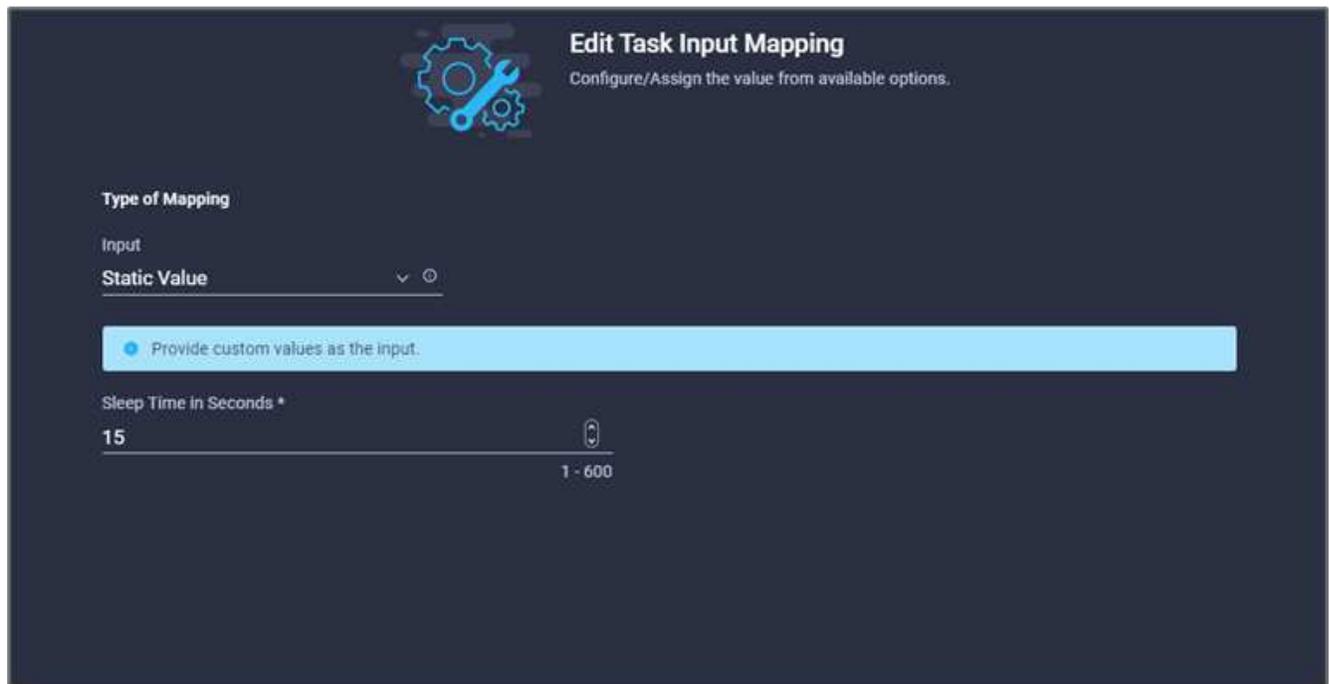
Procédure 9 : tâche de veille pour la synchronisation

Terraform Apply nécessite un runId, qui est généré dans le cadre de la tâche Plan Terraform. L'attente de quelques secondes entre le Plan Terraform et les actions d'application Terraform évite les problèmes de synchronisation.

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Core Tasks > Sleep Task** dans la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Démarrer Nouveau plan Terraform** et **tâche veille**. Cliquez sur **Enregistrer**.

The screenshot displays a workflow editor interface. At the top, there are status indicators: a yellow triangle for 'Invalid' and a red square for '1 error found. Resolve errors to execute.' A 'Actions' dropdown menu is visible in the top right. The workflow consists of several tasks connected by arrows: 'Start', 'Create volume in FlexPod' (Storage), 'Add Storage Export Policy to V...' (Storage), 'Map volume to datastore' (Virtualization), 'Add Terraform Workspace' (Terraform Cloud), 'Add Terraform Variable' (Terraform Cloud), 'Add Terraform sensitive Variable' (Terraform Cloud), 'Start New Terraform Plan' (Terraform Cloud), 'Sleep Task' (CoreTasks), 'Success', and 'Failed'. A 'Sleep Task' configuration panel is open on the right, showing the 'General' tab. The panel includes fields for 'Name *' (Sleep Task), 'Version' (1 (default)), 'Task Type' (Sleep Task), and 'User Description' (Pauses the current workflow for the specified duration.). Below these are 'Task Details' (Pauses the current workflow for the specified duration.). At the bottom right, there are 'Save' and 'Execute' buttons, and a timestamp 'Last saved 2 minutes ago'.

4. Cliquez sur **tâche veille**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche. Dans cet exemple, le nom de la tâche est **Synchroniser**.
5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **temps de veille en secondes**.
7. Choisissez **valeur statique** et saisissez **15** dans pour le **temps de veille en secondes**.

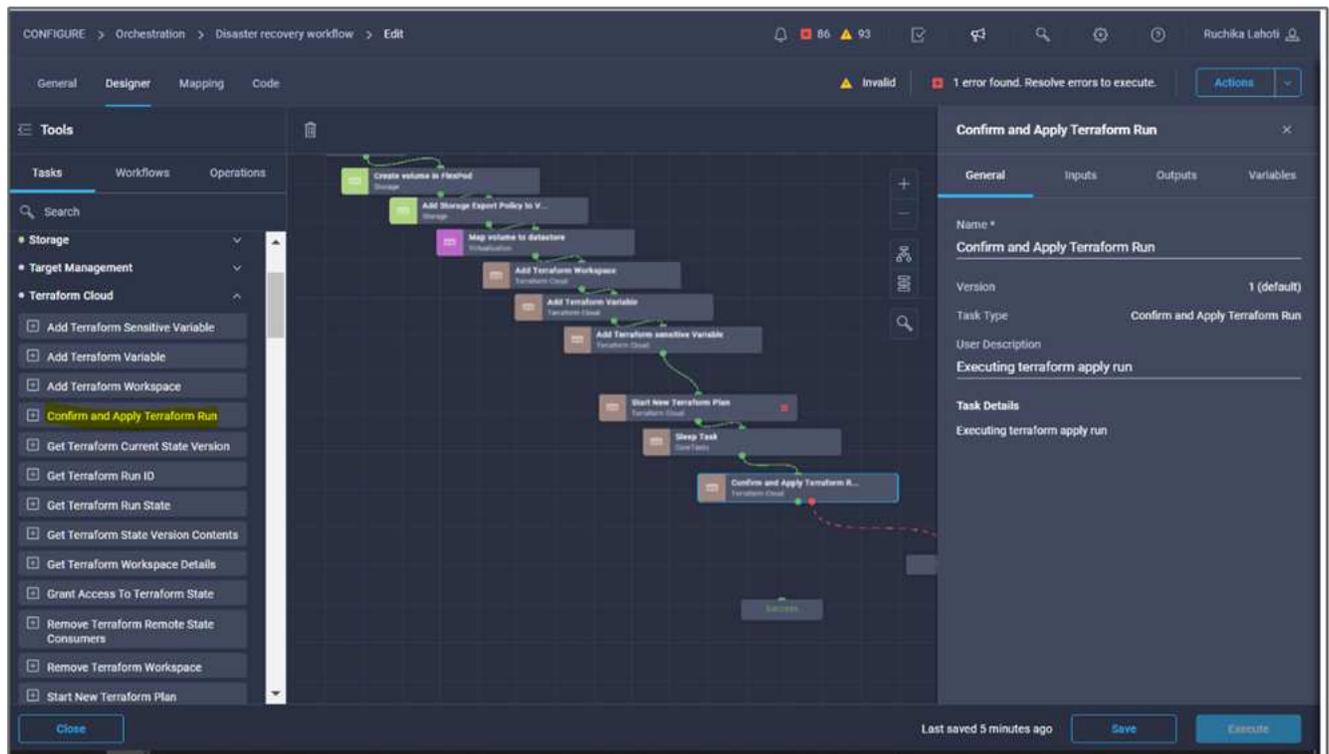


8. Cliquez sur **carte**.
9. Cliquez sur **Enregistrer**.

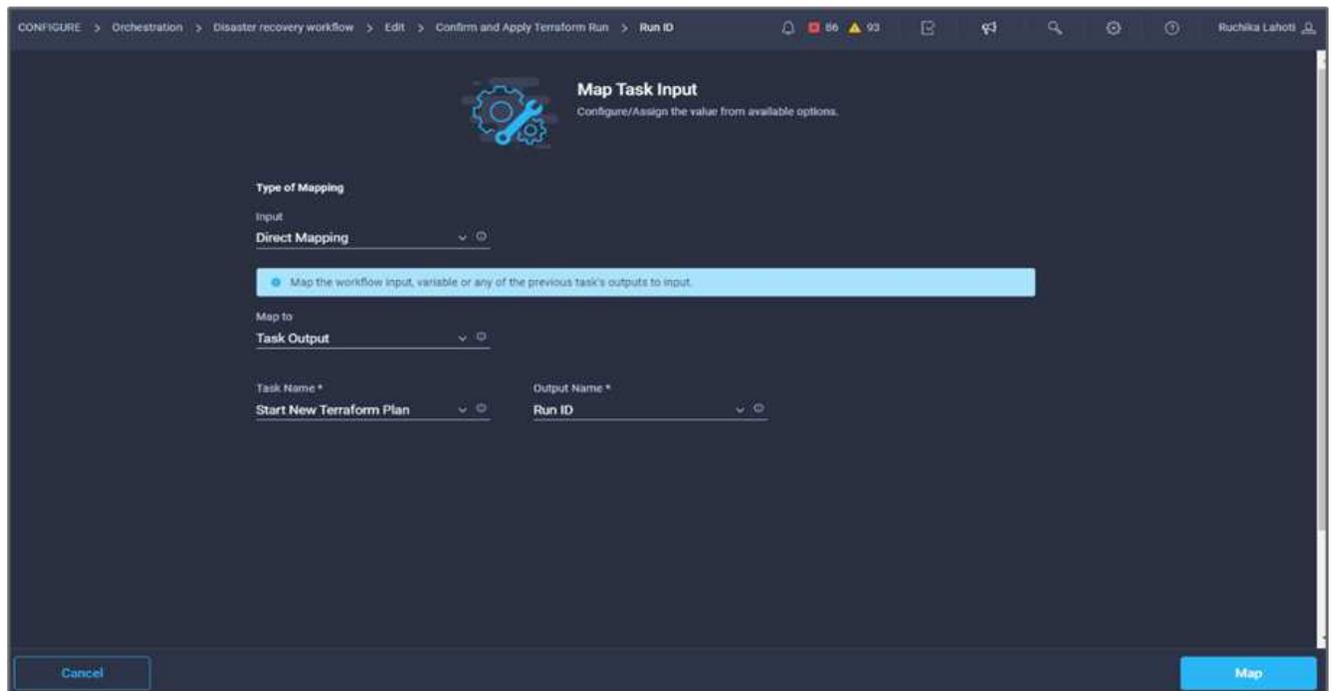
La tâche de veille est terminée. Ensuite, créez la dernière tâche de ce flux de travail, en confirmant et en appliquant l'exécution Terraform.

Procédure 10 : confirmer et appliquer Terraform Run

1. Accédez à l'onglet **Designer** et cliquez sur **tâches** dans la section **Outils**.
2. Faites glisser et déposez la tâche **Terraform Cloud > confirmer et appliquer Terraform Run** à partir de la section **Tools** de la zone **Design**.
3. Utilisez Connector pour connecter les tâches **Synchroniser** et **confirmer et appliquer Terraform Run**. Cliquez sur **Enregistrer**.
4. Cliquez sur **confirmer et appliquer Terraform Run**. Dans la zone **Propriétés de tâche**, cliquez sur l'onglet **général**. Vous pouvez également modifier le nom et la description de cette tâche.



5. Dans la zone **Propriétés de tâche**, cliquez sur **entrées**.
6. Cliquez sur **carte** dans le champ **Terraform Cloud Target**.
7. Choisissez **valeur statique** et cliquez sur **Sélectionner la cible de nuage Terraform**. Sélectionnez le compte Terraform Cloud for Business ajouté dans "[Configurez Cisco Intersight Service pour HashiCorp Terraform](#)". »
8. Cliquez sur **carte**.
9. Cliquez sur **Map** dans le champ **Run ID**.
10. Choisissez **mappage direct** et cliquez sur **sortie tâche**.
11. Cliquez sur **Nom de la tâche** et cliquez sur **Démarrer Nouveau plan Terraform**.
12. Cliquez sur **Nom de sortie**, puis sur **ID d'exécution**.



13. Cliquez sur **carte**.
14. Cliquez sur **Enregistrer**.
15. Cliquez sur **alignement automatique du flux de travail** pour que toutes les tâches soient alignées.
Cliquez sur **Enregistrer**.



La tâche confirmer et appliquer Terraform Run est terminée. Utilisez Connector pour vous connecter entre la tâche **confirmer et appliquer Terraform Run** et les tâches **Success** et **failed**.

Procédure 11 : importation d'un flux de travail conçu par Cisco

Cisco Intersight Cloud Orchestrator vous permet d'exporter des workflows d'un compte Cisco Intersight vers votre système, puis de les importer dans un autre compte. Un fichier JSON a été créé en exportant le flux de travail créé qui peut être importé vers votre compte.

Un fichier JSON pour le composant de flux de travail est disponible dans "[Référentiel GitHub](#)".

"Next : exécution Terraform à partir du contrôleur."

Exécution Terraform à partir du contrôleur

"Précédent : flux de travail de reprise après incident."

Nous pouvons exécuter le plan Terraform à l'aide d'un contrôleur. Vous pouvez ignorer cette section si vous avez déjà exécuté votre plan Terraform à l'aide d'un flux de travail ICO.

Prérequis

La configuration de la solution commence par une station de travail de gestion qui a accès à Internet et avec une installation de Terraform.

Vous trouverez un guide d'installation de Terraform ["ici"](#).

Cloner GitHub

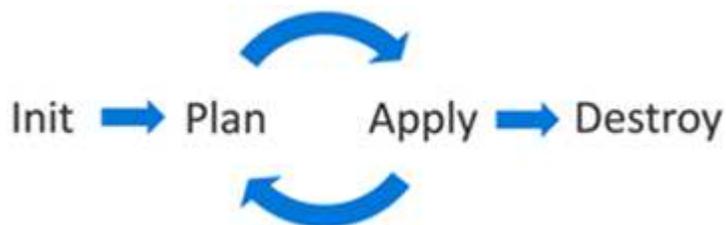
La première étape du processus consiste à cloner le GitHub repo vers un nouveau dossier vide sur la station de travail de gestion. Pour cloner le référentiel GitHub, procédez comme suit :

1. À partir du poste de travail de gestion, créez un nouveau dossier pour le projet. Créez un nouveau dossier dans ce dossier nommé `/root/snapmirror-cvo` Et clonez le référentiel GitHub.
2. Ouvrez une interface de ligne de commande ou de console sur le poste de travail de gestion et modifiez les répertoires dans le nouveau dossier que vous venez de créer.
3. Clonez la collection GitHub à l'aide de la commande suivante :

```
Git clone https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO
```

1. Remplacez les répertoires par le nouveau dossier nommé `snapmirror-cvo`.

Exécution Terraform



- **Init.** initialiser l'environnement Terraform (local). Généralement exécuté une seule fois par session.
- **Plan.** Comparez l'état du terraform avec l'état d'entrée dans le nuage et construisez et affichez un plan d'exécution. Cela ne modifie pas le déploiement (lecture seule).
- **Appliquer.** appliquer le plan à partir de la phase du plan. Cela peut potentiellement changer le déploiement (lecture et écriture).
- **Détruire.** toutes les ressources qui sont régies par cet environnement terraform spécifique.

Pour plus de détails, voir ["ici"](#).

["Ensuite, validation de la solution."](#)

Validation des solutions

["Précédent : exécution Terraform à partir du contrôleur."](#)

Dans cette section, nous revisitons la solution avec un exemple de workflow de réplication des données et prenons quelques mesures pour vérifier l'intégrité de la réplication des données depuis l'instance NetApp ONTAP exécutée dans FlexPod vers NetApp Cloud Volumes ONTAP s'exécutant sur Google Cloud.

Nous avons utilisé Cisco Intersight workflow orchestrator dans cette solution et nous continuerons à l'utiliser pour notre cas d'utilisation.

De fait, le nombre limité de flux de travail Cisco Intersight utilisés dans cette solution ne représente pas l'ensemble complet des flux de travail utilisés par Cisco Intersight. Vous pouvez créer des flux de travail personnalisés en fonction de vos exigences spécifiques et les avoir déclenchés à partir de Cisco Intersight.

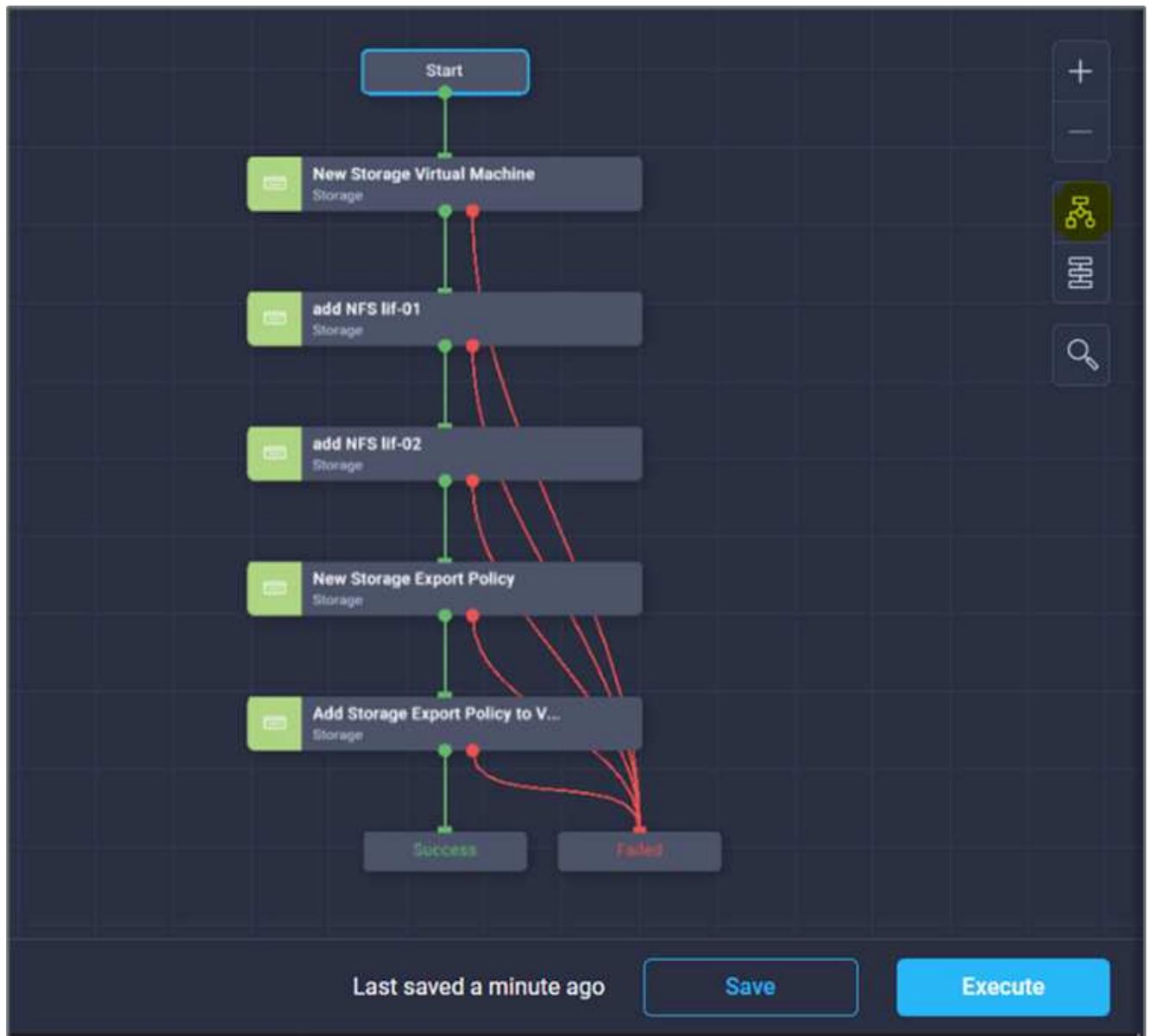
Pour valider un scénario de reprise sur incident réussi, commencez par déplacer les données d'un volume dans ONTAP qui fait partie de FlexPod vers Cloud Volumes ONTAP à l'aide de SnapMirror. Vous pouvez alors tenter d'accéder aux données à partir de l'instance de calcul cloud Google, suivie d'un contrôle de l'intégrité des données.

Les étapes générales suivantes permettent de vérifier les critères de réussite de cette solution :

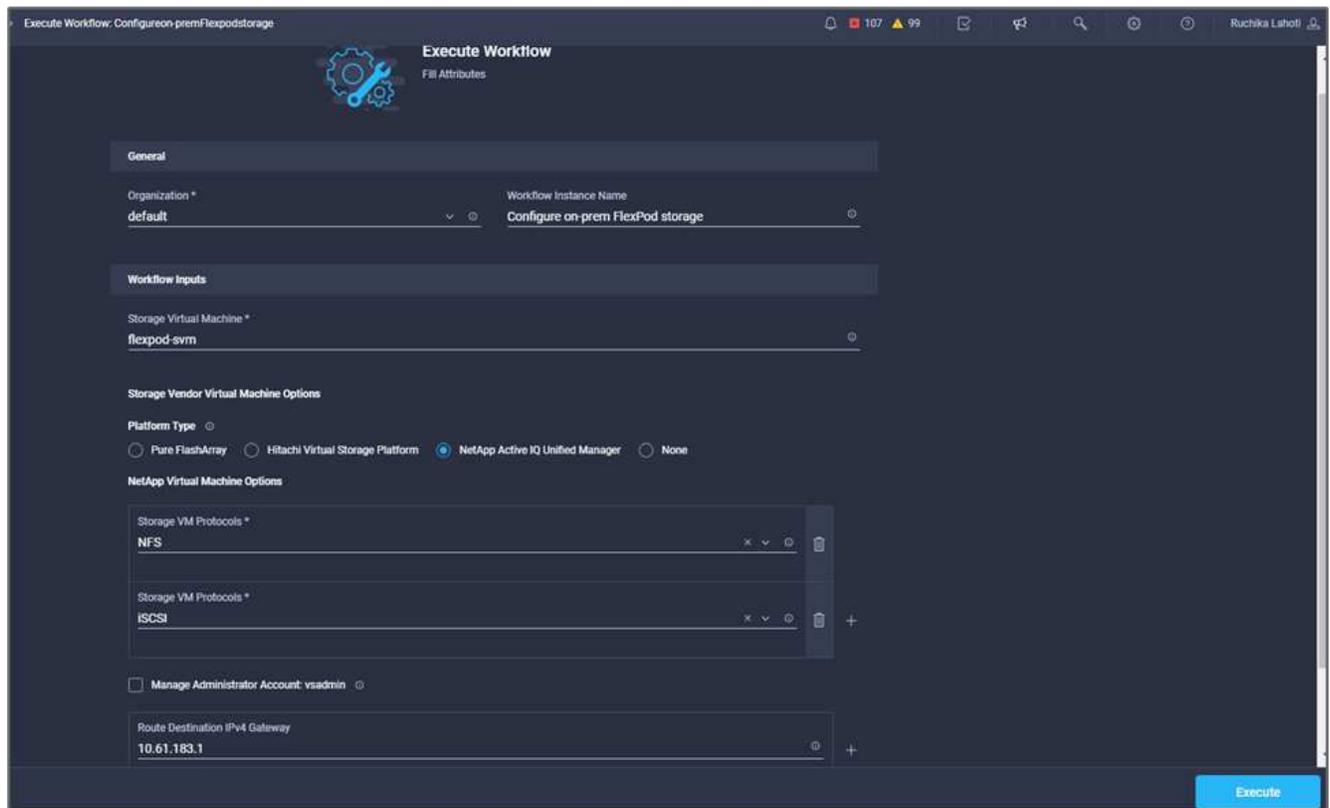
1. Générer un checksum SHA256 sur l'exemple de dataset présent dans un volume ONTAP dans FlexPod.
2. Configurez une relation SnapMirror volume entre ONTAP dans FlexPod et Cloud Volumes ONTAP.
3. Répliquer l'exemple de jeu de données de FlexPod vers Cloud Volumes ONTAP.
4. Interrompre la relation SnapMirror et promouvoir le volume en Cloud Volumes ONTAP vers la production.
5. Mappez le volume Cloud Volumes ONTAP avec le dataset sur une instance de calcul dans Google Cloud.
6. Générer un checksum SHA256 sur l'exemple de dataset dans Cloud Volumes ONTAP.
7. Comparez la somme de contrôle de la source et de la destination, probablement les sommes de contrôle des deux côtés correspondent.

Pour exécuter le workflow sur site, procédez comme suit :

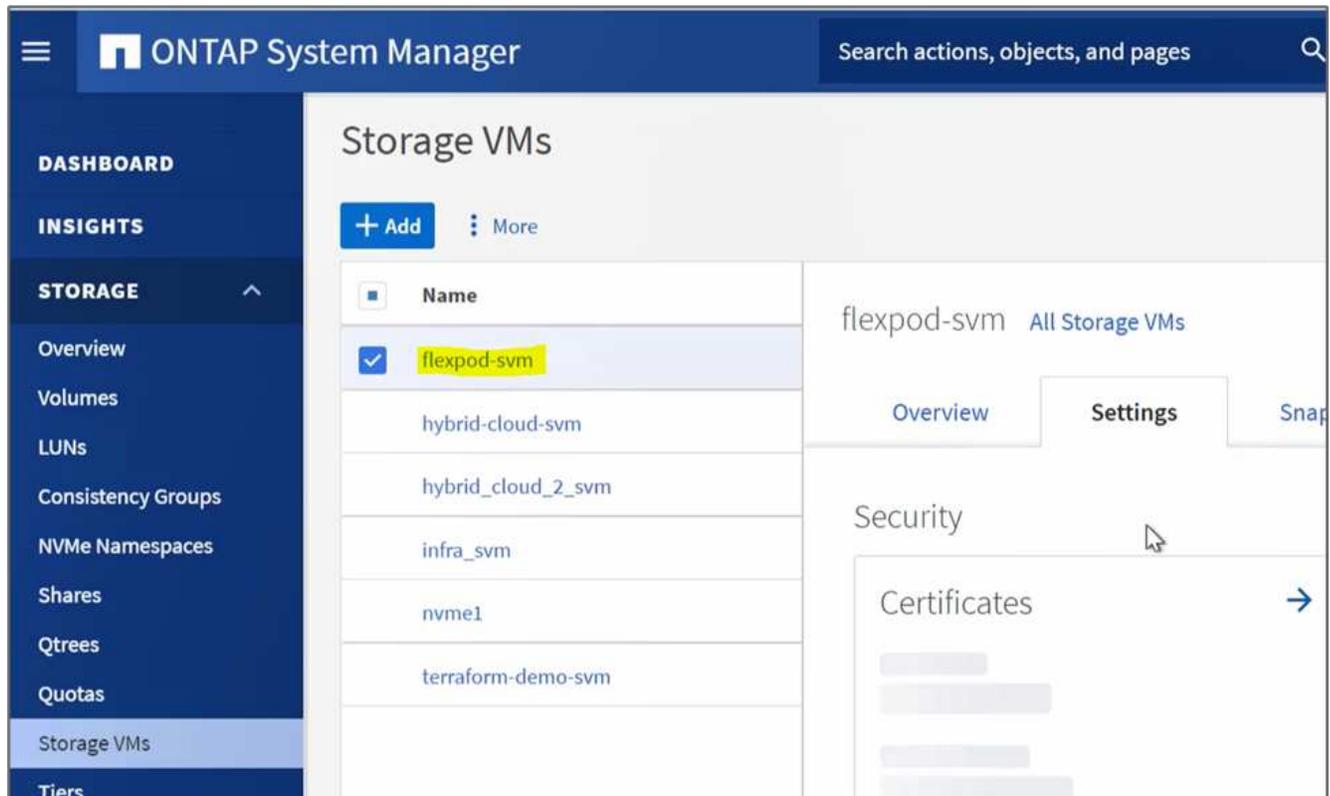
1. Créez un workflow dans InterSight pour les systèmes FlexPod sur site.



2. Fournissez les entrées requises et exécutez le flux de travail.



3. Vérifier le nouveau SVM créé dans System Manager



4. Créez et exécutez un autre workflow de reprise d'activité pour créer un volume dans FlexPod sur site et établir une relation SnapMirror entre ce volume dans FlexPod et Cloud Volumes ONTAP.



5. Vérifiez le nouveau volume créé dans ONTAP System Manager.

Name	Storage VM	Status	Capacity
application_copy	hybrid-cloud-svm	Online	3.12 MiB used / 19 GiB available / 20 GiB
audit_log_vol	hybrid-cloud-svm	Online	32.7 MiB used / 200 GiB available / 200 GiB
hybrid_cloud_svm_root	hybrid-cloud-svm	Online	1.68 MiB used / 971 MiB available / 1 GiB
test	hybrid-cloud-svm	Online	648 KiB used / 972 MiB available / 1 GiB
Test_Vol1	hybrid-cloud-svm	Online	10.6 MiB used / 9.99 GiB available / 10 GiB

6. Montez le même volume NFS sur une machine virtuelle sur site, puis copiez l'exemple de dataset et exécutez le checksum.

```

root@hybridcloudbackup:/snapmirror_demo# mount -t nfs 172.22.4.157:/Test_Vol1 /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo# df -kh
Filesystem      Size  Used Avail Use% Mounted on
udev            1.9G   0 1.9G   0% /dev
tmpfs           394M  1.1M 393M   1% /run
/dev/sda2       16G   11G 4.2G  72% /
tmpfs           2.0G   0 2.0G   0% /dev/shm
tmpfs           5.0M   0 5.0M   0% /run/lock
tmpfs           2.0G   0 2.0G   0% /sys/fs/cgroup
/dev/loop1      55M   55M   0 100% /snap/core18/1705
/dev/loop2      69M   69M   0 100% /snap/lxd/14804
/dev/loop0      28M   28M   0 100% /snap/snapd/7264
172.22.4.157:/Test_Vol1 10G 512K 10G   1% /snapmirror_demo
root@hybridcloudbackup:/snapmirror_demo#

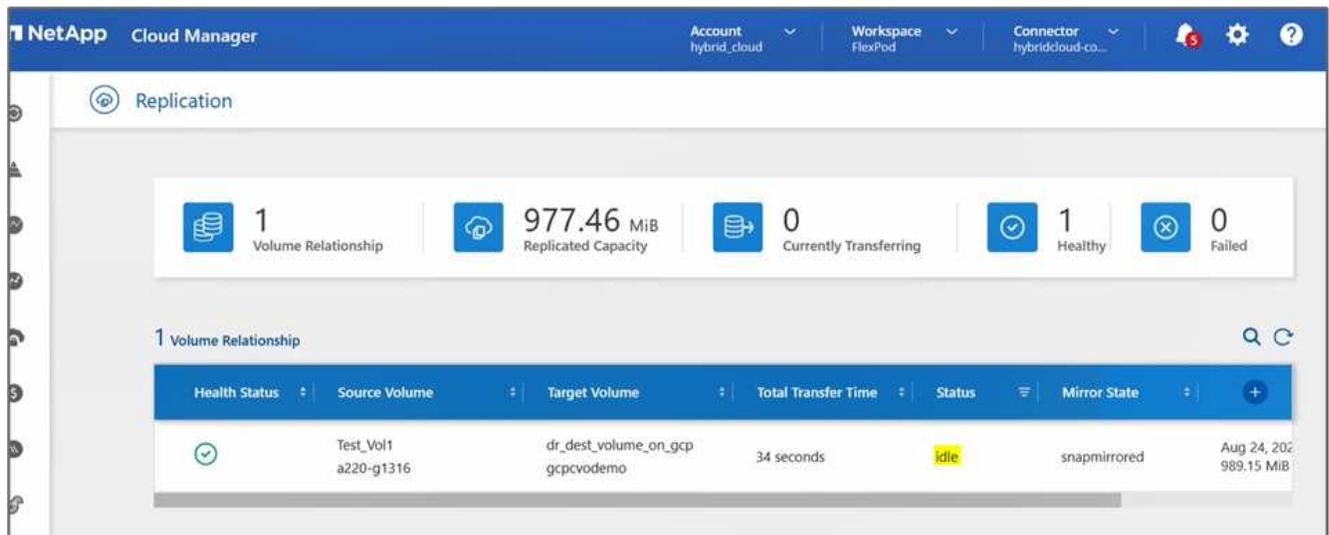
```

```

root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo# sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59 test.zip
root@hybridcloudbackup:/snapmirror_demo#
root@hybridcloudbackup:/snapmirror_demo#

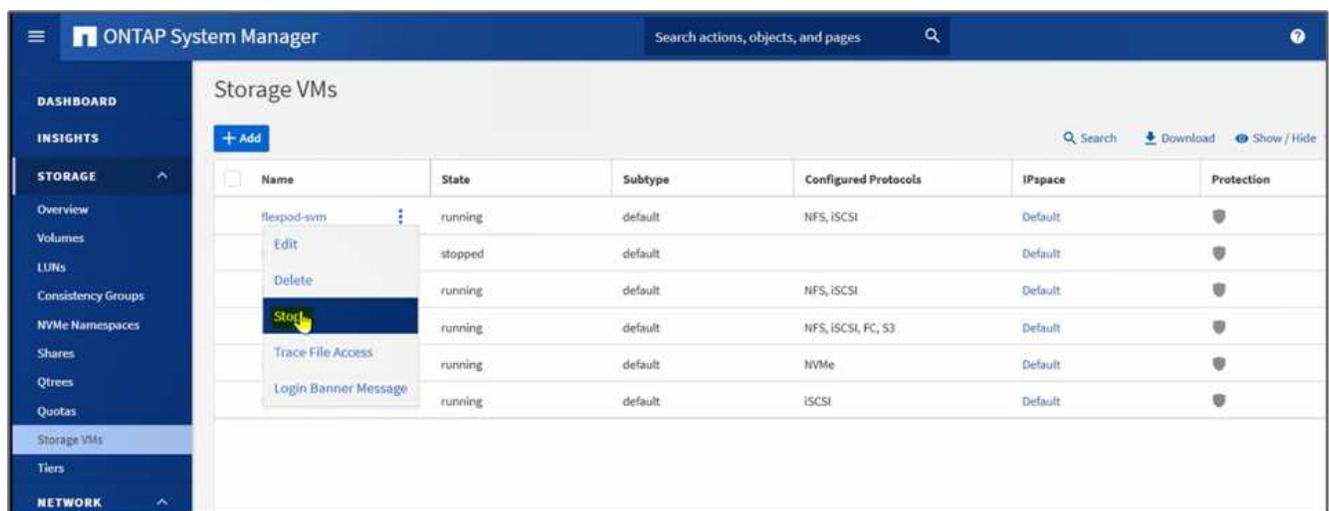
```

7. Vérifiez l'état de la réplication dans Cloud Manager. Le transfert de données peut prendre quelques minutes en fonction de la taille des données. Une fois cette opération terminée, vous pouvez voir l'état de SnapMirror comme **Idle**.

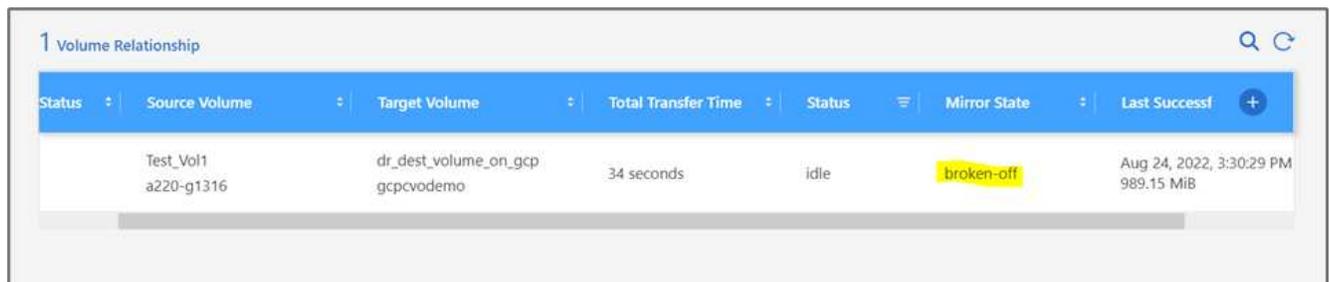
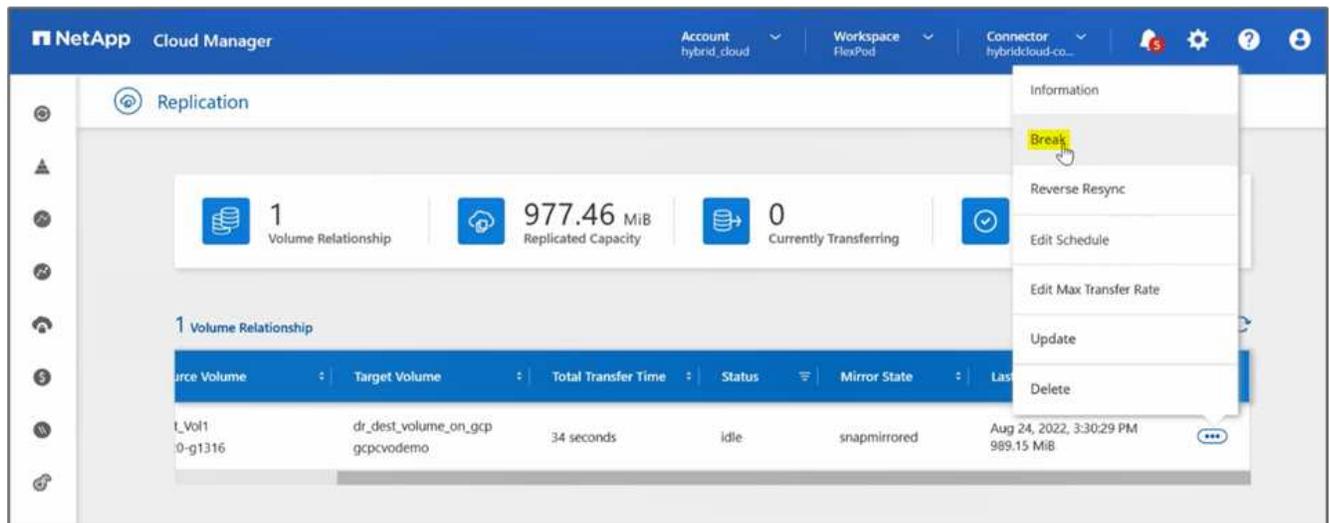


8. Lorsque le transfert de données est terminé, simuler un incident côté source en arrêtant le SVM qui héberge le Test_vol1 volumétrie.

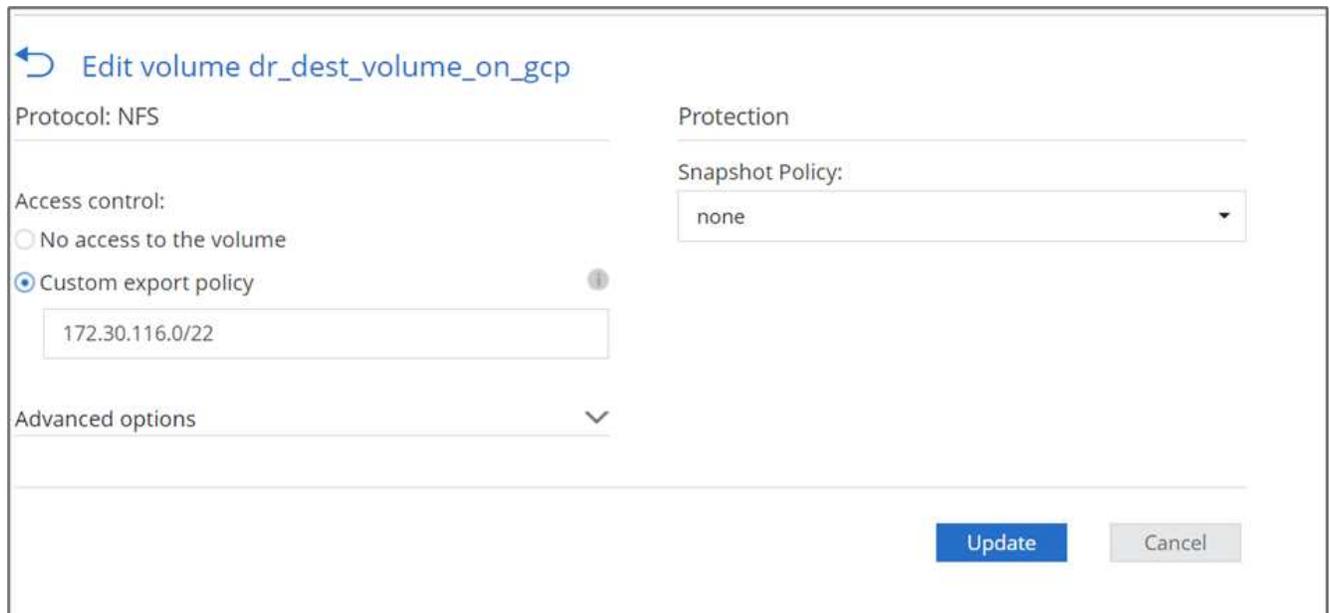
Après l'arrêt du SVM, le Test_vol1 Le volume n'est pas visible dans Cloud Manager.



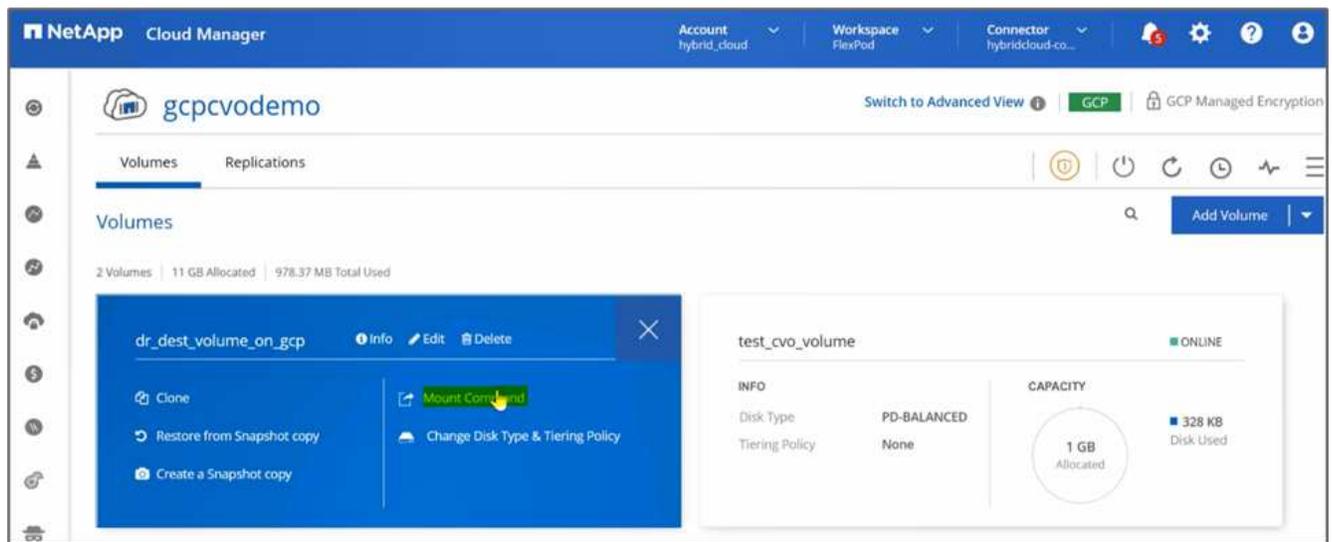
9. Interrompre la relation de réplication et promouvoir le volume de destination Cloud Volumes ONTAP en production.



10. Modifiez le volume et activez l'accès client en l'associant à une export policy.



11. Procurez-vous la commande de montage prête à l'emploi pour le volume.



12. Monter le volume sur une instance de calcul, vérifier la présence des données dans le volume de destination et générer le checksum SHA256 du `sample_dataset_2GB` fichier.

```
drwxr-xr-x 21 root root          4096 Aug 24 10:20 ../
-rwxr-xr-x  1 nobody 4294967294 1015306240 Aug 24 09:59 test.zip*
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$ sha256sum test.zip
888a23c8495ad33fdf11a931ffc344c3643f15d5cefedbbf1326016e31ec5a59 test.zip
ruchikal_netapp_com@demo-nfs:/snapmirror_dest$
```

13. Comparer les valeurs de somme de contrôle à la fois à la source (FlexPod) et à la destination (Cloud Volumes ONTAP).
14. Les checksums correspondent à la source et à la destination.

Vous pouvez confirmer que la réplication des données de la source vers la destination a été correctement effectuée et que l'intégrité des données a été maintenue. Ces données peuvent désormais être consommées en toute sécurité par les applications afin de servir les clients pendant que le site source passe par la restauration.

"Suivant: Conclusion."

Conclusion

"Précédent : validation de la solution."

Dans cette solution, le service de données cloud NetApp, Cloud Volumes ONTAP et l'infrastructure de data Center FlexPod ont été utilisés pour créer une solution de reprise après incident avec un cloud public optimisé par Cisco Intersight Cloud Orchestrator. La solution FlexPod a constamment évolué pour permettre aux clients de moderniser leurs applications et leurs processus de distribution. Avec cette solution, vous pouvez créer un plan de reprise après incident BCDR avec le cloud public, point de passage à un plan de reprise après incident transitoire ou à plein temps, tout en réduisant le coût de la solution de reprise après incident.

La réplication des données entre FlexPod sur site et NetApp Cloud Volumes ONTAP a été gérée par la technologie SnapMirror éprouvée, mais vous pouvez également sélectionner d'autres outils NetApp de transfert et de synchronisation comme Cloud Sync pour vos besoins en termes de mobilité des données. Sécurité des données à la volée assurée par des technologies de chiffrement intégrées basées sur TLS/AES.

Que vous ayez un plan de reprise sur incident temporaire pour une application ou un plan de reprise sur incident à temps plein pour une entreprise, le portefeuille de produits utilisés dans cette solution peut répondre aux deux besoins à grande échelle. Optimisé par Cisco Intersight Workflow Orchestrator, il en va de même pour l'automatisation avec des flux de travail prédéfinis qui éliminent non seulement les processus de reconstruction, mais accélèrent également la mise en œuvre d'un plan de CDR.

Cette solution permet de gérer FlexPod sur site et la réplication des données dans un cloud hybride de manière très simple et pratique, grâce à l'automatisation et à l'orchestration fournies par Cisco Intersight Cloud Orchestrator.

Où trouver des informations complémentaires

Pour en savoir plus sur les informations données dans ce livre blanc, consultez ces documents et/ou sites web :

GitHub

- Toutes les configurations Terraform utilisées

["https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO"](https://github.com/NetApp-Automation/FlexPod-hybrid-cloud-for-GCP-with-Intersight-and-CVO)

- Fichiers JSON pour l'importation des flux de production

["https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows"](https://github.com/ucs-compute-solutions/FlexPod_DR_Workflows)

Cisco Intersight

- Centre d'aide Cisco Intersight

["https://intersight.com/help/saas/home"](https://intersight.com/help/saas/home)

- Documentation Cisco Intersight Cloud Orchestrator :

["https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator"](https://intersight.com/help/saas/features/orchestration/configure#intersight_cloud_orchestrator)

- Cisco Intersight Service pour la documentation Terraform de HashiCorp

["https://intersight.com/help/saas/features/terraform_cloud/admin"](https://intersight.com/help/saas/features/terraform_cloud/admin)

- Fiche technique Cisco Intersight

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/intersight-ds.html)

- Fiche technique Cisco Intersight Cloud Orchestrator

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-cloud-orch-aag-cte-en.html)

- Fiche technique Cisco Intersight Service for HashiCorp Terraform

["https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html"](https://www.cisco.com/c/en/us/products/collateral/cloud-systems-management/intersight/nb-06-intersight-terraf-ser-aag-cte-en.html)

FlexPod

- Page d'accueil de FlexPod

["https://www.flexpod.com"](https://www.flexpod.com)

- Guides de conception et de déploiement validés par Cisco pour FlexPod

["FlexPod Datacenter avec Cisco UCS 4.2\(1\) en mode géré UCS, VMware vSphere 7.0 U2 et NetApp ONTAP 9.9 : Guide de conception"](#)

- FlexPod Datacenter avec Cisco UCS X-Series

["https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html"](https://www.cisco.com/c/en/us/td/docs/unified_computing/ucs/UCS_CVDs/flexpod_xseries_esxi7u2_design.html)

Interopérabilité

- Matrice d'interopérabilité NetApp

["http://support.netapp.com/matrix/"](http://support.netapp.com/matrix/)

- Outil d'interopérabilité matérielle et logicielle Cisco UCS

["http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html"](http://www.cisco.com/web/techdoc/ucs/interoperability/matrix/matrix.html)

- Guide de compatibilité VMware

["http://www.vmware.com/resources/compatibility/search.php"](http://www.vmware.com/resources/compatibility/search.php)

Documents de référence de NetApp Cloud Volumes ONTAP

- NetApp Cloud Manager

["https://docs.netapp.com/us-en/occm/concept_overview.html"](https://docs.netapp.com/us-en/occm/concept_overview.html)

- Cloud Volumes ONTAP

<https://docs.netapp.com/us-en/cloud-manager-cloud-volumes-ontap/task-getting-started-gcp.html>

- Calculateur de coût total de possession Cloud Volumes ONTAP

<https://cloud.netapp.com/google-cloud-calculator>

- Cloud Volumes ONTAP Sizer

["https://cloud.netapp.com/cvo-sizer"](https://cloud.netapp.com/cvo-sizer)

- Outil d'évaluation du cloud

<https://cloud.netapp.com/assessments>

- Le cloud hybride NetApp

<https://cloud.netapp.com/hybrid-cloud>

- Documentation de l'API Cloud Manager

["https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html"](https://docs.netapp.com/us-en/occm/reference_infrastructure_as_code.html)

Résolution des problèmes

["https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_\(CVO\)"](https://kb.netapp.com/Advice_and_Troubleshooting/Cloud_Services/Cloud_Volumes_ONTAP_(CVO))

Terraform

- Terraform Cloud

["https://www.terraform.io/cloud"](https://www.terraform.io/cloud)

- Documentation Terraform

["https://www.terraform.io/docs/"](https://www.terraform.io/docs/)

- Registre NetApp Cloud Manager

["https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/latest"](https://registry.terraform.io/providers/NetApp/netapp-cloudmanager/latest)

GCP

- ONTAP haute disponibilité pour GCP

["https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick"](https://cloud.netapp.com/blog/gcp-cvo-blg-what-makes-cloud-volumes-ontap-high-availability-for-gcp-tick)

- Avantages de GCP

<https://netapp.hosted.panopto.com/Panopto/Pages/Viewer.aspx?id=f3d0368b-7165-4d43-a76e-ae01011853d6>

Informations sur le copyright

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

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

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