Guide du portail pour les administrateurs de fournisseurs de services VMware Cloud Director

19 septembre 2019

VMware Cloud Director 10.0

Vous trouverez la documentation technique la plus récente sur le site Web de VMware, à l'adresse :

https://docs.vmware.com/fr/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

VMware France SAS.
Tour Franklin
100-101 Terrasse Boieldieu
92042 Paris La Défense 8 Cedex
France
www.vmware.com/fr

Copyright © 2018-2020 VMware, Inc. Tous droits réservés. Informations relatives aux copyrights et marques commerciales.

Table des matières

1 À propos de vCloud Director Service Provider Admin Portal 9

2 Démarrage avec vCloud Director Service Provider Admin Portal 10

- Présentation de l'administration de vCloud Director 10
- Connectez-vous à vCloud Director Service Provider Admin Portal 14
- Afficher les tâches 14
- Arrêter une tâche en cours 15
- Afficher les événements 15
- Limites de longueur des noms et des descriptions 16

3 Gestion de ressources vSphere 18

- Ajout de ressources vCenter Server et NSX 19
  - Attacher une instance de vCenter Server seule ou avec une instance de NSX Manager 19
  - Découverte et adoption de vApp 23
  - Attribuer la clé de licence NSX dans vCenter Server 24
  - Enregistrer une instance de NSX-T Manager 25
- Ajout de ressources Cloud 25
  - Centres de données virtuels fournisseur 26
  - Créer un centre de données virtuel fournisseur 26
  - Réseaux externes 30
  - Pools de réseaux 33
- Afficher les instances de vCenter Server 37
- Modifier les paramètres vCenter Server 38
- Activer ou désactiver une instance de vCenter Server 39
- Reconnecter une instance de vCenter Server 39
- Actualiser une instance de vCenter Server 39
- Actualiser les stratégies de stockage d'une instance de vCenter Server 40
- Annuler l'enregistrement d'une instance de vCenter Server 40
- Modifier les paramètres de NSX Manager 41
- Modifier les paramètres de NSX-T Manager 42
- Supprimer une instance de NSX-T Manager 42
- Configuration et gestion de déploiements multisite 42
- Listes de ressources multisites 45

4 Gestion des centres de données virtuels fournisseur 46

- Activer ou désactiver un centre de données virtuel fournisseur 46
- Supprimer un centre de données virtuel fournisseur 47
- Modifier les paramètres généraux d'un centre de données virtuel fournisseur 47

Fusionner les centres de données virtuels fournisseur 48
Afficher les centres de données virtuels d'organisation d'un centre de données virtuel fournisseur 49
Afficher les banques de données sur un centre de données virtuel fournisseur 49
Afficher les réseaux externes sur un centre de données virtuel fournisseur 50
Gestion des stratégies de stockage de machine virtuelle dans un centre de données virtuel fournisseur 51
Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel fournisseur 51
Activer ou désactiver une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur 52
Supprimer une stratégie de stockage de machine virtuelle d'un centre de données virtuel fournisseur 52
Modifier les métadonnées d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur 53
Gestion des pools de ressources dans un centre de données virtuel fournisseur 53
Ajouter un pool de ressources à un centre de données virtuel fournisseur 53
Activer ou désactiver un pool de ressources sur un centre de données virtuel fournisseur 54
Détacher un pool de ressources d'un centre de données virtuel fournisseur 55
Modifier les métadonnées d'un centre de données virtuel fournisseur 55

5 Gestion d'organisations 57
Comprendre comment fonctionnent les baux 57
Créer une organisation 58
Configurer les catalogues d'une organisation 58
Configurer les stratégies d'une organisation 59
Migrer le stockage des locataires 61

6 Gestion des centres de données virtuels d'organisation 63
Compréhension des modèles d'allocation 63
Utilisation suggérée des modèles d'allocation 66
Modèle d'allocation Flex 67
Modèle d'allocation de pool d'allocation 69
Modèle d'allocation de facturation à l'utilisation 70
Modèle d'allocation de pool de réservation 71
Présentation des stratégies de positionnement et de dimensionnement de machine virtuelle 72
Attributs des stratégies de dimensionnement de machine virtuelle 78
Créer une stratégie de positionnement de VM 80
Ajouter une stratégie de positionnement de machine virtuelle à un VDC d'organisation 81
Supprimer une stratégie de positionnement de machine virtuelle 82
Créer une stratégie de dimensionnement de machine virtuelle 83

Ajouter une stratégie de dimensionnement de machine virtuelle à un VDC d'organisation 83
Modifier une stratégie de dimensionnement de machine virtuelle 84
Supprimer une stratégie de dimensionnement de machine virtuelle 85
Créer un centre de données virtuel d'organisation 85
Activer ou désactiver un centre de données virtuel d'organisation 89
Supprimer un centre de données virtuel d'organisation 89
Modifier le nom et la description d'un centre de données virtuel d'organisation 90
Modifier les paramètres de modèle d'allocation d'un centre de données virtuel d'organisation 90
Modification des paramètres de stockage d'un centre de données virtuel d'organisation 91
Modifier les paramètres de provisionnement de machine virtuelle d'un centre de données virtuel d'organisation 91
Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel d'organisation 92
Modifier la stratégie de stockage par défaut sur un centre de données virtuel d'organisation 92
Modifier la limite d'une stratégie de stockage sur un centre de données virtuel d'organisation 93
Modifier les métadonnées d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel d'organisation 93
Activer ou désactiver une stratégie de stockage dans un centre de données virtuel d'organisation 94
Supprimer une stratégie de stockage d'un centre de données virtuel d'organisation 95
Modifier les paramètres réseau d'un centre de données virtuel d'organisation 95
Configuration de la mise en réseau intercentre de données virtuel 96
Modifier les métadonnées d'un centre de données virtuel d'organisation 98
Afficher les pools de ressources d'un centre de données virtuel d'organisation 99
Gestion du pare-feu distribué dans un centre de données virtuel d'organisation 99
Activer le pare-feu distribué dans un centre de données virtuel d'organisation 99
Ajouter une règle de pare-feu distribué 100
Modifier une règle de pare-feu distribué 103
Personnaliser le regroupement d'objets 104
Utilisation des groupes de sécurité 107
Utilisation des balises de sécurité 111

7 Gestion de passerelles Edge NSX Data Center for vSphere 116
Utilisation des clusters Edge 117
Ajouter une passerelle Edge NSX Data Center for vSphere 118
Configuration des services de passerelle Edge NSX Data Center for vSphere 121
Gestion d'un pare-feu de passerelle Edge NSX Data Center for vSphere 121
Gestion du protocole DHCP de la passerelle Edge NSX Data Center for vSphere 126
Ajouter une règle SNAT ou DNAT 131
Configuration de routage avancée 134

Équilibrage de charge 143
Sécuriser l'accès à l'aide de réseaux privés virtuels 158
Gestion des certificats SSL 186
Personnaliser le regroupement d'objets 194
Afficher l'utilisation des réseaux et les allocations IP sur une passerelle Edge 197
Modification des propriétés de la passerelle Edge 197
Activer ou désactiver le routage distribué sur une passerelle Edge 198
Modifier les réseaux externes et les paramètres de passerelle Edge 198
Modifier les paramètres généraux d'une passerelle Edge 199
Modifier la passerelle par défaut sur une passerelle Edge 199
Modifier les paramètres IP d'une passerelle Edge 200
Modifier les pools d'adresses IP sous-alloués d'une passerelle Edge 200
Modifier les limites de débit sur une passerelle Edge 201
Redéployer une passerelle Edge 201
Supprimer une passerelle Edge 202
Statistiques et journaux pour une passerelle Edge 202
Afficher les statistiques 202
Activer la journalisation 203
Activer l'accès de ligne de commande SSH à une passerelle Edge 205

8 Gestion de passerelles Edge NSX-T Data Center 206
Ajouter une passerelle Edge NSX-T Data Center 206
Ajouter un groupe de pare-feu à une passerelle Edge NSX-T 207
Ajouter une règle de pare-feu de passerelle Edge NSX-T 208
Ajouter une règle SNAT ou DNAT à une passerelle Edge NSX-T 209
Configurer un service de redirecteur DNS sur une passerelle Edge NSX-T 211
Modifier les allocations IP d'une passerelle Edge NSX-T 211
Allocation d'adresses IP rapide 212
Créer des profils de port d'application personnalisés 213

9 Gestion des instances de vCenter Server dédiées et des proxys 215
Activer l'accès locataire d'une instance de vCenter Server associée 218
Créer un proxy pour une instance dédiée de vCenter Server 218
Gérer les certificats de proxy et les listes de révocation de certificats 219
Publier une instance de vCenter Server dédiée 219

10 Gestion d'administrateurs système et de rôles 221
Gestion des droits et des rôles 221
Rôles prédéfinis et leurs droits 223
Droits d'administrateur système 226
Droits des rôles de locataire globaux prédéfinis 234

Gestion des bundles de droits 240
Gestion des rôles de locataire globaux 243
Gestion des rôles de fournisseur 246
Gestion des utilisateurs et des groupes de fournisseur 248
Gestion des utilisateurs de fournisseur 248
Gestion des groupes de fournisseurs 252

11 Gestion de paramètres système 254
Modifier des paramètres système généraux 254
Paramètres système généraux 255
Configurer les paramètres de messagerie du système 257
Modifier la licence vCloud Director 258
Configurez les paramètres de synchronisation du catalogue. 258
Configuration des tâches bloquantes et des notifications 259
Configurer un Broker AMQP 259
Configurer les paramètres des tâches bloquantes 260
Configurer des adresses publiques 261
Gestion des fournisseurs d'identité 263
Gestion des connexions LDAP 264
Configurer votre système pour utiliser un fournisseur d'identité SAML 267
Gestion des plug-ins 269
Télécharger un plug-in 270
Activer ou désactiver un plug-in 270
Supprimer un plug-in 271
Publier ou annuler la publication d'un plug-in d'une organisation 271
Personnalisation des portails vCloud Director 271
Configurer la stratégie de mot de passe 273
Configurer les services vSphere 274

12 Surveillance de vCloud Director 275
vCloud Director et rapport de coût 275
Afficher les informations d'utilisation d'un centre de données virtuel fournisseur 276

13 Gestion des services 277
Intégration de vRealize Orchestrator à vCloud Director 277
Inscrire une instance de vRealize Orchestrator auprès de vCloud Director 278
Créer une catégorie de service 279
Modifier une catégorie de service 279
Importer un service 280
Rechercher un service 281
Exécuter un service 281

Modifier une catégorie de service 282
Annuler l'inscription d'un service 282
Publier un service 283

14 Gestion des entités personnalisées 284
Rechercher une entité personnalisée 284
Modifier la définition d'une entité personnalisée 285
Ajouter une définition d'entité personnalisée 285
Instances d'entité personnalisée 286
Associer une action à une entité personnalisée 287
Dissocier une action depuis une entité personnalisée 287
Publier une entité personnalisée 288
Supprimer une entité personnalisée 288

À propos de vCloud Director Service Provider Admin Portal

1

Le *Guide de vCloud Director Service Provider Admin Portal* fournit des informations sur l'utilisation de Service Provider Admin Portal. Le service provider admin portal vous permet de gérer et de surveiller des organisations, des droits, des rôles, des utilisateurs et des groupes dans votre cloud. Vous pouvez également créer et gérer des réseaux de centres de données virtuels d'organisation dépendant de NSX-T.

Public cible

Ce guide est destiné aux administrateurs du fournisseur de services qui souhaitent utiliser les fonctionnalités proposées sur vCloud Director Service Provider Admin Portal.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui pourraient vous être inconnus. Pour obtenir les définitions des termes employés dans la documentation technique VMware, accédez à https://docs.vmware.com.

Démarrage avec vCloud Director Service Provider Admin Portal

2

vCloud Director Service Provider Admin Portal est une interface dédiée pour les administrateurs du fournisseur de services.

Ce chapitre contient les rubriques suivantes :

- Présentation de l'administration de vCloud Director
- Connectez-vous à vCloud Director Service Provider Admin Portal
- Afficher les tâches
- Arrêter une tâche en cours
- Afficher les événements
- Limites de longueur des noms et des descriptions

Présentation de l'administration de vCloud Director

VMware vCloud Director vous permet de créer des environnements Cloud sécurisés à locataires multiples en regroupant des ressources d'infrastructure virtuelle en centres de données virtuels et en les présentant aux utilisateurs via des portails Web et des interfaces de programmation comme un service entièrement automatisé, basé sur un catalogue.

Le *Guide du portail d'administration des fournisseurs de services vCloud Director* fournit des informations sur l'ajout de ressources au système, la création et le provisionnement des organisations, la gestion des ressources et des organisations, ainsi que la surveillance du système.

Ressources vSphere et NSX

vCloud Director dépend des ressources vSphere pour fournir un CPU et de la mémoire nécessaires à l'exécution de machines virtuelles. En outre, les banques de données vSphere fournissent un stockage pour les fichiers de machine virtuelle et autres fichiers requis pour les opérations de machine virtuelle. vCloud Director utilise également des commutateurs distribués vSphere, des groupes de ports vSphere et NSX Data Center for vSphere pour prendre en charge la mise en réseau de machine virtuelle.

vCloud Director peut également utiliser des ressources à partir de NSX-T Data Center. Pour plus d'informations sur l'enregistrement d'une instance de NSX-T Manager dans votre environnement Cloud, reportez-vous au *Guide du portail d'administration des fournisseurs de services vCloud Director* ou au *Guide de programmation de vCloud API pour fournisseurs de services*.

Vous pouvez utiliser les ressources vSphere et NSX sous-jacentes pour créer des ressources de cloud.

À partir de la version 9.7, vCloud Director peut agir comme un serveur proxy HTTP, avec lequel vous pouvez permettre aux organisations d'accéder à l'environnement vSphere sous-jacent.

Ressources de Cloud

Les ressources de cloud constituent une abstraction de leurs ressources vSphere sous-jacentes. Elles fournissent les ressources de calcul et de mémoire aux machines virtuelles vCloud Director et aux vApp. Un vApp est un système virtuel qui contient une ou plusieurs machines virtuelles individuelles, avec des paramètres qui définissent les détails du fonctionnement. Les ressources de Cloud fournissent aussi un accès au stockage et à la connectivité du réseau.

Les ressources de cloud incluent des centres de données virtuels de fournisseur et d'organisation, des réseaux externes, des réseaux de centres de données virtuels d'organisation et des pools de réseaux.

Pour pouvoir ajouter des ressources de Cloud à vCloud Director, vous devez ajouter des ressources vSphere.

Instances de vCenter Server dédiées et proxys

Une instance de vCenter Server dédiée est une ressource de Cloud qui encapsule une installation de vCenter Server entière. Une instance de vCenter Server dédiée inclut un ou plusieurs proxys qui sont des points d'accès à différents composants de l'environnement vSphere sous-jacent. Le fournisseur peut créer et activer des instances de vCenter Server dédiées et des proxys. Le fournisseur peut publier une instance de vCenter Server dédiée vers les locataires.

Pour créer et gérer des instances de vCenter Server dédiées et des proxys, vous pouvez utiliser Service Provider Admin Portal ou vCloud OpenAPI. Reportez-vous aux sections Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys et *Démarrage de vCloud OpenAPI* à l'adresse https://code.vmware.com.

Centres de données virtuels fournisseur

Un centre de données virtuel fournisseur combine les ressources de calcul et de mémoire d'un pool de ressources vCenter Server unique avec les ressources de stockage d'une ou de plusieurs banques de données accessibles à ce pool de ressources.

Un centre de données virtuel fournisseur peut utiliser les ressources réseau d'une instance de NSX Manager associée à l'instance de vCenter Server ou d'une instance de NSX-T Manager enregistrée dans le cloud.

Vous pouvez créer plusieurs centres de données virtuels fournisseur pour les utilisateurs qui se trouvent dans différents emplacements géographiques ou unités commerciales, ou pour les utilisateurs ayant des conditions requises distinctes en termes de performances.

Centres de données virtuels d'organisation

Un centre de données virtuel d'organisation fournit des ressources à une organisation et il est partitionné depuis un centre de données virtuel fournisseur. Les centres de données virtuels d'organisation fournissent un environnement dans lequel des systèmes virtuels peuvent être stockés, déployés et exécutés. Ils fournissent aussi un stockage pour un support virtuel, comme des disquettes et des CD ROM.

Une seule organisation peut posséder plusieurs centres de données virtuels d'organisation.

Mise en réseau de vCloud Director

vCloud Director prend en charge trois types de réseaux.

- Réseaux externes
- Réseaux de centre de données virtuel d'organisation
- Réseaux vApp

Certains réseaux de centres de données virtuels d'organisation et tous les réseaux vApp reposent sur des pools de réseaux.

Réseaux externes

Un réseau externe est un réseau logique, différencié, basé sur un groupe de ports vSphere. Des réseaux de centres de données virtuels d'organisation peuvent se connecter à des réseaux externes pour fournir une connectivité Internet à des machines virtuelles dans un vApp.

À partir de la version 9.5, vCloud Director prend en charge les réseaux externes IPv6. Un réseau externe IPv6 prend en charge les sous-réseaux IPv4 et IPv6, et un réseau externe IPv4 prend en charge les sous-réseaux IPv4 et IPv6.

Par défaut, seuls les **administrateurs système** créent et gèrent des réseaux externes.

Réseaux de centre de données virtuel d'organisation

Un réseau de centre de données virtuel d'organisation appartient à un centre de données virtuel d'organisation vCloud Director et est accessible à tous les vApp de l'organisation. Un réseau de centre de données virtuel d'organisation permet aux vApp d'une organisation de communiquer entre eux. Pour fournir une connectivité externe, vous pouvez connecter un réseau de centre de données virtuel d'organisation à un réseau externe. Vous pouvez également créer un réseau de centre de données virtuel d'organisation isolé interne à l'organisation.

vCloud Director 9.5 introduit la prise en charge IPv6 pour les réseaux de centre de données virtuel d'organisation directs et acheminés.

À partir de vCloud Director 9.5, les **administrateurs système** peuvent créer des réseaux de centres de données virtuels isolés reposant sur un commutateur logique NSX-T. Les **administrateurs d'organisation** peuvent créer des réseaux de centres de données virtuels isolés dépendant de pools de réseaux.

vCloud Director 9.5 introduit également la mise en réseau entre centres de données virtuels en configurant des réseaux étirés dans des groupes de centres de données virtuels.

Par défaut, seuls les **administrateurs système** peuvent créer des réseaux directs et entre centres de données virtuels. Les **administrateurs système** et les **administrateurs d'organisation** peuvent gérer des réseaux de centres de données virtuels d'organisation, même s'il existe des limites aux opérations qu'un **administrateur d'organisation** peut effectuer.

Réseaux vApp

Un réseau vApp réside dans un vApp et permet aux machines virtuelles contenues dans le vApp de communiquer entre elles. Pour permettre à un vApp de communiquer avec d'autres vApp dans l'organisation, vous pouvez connecter le réseau vApp à un réseau de centre de données virtuel d'organisation. Si le réseau de centre de données virtuel d'organisation est connecté à un réseau externe, le vApp peut communiquer avec les vApp d'autres organisations. Les réseaux vApp dépendent de pools de réseaux.

La plupart des utilisateurs disposant d'un accès à un vApp peuvent créer et gérer leurs propres réseaux vApp. Pour plus d'informations sur l'utilisation de réseaux d'un vApp, reportez-vous à la section *Guide du portail de locataires de vCloud Director*.

Pools de réseaux

Un pool de réseaux est un groupe de réseaux indifférenciés pouvant être utilisé dans un centre de données virtuel d'organisation. Un pool de réseaux repose sur les ressources réseau de vSphere telles que les ID de VLAN ou les groupes de ports. vCloud Director utilise des pools de réseaux pour créer des réseaux de centres de données virtuels d'organisation internes ou acheminés par NAT et tous les réseaux vApp. Le trafic réseau sur chaque réseau dans un pool est isolé à la couche 2 de tous les autres réseaux.

Chaque centre de données virtuel d'organisation dans vCloud Director peut disposer d'un pool de réseaux. Plusieurs centres de données virtuels d'organisation peuvent partager un pool de réseaux. Le pool de réseaux d'un centre de données virtuel d'organisation fournit les réseaux créés pour répondre au quota de réseaux d'un centre de données virtuel d'organisation.

Seuls les **administrateurs système** peuvent créer et gérer des pools de réseaux.

Organisations

vCloud Director prend en charge une architecture à locataires multiples à l'aide des organisations. Une organisation est une unité d'administration pour un ensemble d'utilisateurs, de groupes et de ressources de calcul. Les utilisateurs s'authentifient au niveau de l'organisation, en fournissant des identifiants établis par un administrateur d'organisation lors de la création

ou de l'importation de l'utilisateur. Les **administrateurs système** créent et provisionnent des organisations, tandis que les **administrateurs d'organisation** gèrent les utilisateurs, les groupes et les catalogues d'une organisation. Les tâches des **administrateurs d'organisation** sont décrites dans la section *Guide du portail de locataires de vCloud Director*.

Utilisateurs et groupes

Une organisation peut contenir un nombre arbitraire d'utilisateurs et de groupes. Les **administrateurs d'organisation** peuvent créer des utilisateurs et importer des utilisateurs et des groupes à partir d'un service d'annuaire, tel que LDAP. L'**administrateur système** gère l'ensemble des droits disponibles à chaque organisation. L'**administrateur système** peut créer et publier des rôles de locataire globaux à une ou plusieurs organisations. L'**administrateur d'organisation** peut créer des rôles locaux dans son organisation.

Catalogues

Les organisations utilisent des catalogues pour stocker des modèles de vApp et des fichiers de support. Les membres d'une organisation disposant d'un accès à un catalogue peuvent utiliser les modèles de vApp et les fichiers de support pour créer leurs propres vApp. Un **administrateur système** peut permettre à l'organisation de publier un catalogue pour le mettre à disposition d'autres organisations. Les **administrateurs d'organisation** peuvent ensuite choisir les éléments du catalogue à fournir à leurs utilisateurs.

Connectez-vous à vCloud Director Service Provider Admin Portal

Vous pouvez accéder à vCloud DirectorService Provider Admin Portal à l'aide d'un navigateur Web.

Conditions préalables

Vous devez disposer les droits d'administrateur système pour accéder à vCloud Director Service Provider Admin Portal.

Procédure

1. Dans un navigateur, tapez l'URL de Service Provider Admin Portal de votre site vCloud Director et appuyez sur Entrée.

   Par exemple, tapez `https://vcloud.example.com/provider`.

2. Connectez-vous avec le nom d'utilisateur et le mot de passe d'administrateur système.

Afficher les tâches

Sur Service Provider Admin Portal, vous pouvez afficher les tâches récentes et leur état.

L'affichage des tâches permet de connaître l'état des tâches sur votre portail d'administration de fournisseur en un clin d'œil. La vue affiche à quel moment les tâches ont été exécutées, et si elles ont réussi. Cet outil peut constituer la première étape de dépannage des problèmes rencontrés dans votre environnement.

Les info-bulles bleues et rouges sur l'icône Tâches indiquent le nombre de tâches exécutées et ayant échoué, respectivement.

Procédure

- Dans le menu supérieur droit, sélectionnez l'icône Tâches ( ).

Résultats

Une liste des tâches récentes s'affiche, ainsi que l'heure à laquelle la tâche a été exécutée et l'état de celle-ci.

Arrêter une tâche en cours

Si vous démarrez accidentellement une opération avant l'application ou le passage en revue de tous les paramètres nécessaires, vous pouvez arrêter la tâche en cours.

Par défaut, le panneau **Tâches récentes** s'affiche en bas du portail. Lorsque vous démarrez une opération, par exemple pour créer une machine virtuelle, la tâche s'affiche dans le panneau.

Conditions préalables

Le panneau **Tâches récentes** doit être ouvert.

Procédure

1. Démarrez une opération de longue durée.

   Les opérations de longue durée sont des opérations comme la création d'une machine virtuelle ou un vApp, les opérations d'alimentation effectuées sur les machines virtuelles et vApp, et ainsi de suite.

2. Dans le panneau **Tâches récentes**, cliquez sur l'icône **Annuler** ( ).
3. Dans la boîte de dialogue **Annuler la tâche**, confirmez que vous voulez annuler la tâche en cliquant sur **OK**.

Résultats

L'opération s'arrête.

Afficher les événements

Depuis le portail, vous pouvez consulter la liste de tous les événements, ainsi que leurs détails et leur état.

La vue des événements permet de visualiser l'état des événements dans votre portail. La vue affiche à quel moment les événements se sont produits, et si ils ont réussi. La vue des événements contient des occurrences uniques, telles que les connexions utilisateur et la création ou la suppression d'objets.

Procédure

1 Dans le menu principal (☰), sélectionnez **Événements**.

La liste de tous les événements s'affiche, ainsi que l'heure à laquelle l'événement s'est produit et l'état de l'événement.

2 Cliquez sur l'icône de l'éditeur ( ) pour modifier les détails que vous voulez voir sur les événements.

3 (Facultatif) Cliquez sur un événement pour afficher ses détails.

Détails	Description
Événement	Nom de l'événement. Par exemple, si vous modifiez un vApp pour inclure des machines virtuelles, l'événement qui démarre l'ensemble de l'opération est *Task 'Modify vApp' start*.
Identifiant de l'événement	ID de l'événement.
Type	L'objet sur lequel la tâche a été effectuée. Par exemple, si vous avez créé une machine virtuelle, le type est *vm*.
Cible	Objet cible de l'événement. Par exemple, lorsque vous modifiez un vApp pour y inclure des machines virtuelles, la cible de l'événement *Task 'Modify vApp' start* est *vdcUpdateVapp*.
Status	État de l'événement, tel que Réussite ou Échec.
Espace de noms de service	Nom du service, tel que *com.vmware.vcloud*.
Organisation	Nom de l'organisation
Propriétaire	Utilisateur qui a déclenché l'événement.
Heure de l'événement	Date et heure auxquelles l'événement s'est produit.

Limites de longueur des noms et des descriptions

Appliquez les règles suivantes lorsque vous entrez des valeurs dans vCloud Director.

Les valeurs de chaîne pour l'attribut `name` et les éléments `Description` et `ComputerName` ont des limites de longueur qui dépendent de l'objet auquel ils sont associés.

Tableau 2-1. Limites de longueur des propriétés d'objet

Objet	Propriété	Nombre maximal de caractères
Catalog	name	128
Catalog	Description	256
EdgeGateway	name	35
Media	name	128
Media	Description	256
VApp	name	128
VApp	Description	256
VAppTemplate	name	128
VAppTemplate	Description	256
Vdc	name	128
Vdc	Description	256
Vm	name	128
Vm	ComputerName	15 sous Windows, 63 sur toutes les autres plates-formes
Vm	Description	256

Gestion de ressources vSphere 3

vCloud Director tire ses ressources d'une infrastructure virtuelle vSphere sous-jacente. Après l'enregistrement de ressources vSphere dans vCloud Director, vous pouvez allouer ces ressources à des organisations au sein de l'installation vSphere à utiliser.

vCloud Director utilise un ou plusieurs environnements vCenter Server pour sauvegarder ses centres de données virtuels. À partir de la version 9.7, vCloud Director peut également utiliser un environnement vCenter Server pour encapsuler un SDDC avec un ou plusieurs proxys. Vous pouvez permettre aux locataires d'utiliser ces proxys comme Access Point à l'environnement vSphere sous-jacent depuis vCloud Director avec leurs comptes vCloud Director.

Pour pouvoir utiliser une instance de vCenter Server dans vCloud Director, vous devez attacher cette instance de vCenter Server.

Lorsque vous créez un centre de données virtuel fournisseur soutenu par une instance de vCenter Server attachée, cette instance de vCenter Server est indiquée comme étant publiée sur le fournisseur de services, et est également dite incluse dans la portée du fournisseur. Pour plus d'informations sur la création d'un centre de données virtuel fournisseur, reportez-vous à la section Créer un centre de données virtuel fournisseur.

Lorsque vous créez un SDDC qui encapsule une instance de vCenter Server attachée, vous avez dédié l'instance de vCenter Server à un locataire. Cette instance de vCenter Server s'affiche comme étant publiée sur un locataire (et est également dite incluse dans la portée du locataire). Pour plus d'informations sur la création d'un SDDC, reportez-vous à la section Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys.

Note Par défaut, avec une instance de vCenter Server attachée, vous pouvez créer un VDC fournisseur ou une instance dédiée de vCenter Server. Si vous avez créé un VDC fournisseur soutenu par une instance de vCenter Server, vous ne pouvez pas utiliser cette instance de vCenter Server pour créer une instance dédiée de vCenter Server, et inversement.

Ce chapitre contient les rubriques suivantes :

- Ajout de ressources vCenter Server et NSX
- Ajout de ressources Cloud
- Afficher les instances de vCenter Server

- Modifier les paramètres vCenter Server
- Activer ou désactiver une instance de vCenter Server
- Reconnecter une instance de vCenter Server
- Actualiser une instance de vCenter Server
- Actualiser les stratégies de stockage d'une instance de vCenter Server
- Annuler l'enregistrement d'une instance de vCenter Server
- Modifier les paramètres de NSX Manager
- Modifier les paramètres de NSX-T Manager
- Supprimer une instance de NSX-T Manager
- Configuration et gestion de déploiements multisite
- Listes de ressources multisites

Ajout de ressources vCenter Server et NSX

vCloud Director dépend des ressources vSphere pour fournir un CPU, de la mémoire et un stockage afin d'exécuter des machines virtuelles. En outre, à partir de la version 9.7, vCloud Director peut agir comme un serveur HTTP entre les locataires et l'environnement vSphere sous-jacent.

Pour plus d'informations sur la configuration système requise de vCloud Director et sur les versions prises en charge de vCenter Server et ESXi, consultez les *matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Attacher une instance de vCenter Server seule ou avec une instance de NSX Manager

Vous pouvez attacher une instance de vCenter Server afin que ses ressources soient disponibles dans vCloud Director. Vous pouvez attacher une instance de vCenter Server uniquement avec son instance de NSX Manager associée. Pour les instances de vCenter Server dédiées ou pour celles associées à une instance de NSX-T Manager, vous pouvez attacher une instance de vCenter Server seule.

vCloud Director peut utiliser une instance de vCenter Server avec l'instance de NSX Manager qui lui est associée ou avec une instance de NSX-T Manager.

Si vous souhaitez que vCloud Director utilise cette instance de vCenter Server avec l'instance de NSX Manager qui lui est associée, vous devez attacher les instances de vCenter Server et de NSX Manager ensemble.

Si vous souhaitez que vCloud Director utilise cette instance de vCenter Server avec une instance de NSX-T Manager, vous devez attacher l'instance de vCenter Server seule. Après avoir attaché l'instance de vCenter Server seule, vous devez Enregistrer une instance de NSX-T Manager.

Note Après avoir attaché une instance de vCenter Server seule, vous ne pouvez pas ajouter l'instance de NSX Manager qui lui est associée ultérieurement. Vous pouvez annuler l'enregistrement et reconnecter l'instance de vCenter Server, ainsi que l'instance de NSX Manager qui lui est associée.

Vous pouvez attacher une instance de vCenter Server à n'importe quel site à partir de votre environnement vCloud Director.

Conditions préalables

- Si vous avez configuré vCloud Director pour vérifier les certificats SSO vCenter et vSphere, vérifiez que vous avez téléchargé les certificats vCenter Server vers vCloud Director. Pour plus d'informations sur les paramètres système généraux, reportez-vous à la section Modifier des paramètres système généraux.
- Si vous avez configuré vCloud Director pour vérifier les certificats NSX Manager, vérifiez que vous avez téléchargé les certificats NSX Manager vers vCloud Director. Pour plus d'informations sur les paramètres système généraux, reportez-vous à la section Modifier des paramètres système généraux.

Procédure

1 Ajouter l'instance de vCenter Server

   Pour ajouter une instance de vCenter Server, vous saisissez les détails d'accès du système vCenter Server.

2 (Facultatif) Ajouter l'instance de NSX Manager associée

   Si vous souhaitez que vCloud Director utilise cette instance de vCenter Server avec l'instance de NSX Manager qui lui est associée, vous devez ajouter les détails d'accès de NSX Manager.

Ajouter l'instance de vCenter Server

Pour ajouter une instance de vCenter Server, vous saisissez les détails d'accès du système vCenter Server.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le volet de gauche, cliquez sur **vCenter**, puis sur **Ajouter**.

3 Si vous disposez d'un déploiement de vCloud Directormultisite, dans le menu déroulant **Site**, sélectionnez le site auquel vous souhaitez ajouter cette instance de vCenter Server, puis cliquez sur **Suivant**.

4 Entrez le nom et, éventuellement, la description de l'instance de vCenter Server dans vCloud Director.

5 Entrez l'URL de l'instance de vCenter Server.

Si le port par défaut est utilisé, vous pouvez ignorer le numéro de port. Si un port personnalisé est utilisé, indiquez-en le numéro.

Par exemple, **`https://`***`Nom_de_domaine_complet_ou_adresse_IP`*`:<numéro_de_port_personnalisé>`.

6 Entrez le nom d'utilisateur et le mot de passe du compte d'**administrateur** vCenter Server.

7 (Facultatif) Pour désactiver l'instance de vCenter Server après l'enregistrement, désactivez le bouton bascule **Activé**.

8 Configurez l'URL du client Web vCenter Server.

Option	Description
Utiliser les services vSphere pour fournir l'URL	Pour utiliser cette option, vous devez utiliser l'API vCloud pour configurer vCloud Director afin d'utiliser le service de recherche vSphere.
URL de vSphere Web Client	Pour utiliser cette option, vous devez entrer l'URL de vSphere Web Client. Par exemple, **`https://example.vmware.com/vsphere-client`**.

9 Si vous souhaitez ajouter une instance de vCenter Server dédiée à un locataire qui ne sera pas utilisé comme VDC fournisseur, activez l'option **Activer l'accès locataire**.

10 Cliquez sur **Suivant**.

11 (Facultatif) Ignorez l'ajout de l'instance de NSX Manager associée à l'instance de vCenter Server et terminez l'enregistrement.

Si vous souhaitez que vCloud Director utilise cette instance de vCenter Server avec une instance de NSX-T Manager, vous devez ajouter l'instance de vCenter Server seule.

Note Vous ne pouvez pas ajouter l'instance de NSX Manager associée à une étape ultérieure. Vous pouvez annuler l'enregistrement et reconnecter l'instance de vCenter Server, ainsi que l'instance de NSX Manager qui lui est associée.

a Sur la page **Paramètres de NSX-V Manager**, désactivez le bouton bascule **Configurer les paramètres**, puis cliquez sur **Suivant**.

b Sur la page **Prêt à terminer**, vérifiez les détails de l'enregistrement et cliquez sur **Terminer**.

(Facultatif) Ajouter l'instance de NSX Manager associée

Si vous souhaitez que vCloud Director utilise cette instance de vCenter Server avec l'instance de NSX Manager qui lui est associée, vous devez ajouter les détails d'accès de NSX Manager.

Procédure

1 Sur la page **Paramètres de NSX-V Manager**, laissez le bouton bascule **Configurer les paramètres** activé.

2 Entrez l'URL de l'instance de NSX Manager.

Si le port par défaut est utilisé, vous pouvez ignorer le numéro de port. Si un port personnalisé est utilisé, indiquez-en le numéro.

Par exemple, **`https://`** ***`Nom_de_domaine_complet_ou_adresse_IP`*****`:<numéro_de_port_personnalisé>`**.

3 Entrez le nom d'utilisateur et le mot de passe du compte d'**administrateur** NSX.

4 (Facultatif) Pour activer la mise en réseau intercentre de données virtuel pour les centres de données virtuels dépendant de cette instance de vCenter Server, activez le bouton bascule **Mise en réseau inter-VDC** et saisissez les propriétés du déploiement de machines virtuelles de contrôle, ainsi qu'un nom pour l'étendue du fournisseur de réseau.

Les propriétés du déploiement de machines virtuelles de contrôle sont utilisées pour déployer un dispositif sur l'instance de NSX Manager pour la mise en réseau intercentre de données virtuel de composants, comme un routeur universel.

Option	Description
Chemin du pool de ressources	Chemin d'accès hiérarchique à un pool de ressources spécifique dans l'instance de vCenter Server, commençant par le cluster, *Cluster/Resource_Pool_Parent/Target_Resource* . Par exemple, **`TestbedCluster1/mgmt-rp`**. Vous pouvez également entrer l'ID de la référence d'objet géré du pool de ressources. Par exemple, **`resgroup-1476`**.
Nom de la banque de données	Nom de la banque de données permettant d'héberger les fichiers du dispositif. Par exemple, **`shared-disk-1`**.
Interface de gestion	Nom du réseau dans vCenter Server ou groupe de ports utilisé pour l'interface de gestion du DLR HA. Par exemple, **`TestbedPG1`**.
Étendue du fournisseur de réseau	Correspond au domaine d'erreur de réseau dans les topologies réseau des groupes de centres de données. Par exemple, **`boston-fault1`**. Pour plus d'informations sur la gestion des groupes entre centres de données virtuels, reportez-vous au *Guide du portail de locataires de vCloud Director*.

5 Sur la page **Prêt à terminer**, vérifiez les détails de l'enregistrement et cliquez sur **Terminer**.

Étape suivante

- Attribuer la clé de licence NSX dans vCenter Server.
- Créer un centre de données virtuel fournisseur.

Découverte et adoption de vApp

Dans la configuration par défaut, un VDC d'organisation découvre les machines virtuelles créées sur un pool de ressources vCenter Server soutenant le VDC. Le système construit un vApp simplifié, appartenant à l'administrateur système, afin qu'il contienne chaque machine virtuelle découverte. Une fois que l'administrateur système vous accorde l'accès à un vApp découvert, vous pouvez référencer la machine virtuelle dans celui-ci lorsque vous composez ou recomposez un vApp, ou lorsque vous modifiez le vApp pour l'adopter et l'importer.

Les vApp découverts contiennent exactement une machine virtuelle et sont soumis à plusieurs contraintes qui ne s'appliquent pas aux vApp créés dans vCloud Director. Que vous les adoptiez ou non, ceux-ci peuvent être utiles en tant que source de machines virtuelles à utiliser lors de la composition ou recomposition d'un vApp.

Chaque vApp découvert bénéficie d'un nom qui est dérivé du nom de la machine virtuelle vCenter qu'il contient et d'un préfixe spécifié par l'administrateur de votre organisation.

Si vous souhaitez découvrir d'autres vApp, un administrateur système peut utiliser l'API vCloud pour créer des VDC d'organisation qui adoptent des pools de ressources spécifiés disponibles auprès d'un VDC fournisseur. vCenter Les machines virtuelles de ces pools de ressources adoptés apparaissent dans le nouveau VDC en tant que vApp découverts et sont des candidats pour une adoption.

Note Les machines virtuelles avec des disques durs IDE sont découvertes uniquement si elles sont hors tension.

Si une ou plusieurs machines virtuelles vCenter ne sont pas découvertes par vCloud Director, vous pouvez examiner les raisons possibles en déboguant la découverte de machines virtuelles de vCenter Server. Pour plus d'informations, consultez le *Guide d'installation, de configuration et de mise à niveau de vCloud Director*.

Activation de la découverte de machines virtuelles

La découverte de machines virtuelles est activée par défaut. Pour désactiver la détection de machines virtuelles, un administrateur système doit décocher la case **Découverte de VM activée** dans l'onglet **Paramètres système > Général**. Un administrateur d'organisation peut utiliser l'API vCloud pour désactiver la découverte de machines virtuelles pour les VDC individuels ou pour tous les VDC d'une organisation.

Utilisation d'une machine virtuelle à partir d'un vApp découvert

Lorsque l'administrateur système vous accorde l'accès à un vApp découvert, vous pouvez utiliser sa machine virtuelle de la même manière qu'une machine virtuelle que contient un autre vApp ou modèle de vApp. Par exemple, vous pouvez lui spécifier à quel moment vous construisez un nouveau vApp. Vous pouvez également cloner un vApp découvert ou modifier son nom, sa description ou ses paramètres de bail sans déclencher le processus d'adoption.

Adoption d'un vApp découvert

Vous pouvez adopter un vApp découvert en modifiant son réseau vApp ou en ajoutant une machine virtuelle à ce vApp. Une fois que vous avez adopté un vApp découvert, le système l'importe et le traite comme s'il avait été créé dans vCloud Director. Lorsqu'un vApp adopté est récupéré avec une demande d'API vCloud, il inclut un élément nommé `autoNature`. Cet élément a la valeur `false` si le vApp découvert a été adopté ou créé dans vCloud Director. Vous ne pouvez pas restaurer un vApp adopté vers un vApp découvert.

Si vous supprimez ou déplacez la machine virtuelle que contient un vApp découvert, le système supprime également le vApp qui la contient. Ce comportement ne s'applique pas aux vApp adoptés.

Le vApp créé pour contenir une machine virtuelle vCenter découverte est semblable à celui créé lorsque vous importez manuellement une machine virtuelle en tant que vApp, mais il est simplifié et il se peut que vous soyez amené à le modifier avant de pouvoir le déployer dans votre VDC. Par exemple, vous devrez modifier ses propriétés de mise en réseau et de stockage, et effectuer d'autres ajustements spécifiques aux besoins de votre organisation.

Note L'adoption d'une machine virtuelle ne conserve pas ses paramètres de réservation, de limite et de parts qui sont configurés dans vCenter Server. Les machines virtuelles importées reçoivent leurs paramètres d'allocation de ressources du centre de données virtuel d'organisation sur lequel elles résident.

Attribuer la clé de licence NSX dans vCenter Server

Si vous avez attaché une instance de vCenter Server, ainsi que l'instance de NSX Manager qui lui est associée, vous devez utiliser le client vSphere pour attribuer une clé de licence pour l'instance de NSX Manager qui prend en charge la mise en réseau vCloud Director.

Conditions préalables

Cette opération est limitée aux administrateurs système.

Procédure

1. Depuis un client vSphere qui est connecté au système vCenter Server, sélectionnez **Accueil > Licences**.
2. Pour la vue de rapport, sélectionnez **Actif**.
3. Cliquez avec le bouton droit de la souris sur l'actif NSX Manager et sélectionnez **Changer la clé de licence**.
4. Sélectionnez **Affecter une nouvelle clé de licence** et cliquez sur **Entrer clé**.
5. Saisissez la clé de licence, saisissez une étiquette facultative pour la clé, et cliquez sur **OK**.

   Utilisez la clé de licence NSX Manager que vous avez reçu lorsque vous avez acheté vCloud Director. Vous pouvez utiliser cette clé de licence dans plusieurs instances de vCenter Server.
6. Cliquez sur **OK**.

Enregistrer une instance de NSX-T Manager

Vous pouvez enregistrer une instance de NSX-T Manager avec vCloud Director, afin que vCloud Director puisse utiliser ses ressources réseau. Un centre de données virtuel fournisseur peut utiliser des ressources réseau de NSX Data Center for vSphere ou de NSX-T Data Center.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **NSX-T Manager**, puis sur **Ajouter**.
3. Si vous disposez d'un déploiement de vCloud Directormultisite, dans le menu déroulant **Site**, sélectionnez le site auquel vous souhaitez ajouter cette instance de NSX-T Manager, puis cliquez sur **Suivant**.
4. Entrez le nom et, éventuellement, la description de l'instance de NSX-T Manager dans vCloud Director.
5. Entrez l'URL de l'instance de NSX-T Manager.

   Par exemple, **`https://`***`nom_de_domaine_complet_ou_adresse_IP`*.
6. Entrez le nom d'utilisateur et le mot de passe du compte d'**administrateur**NSX-T Manager.
7. Cliquez sur **Enregistrer**.

Étape suivante

Pour plus d'informations sur la création d'un centre de données virtuel fournisseur dépendant de NSX-T Data Center, consultez le *Guide de programmation de vCloud API pour fournisseurs de services* sur le site https://code.vmware.com.

Ajout de ressources Cloud

Les ressources Cloud constituent une abstraction de leurs ressources vSphere sous-jacentes et fournissent les ressources en calcul et en mémoire pour les machines virtuelles vCloud Director et les vApp, ainsi qu'un accès au stockage et à la connectivité du réseau.

Les ressources de cloud incluent des centres de données virtuels de fournisseur et d'organisation, des réseaux externes, des réseaux de centres de données virtuels d'organisation et des pools de réseaux. Avant de pouvoir ajouter des ressources Cloud à vCloud Director, vous devez ajouter des ressources vSphere.

Pour plus d'informations sur les centres de données virtuels d'organisation, consultez le Chapitre 6 Gestion des centres de données virtuels d'organisation.

Pour plus d'informations sur les réseaux de centres de données virtuels d'organisation, reportez-vous au chapitre *Gestion de réseaux de centres de données virtuels d'organisation* dans le *Guide du portail de locataires de vCloud Director*.

vCloud Director 9.7 introduit le SDDC ou instance de vCenter Server dédiée en tant que ressource cloud qui encapsule une installation de vCenter Server complète. Le fournisseur peut créer et activer une instance de vCenter Server dédiée, la publier vers des locataires, et créer et activer des proxys vers différents composants de l'environnement vSphere sous-jacent. Pour créer, publier vers des locataires et gérer des instances et des proxys vCenter Server, vous pouvez utiliser Service Provider Admin Portal ou vCloud OpenAPI. Consultez le Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys ou la section *Démarrage de vCloud OpenAPI* à l'adresse https://code.vmware.com.

Centres de données virtuels fournisseur

Un centre de données virtuel (VDC) fournisseur combine les ressources de calcul et de mémoire de pools de ressources de vCenter Server aux ressources de stockage d'une ou de plusieurs stratégies de stockage issues d'une instance unique de vCenter Server. Pour les ressources réseau, un VDC fournisseur peut utiliser NSX Data Center for vSphere ou NSX-T Data Center.

- Vous pouvez créer et gérer un VDC fournisseur reposant sur une instance attachée de vCenter Server et son instance associée de NSX Manager à l'aide de Service Provider Admin Portal ou de l'API vCloud.
- Vous pouvez créer et gérer un VDC fournisseur reposant sur une instance attachée de vCenter Server et une instance de NSX-T Manager à l'aide de Service Provider Admin Portal ou de l'API vCloud.

Un système vCloud Director typique inclut plusieurs VDC fournisseur configurés pour répondre à différentes exigences de niveau de service. Chaque VDC fournisseur dispose d'un pool de ressources principal. Vous pouvez ajouter et supprimer des pools de ressources non principaux depuis l'instance de sauvegarde de vCenter Server. Vous ne pouvez pas supprimer le pool de ressources principal.

Créer un centre de données virtuel fournisseur

Pour mettre les ressources de calcul, de mémoire et de stockage vSphere à la disposition de vCloud Director, vous créez un centre de données virtuel (VDC) fournisseur.

Pour qu'une organisation puisse commencer à déployer des machines virtuelles ou à créer des catalogues, l'**administrateur système** doit créer un VDC fournisseur et les VDC d'organisation qui consomment ses ressources. La relation entre les VDC fournisseur et les VDC d'organisation qu'ils prennent en charge est une décision administrative qui repose sur l'étendue de vos offres de service, la capacité et la répartition géographique de votre infrastructure vSphere, ainsi que sur d'autres éléments à prendre en compte. Étant donné qu'un VDC fournisseur restreint la capacité et les services de vSphere accessibles par les locataires, les **administrateurs système** créent généralement des VDC fournisseur qui fournissent différentes classes de service, en fonction de mesures telles que les performances, la capacité et les fonctionnalités. Les locataires peuvent ensuite être provisionnés avec des VDC d'organisation qui fournissent des classes spécifiques de service définies par la configuration du VDC fournisseur de sauvegarde.

Avant de créer un VDC fournisseur, évaluez l'ensemble de fonctionnalités vSphere que vous prévoyez de proposer à vos locataires. Certaines de ces capacités peuvent être mises en œuvre dans le pool de ressources principal du VDC fournisseur. D'autres peuvent nécessiter la création de pools de ressources supplémentaires basés sur des clusters vSphere spécialement configurés et les ajouter au VDC comme décrit dans Ajouter un pool de ressources à un centre de données virtuel fournisseur.

La plage des versions d'ESXi installées sur les hôtes du cluster sur lesquels repose un pool de ressources détermine l'ensemble des systèmes d'exploitation invités et versions de matériel virtuel disponibles pour les machines virtuelles déployées dans les VDC d'organisation reposant sur le VDC fournisseur.

Conditions préalables

- Connectez-vous à Service Provider Admin Portal en tant qu'**administrateur système**.
- Vérifiez que vous avez créé le pool de ressources principal cible avec une capacité disponible dans un cluster configuré pour utiliser le DRS automatisé. Vous pouvez utiliser un pool de ressources pour un seul VDC fournisseur. Pour créer un pool de ressources, vous pouvez utiliser vSphere Client.

  Si vous prévoyez d'utiliser un pool de ressources faisant partie d'un cluster utilisant vSphere High Availability (HA), vous devez savoir comment vSphere HA calcule la taille d'emplacement. Pour plus d'informations sur les tailles d'emplacement et la personnalisation du comportement de vSphere HA, consultez le *Guide de disponibilité vSphere*.
- Si vous utilisez NSX Data Center for vSphere pour les ressources réseau du VDC fournisseur :
  - Vérifiez que l'instance de vCenter Server qui contient le pool de ressources principal cible est attachée et dispose d'une clé de licence NSX Data Center for vSphere.
  - Configurer l'infrastructure VXLAN dans NSX Manager. Consultez le *Guide d'administration de NSX* concerné.

    Si vous souhaitez utiliser un pool de réseaux VXLAN personnalisé dans ce VDC fournisseur (plutôt que le pool de réseaux VXLAN par défaut), créez maintenant ce pool de réseaux. Reportez-vous à Créez un pool de réseaux reposant sur une zone de transport NSX Data Center for vSphere..
- Si vous utilisez NSX-T Data Center pour les ressources réseau du VDC fournisseur :
  - Ajouter un réseau externe reposant sur un routeur logique de niveau 0 NSX-T Data Center
  - Créez un pool de réseaux reposant sur une zone de transport NSX-T Data Center.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.

3 Cliquez sur **Nouveau**.

4 Si vous disposez d'un déploiement de vCloud Director multisite, dans le menu déroulant **Site**, sélectionnez le site auquel vous souhaitez ajouter cette instance de VDC fournisseur, puis cliquez sur **Suivant**.

5 Entrez le nom du VDC fournisseur et, éventuellement, une description.

Vous pouvez utiliser ces zones de texte afin d'indiquer les fonctionnalités vSphere disponibles pour les VDC d'organisation sauvegardés par ce VDC fournisseur. Par exemple, **vSphere HA** ou les **stratégies de stockage disposant de la prise en charge d'IOPS.**

6 (Facultatif) Pour activer le VDC fournisseur lors de la création, activez l'option **État**.

Vous ne pouvez pas utiliser les ressources de calcul et de stockage d'un VDC désactivé pour la création d'un VDC d'organisation.

7 Cliquez sur **Suivant**.

8 Sélectionnez une instance de vCenter Server pour fournir des pool de ressources au VDC fournisseur, puis cliquez sur **Suivant**.

Cette page répertorie les instances de vCenter Server enregistrées dans vCloud Director. Cliquez sur une instance de vCenter Server pour en afficher les pools de ressources disponibles.

9 Sélectionnez un pool de ressources à utiliser comme pool de ressources principal pour ce VDC fournisseur.

Vous pouvez utiliser un pool de ressources pour un VDC fournisseur. Lorsque vous ajoutez un pool de ressources à un VDC fournisseur, ce pool de ressources et sa chaîne parente ne peuvent plus être sélectionnés pour d'autres VDC fournisseur.

10 Sélectionnez la version de matériel virtuel la plus élevée que vous souhaitez que le VDC fournisseur prenne en charge, puis cliquez sur **Suivant**.

Le système détermine la version de matériel virtuel la plus haute prise en charge par tous les hôtes du cluster qui soutient le pool de ressources et il la propose comme valeur par défaut dans le menu déroulant **Version du matériel la plus haute prise en charge**. Vous pouvez utiliser cette valeur par défaut ou sélectionner une version de matériel antérieure dans le menu. La version que vous spécifiez devient la version du matériel virtuel la plus haute disponible pour une machine virtuelle déployée dans un VDC d'organisation reposant sur ce VDC fournisseur. Si vous sélectionnez une version de matériel virtuel antérieure,

certains systèmes d'exploitation invités risquent de ne pas être pris en charge sur ces machines virtuelles. Une fois que vous avez créé le VDC fournisseur avec la version matérielle sélectionnée, vous pouvez uniquement mettre à niveau la version, mais vous ne pouvez pas la rétrograder.

Note La version matérielle disponible pour le VDC fournisseur dépend de la version la plus élevée disponible de l'hôte ESXi dans le cluster cible. Si la version matérielle prise en charge la plus élevée de l'hôte ESXi n'est pas disponible pour la sélection, vérifiez dans vSphere Client que la compatibilité par défaut pour la création de machine virtuelle sur le centre de données est définie sur **`Utiliser le paramètre de centre de données et la version d'hôte`**. Vous pouvez également définir le paramètre de compatibilité par défaut sur la version matérielle la plus élevée souhaitée pour le cluster.

La version du matériel de machine virtuelle la plus haute prise en charge dans vCloud Director 10.0 est la version 14.

11 Sélectionnez une ou plusieurs stratégies de stockage pour le VDC fournisseur, puis cliquez sur **Suivant**.

Toutes les stratégies de stockage vSphere prises en charge par le pool de ressources que vous avez sélectionné sont répertoriées.

Important vCloud Director ne prend pas en charge les stratégies de stockage de machine virtuelle pour les services de données basés sur un hôte, comme le chiffrement et Storage I/O Control.

12 Configurez le pool de réseaux pour ce VDC fournisseur.

Chaque VDC fournisseur doit disposer d'un pool de réseaux. Vous pouvez demander au système d'en créer un avec une étendue par défaut ou utiliser un VXLAN personnalisé basé sur une instance spécifique de NSX Data Center for vSphere ou un pool Geneve basé sur une zone de transport NSX-T Data Center.

Option	Description
Créer un pool de réseaux VXLAN par défaut	Le système crée un pool VXLAN pour ce VDC fournisseur.
Sélectionner un pool de réseaux VXLAN dans la liste	Vous sélectionnez un pool de réseaux dans une liste pour utiliser un pool VXLAN personnalisé basé sur une zone de transport NSX spécifique.
Sélectionner une instance de NSX-T Manager et un pool de réseaux Geneve	Vous sélectionnez un pool de réseaux dans une liste pour utiliser un pool VXLAN personnalisé reposant sur une zone de transport NSX-T Data Center.

13 Vérifiez vos choix et cliquez sur **Terminer** pour créer le VDC fournisseur.

Étape suivante

Vous pouvez ajouter des pools de ressources secondaires qui permettent au VDC fournisseur de fournir des fonctionnalités spécialisées (par exemple, des clusters Edge, des groupes d'affinité et des hôtes à configuration spéciale) dont certaines organisations peuvent avoir besoin. Reportez-vous à la section Ajouter un pool de ressources à un centre de données virtuel fournisseur.

Réseaux externes

Un réseau externe vCloud Director fournit une interface de liaison montante qui connecte des réseaux et des machines virtuelles dans le système à un réseau à l'extérieur du système, comme un VPN, un intranet d'entreprise ou l'Internet public. Seul un **administrateur système** peut créer un réseau externe.

Si vous disposez de plusieurs instances de vCenter Server enregistrées sur le système, vous pouvez créer plusieurs réseaux externes, chacun reposant sur un réseau vSphere ou un routeur logique de niveau 0.

vCloud Director prend en charge les réseaux externes IPv4 et IPv6.

Note La plage d'adresses IP que vous définissez lors de la création du réseau externe est allouée à une passerelle Edge ou aux machines virtuelles connectées directement à ce réseau. De ce fait, les adresses IP ne doivent pas être utilisées en dehors de vCloud Director.

Réseaux externes reposant sur des réseaux vSphere

Les réseaux externes peuvent reposer sur un réseau vSphere unique ou sur plusieurs réseaux vSphere.

- Réseaux externes reposant sur une seule instance de vSphere.

  Pour fournir à chaque consommateur du réseau externe un ensemble d'adresses IP qui ne se chevauchent pas sur le réseau vSphere, **l'administrateur système** doit configurer les plages d'adresses IP sur le VLAN sous-jacent manuellement.

- Réseaux externes reposant sur plusieurs réseaux vSphere.

  Un réseau externe peut reposer sur plusieurs réseaux vSphere. Cette approche peut simplifier la gestion des adresses IP dans vCloud Director. Vous pouvez modifier les propriétés d'un réseau externe pour modifier les sauvegardes de son réseau.

  Ce type de réseau présente plusieurs contraintes.

  - Le réseau doit comporter au maximum un réseau vSphere de sauvegarde sur chaque instance de vCloud Director enregistrée sur le système.
  - Les commutateurs réseau de soutien doivent tous être du même type, commutateur vSphere Distributed Switch ou commutateur standard.

Réseaux externes reposant sur un routeur logique de niveau 0

Un réseau externe peut reposer sur un routeur logique NSX-T Data Center de niveau 0.

Ajouter un réseau externe reposant sur des ressourcesvSphere

En ajoutant un réseau externe, vous pouvez enregistrer des ressources réseau vSphere qui seront utilisées par vCloud Director. Vous pouvez créer des réseaux de VDC d'organisation qui se connectent à un réseau externe.

Vous pouvez ajouter un réseau externe IPv4 ou IPv6. Un réseau externe IPv6 prend en charge les sous-réseaux IPv4 et IPv6, et un réseau externe IPv4 prend en charge les sous-réseaux IPv4 et IPv6.

Conditions préalables

Vérifiez qu'un groupe de ports vSphere est disponible avec ou sans jonction VLAN. Des groupes de ports élastiques avec liaison de port statique garantissent des performances optimales.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **Réseaux externes**, puis sur **Nouveau**.
3. Sélectionnez **Ressources vSphere**, sélectionnez le type de groupes de ports sur lequel reposera le réseau, puis cliquez sur **Suivant**.
4. Entrez un nom et une description facultative pour le nouveau réseau externe.
5. Sélectionnez les groupes de ports sur lesquels reposera le réseau externe, puis cliquez sur **Suivant**.
6. Configurez au moins un sous-réseau et cliquez sur **Suivant**.
   a. Pour ajouter un sous-réseau, cliquez sur **Ajouter**.
   b. Entrez les paramètres CIDR (Classless Inter-Domain Routing) du réseau.

      Utilisez le format *adresse_IP_de_passerelle_réseau/longueur_préfixe_de_sous-réseau*, par exemple, **`192.167.1.1/24`**.
   c. (Facultatif) Entrez les paramètres DNS.
   d. Configurez un pool d'adresses IP statiques en ajoutant au moins une plage d'adresses IP ou une adresse IP.
   e. Cliquez sur **OK**.
   f. (Facultatif) Pour ajouter un autre sous-réseau, répétez cette étape.
7. Passez les paramètres du réseau en revue et cliquez sur **Terminer**.

Étape suivante

Vous pouvez créer un réseau VDC d'organisation qui se connecte à un réseau externe.

Ajouter un réseau externe reposant sur un routeur logique de niveau 0 NSX-T Data Center

Pour enregistrer des ressources réseau NSX-T Data Center pour une utilisation par vCloud Director, ajoutez un réseau externe reposant sur un routeur logique de niveau 0.

Procédure

1 Créez un routeur logique de niveau 0.

- Créez le routeur de niveau 0 dans NSX-T Manager.
  a Connectez-vous avec des privilèges administratifs à l'instance de NSX-T Manager.
  b Cliquez sur **Mise en réseau**, sur **Passerelles de niveau 0**, puis sur **Ajouter la passerelle de niveau 0**.
  c Entrez un nom pour le routeur de niveau 0.
  d Sélectionnez un mode de haute disponibilité.

  Note Par défaut, le mode actif-actif est utilisé. En mode actif-actif, la charge du trafic est équitablement répartie entre tous les membres. En mode actif-veille, le trafic est traité par un membre actif choisi. Si le membre actif échoue, un nouveau membre devient actif.

  e Sélectionnez un cluster Edge NSX-T existant dans le menu déroulant sur lequel reposera le routeur logique de niveau 0, puis cliquez sur **Enregistrer**.
- Créez le routeur logique de niveau 0 à l'aide de l'API NSX Policy.

2 Connectez-vous à vCloud Director Service Provider Admin Portal.

3 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

4 Dans le volet de gauche, cliquez sur **Réseaux externes**, puis sur **Nouveau**.

5 Sélectionnez **Ressources NSX-T (routeur de niveau 0)**, sélectionnez une instance enregistrée de NSX-T Manager sur laquelle reposera le réseau, puis cliquez sur **Suivant**.

6 Entrez un nom et une description facultative pour le nouveau réseau externe.

7 Sélectionnez un routeur de niveau 0 à connecter au réseau externe, puis cliquez sur **Suivant**.

8 Configurez au moins un sous-réseau et cliquez sur **Suivant**.
  a Pour ajouter un sous-réseau, cliquez sur **Ajouter**.
  b Entrez les paramètres CIDR (Classless Inter-Domain Routing) du réseau.
  c (Facultatif) Entrez les paramètres DNS.
  d Configurez un pool d'adresses IP statiques en ajoutant au moins une plage d'adresses IP ou une adresse IP.

e Cliquez sur **OK**.

f (Facultatif) Pour ajouter un autre sous-réseau, répétez les étapes 8.a à 8.e.

9 Passez les paramètres du réseau en revue et cliquez sur **Terminer**.

Étape suivante

Utilisez le routeur de niveau 0 pour créer une liaison montante vers le réseau externe.

Pools de réseaux

Un pool de réseaux est un groupe de réseaux non différenciés, disponible dans un VDC d'organisation pour créer des réseaux vApp et certains types de réseaux VDC d'organisation.

Un pool de réseaux repose sur les ressources réseau de vSphere telles que les ID de VLAN ou les groupes de ports, les ressources de NSX Data Center for vSphere ou les ressources de NSX-T Data Center.

vCloud Director utilise des pools de réseaux pour créer des réseaux VDC d'organisation internes ou routés par NAT et tous les réseaux vApp. Le trafic réseau sur chaque réseau dans un pool est isolé à la couche 2 de tous les autres réseaux.

Chaque VDC d'organisation dans vCloud Director peut disposer d'un pool de réseaux. Plusieurs VDC d'organisation peuvent partager le même pool de réseaux. Le pool de réseaux d'un VDC d'organisation fournit les réseaux créés pour répondre au quota de réseaux d'un VDC d'organisation.

Pools de réseaux VXLAN

Chaque VDC fournisseur reposant sur NSX Data Center for vSphere inclut un pool de réseaux VXLAN.

Lorsque vous créez un VDC fournisseur reposant sur NSX Data Center for vSphere, vous pouvez associer ce VDC fournisseur à un pool de réseaux VXLAN existant ou vous pouvez créer un pool de réseaux VXLAN pour le VDC fournisseur.

Un pool de réseaux VXLAN récemment créé obtient un nom dérivé du nom du VDC fournisseur conteneur qui lui est affecté au moment de la création. Vous ne pouvez pas supprimer ou modifier ce pool de réseaux. Si vous renommez un VDC fournisseur, son pool de réseaux VXLAN est automatiquement renommé.

Note Pour garantir des performances de réseau optimales dans votre infrastructure, créez un pool de réseaux VXLAN et associez-le à tous vos VDC fournisseurs lors de leur création.

Les réseaux VXLAN de vCloud Director sont basés sur la norme IETF VXLAN et offrent divers avantages.

- Des réseaux logiques étendant des limites de couche 3
- Des réseaux logiques étendant plusieurs racks sur une seule couche 2
- Imbrication de diffusion

- Meilleures performances
- Plus grande échelle (jusqu'à 16 millions d'adresses réseau)

Pour plus d'informations sur les réseaux VXLAN dans un environnement vCloud Director, consultez le *Guide d'administration de NSX*.

Créez un pool de réseaux reposant sur une zone de transport NSX Data Center for vSphere.

Pour enregistrer une zone de transport NSX Data Center for vSphere en vue d'une utilisation par vCloud Director, ajoutez un pool de réseaux reposant sur VXLAN.

Conditions préalables

Créez une zone de transport NSX Data Center for vSphere sur n'importe quelle instance de vCenter Server enregistrée dans vCloud Director. Consultez le *Guide d'administration de NSX*.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Pools de réseaux**, puis sur **Nouveau**.
3. Entrez un nom et, éventuellement, une description pour le nouveau pool de réseaux, puis cliquez sur **Suivant**.
4. Sélectionnez **Reposant sur VXLAN** et cliquez sur **Suivant**.
5. Sélectionnez une instance de vCenter Server pour spécifier la zone de transport VXLAN à utiliser par ce pool de réseaux, puis cliquez sur **Suivant**.
6. Sélectionnez une zone de transport de NSX Data Center for vSphere sur laquelle reposera le nouveau pool de réseaux, puis cliquez sur **Suivant**.

   Note Afin de créer un pool de réseaux universel pour la mise en réseau entre centres de données virtuels, sélectionnez une zone de transport de type UNIVERSAL_VXLAN.
7. Passez les paramètres du pool de réseaux en revue et cliquez sur **Terminer**.

Étape suivante

Créez un réseau VDC d'organisation reposant sur un pool de réseaux ou associez le pool de réseaux à un VDC d'organisation et créez des réseaux vApp.

Pools de réseaux Geneve

Chaque VDC fournisseur reposant sur NSX-T Data Center inclut un pool de réseaux Geneve.

Geneve est la norme de virtualisation réseau qui fournit la capacité de superposition dans NSX-T Data Center.

Lorsque vous créez un VDC fournisseur reposant sur NSX-T Data Center, vous pouvez associer ce VDC fournisseur à un pool de réseaux Geneve existant ou vous pouvez créer un pool de réseaux Geneve pour le VDC fournisseur.

Les réseaux vCloud Director Geneve offrent un certain nombre d'avantages.

- Des réseaux logiques étendant des limites de couche 3
- Des réseaux logiques étendant plusieurs racks sur une seule couche 2
- Imbrication de diffusion
- Meilleures performances
- Plus grande échelle (jusqu'à 16 millions d'adresses réseau)

Créez un pool de réseaux reposant sur une zone de transport NSX-T Data Center.

Pour enregistrer une zone de transport NSX-T Data Center pour une utilisation par vCloud Director, créez un pool de réseaux reposant sur Geneve.

Conditions préalables

Créez une zone de transport NSX-T Data Center qui repose sur la superposition. Pour plus d'informations sur la création de la zone de transport et l'encapsulation générique de virtualisation du réseau, appelée superposition Geneve, reportez-vous à la *documentation du produit NSX-T Data Center*.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Pools de réseaux**, puis sur **Nouveau**.
3. Entrez un nom et, éventuellement, une description pour le nouveau pool de réseaux, puis cliquez sur **Suivant**.
4. Sélectionnez **Reposant sur Geneve** et cliquez sur **Suivant**.
5. Sélectionnez une instance de NSX-T Manager pour fournir la zone de transport pour ce pool de réseaux, puis cliquez sur **Suivant**.
6. Sélectionnez une zone de transport NSX-T et cliquez sur **Suivant**.
7. Passez les paramètres du pool de réseaux en revue et cliquez sur **Terminer**.

Étape suivante

Créez un réseau VDC d'organisation reposant sur un pool de réseaux ou associez le pool de réseaux à un VDC d'organisation et créez des réseaux vApp.

Créer un pool de réseaux dépendant d'ID de VLAN

Pour enregistrer des ID de VLAN vSphere pour une utilisation par vCloud Director, ajoutez un pool de réseaux reposant sur un VLAN. Un pool de réseaux reposant sur un VLAN garantit la sécurité, l'évolutivité et les performances des réseaux VDC d'organisation.

Conditions préalables

Vérifiez qu'une plage d'ID de VLAN et un commutateur distribué vSphere sont disponibles dans vSphere. Les ID de VLAN doivent être des ID valides, configurés dans le commutateur physique auquel les serveurs ESXi sont connectés.

Attention Les VLAN doivent être isolés à la couche de niveau 2. Une isolation incorrecte des VLAN peut entraîner une interruption sur le réseau.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Pools de réseaux**, puis sur **Nouveau**.
3. Entrez un nom et, éventuellement, une description pour le nouveau pool de réseaux, puis cliquez sur **Suivant**.
4. Cliquez sur **Reposant sur le VLAN**, puis sur **Suivant**.
5. Sélectionnez une instance de vCenter Server pour spécifier le commutateur virtuel distribué à utiliser par ce pool de réseaux, puis cliquez sur **Suivant**.
6. Entrez une plage d'ID de VLAN et cliquez sur **Suivant**.
7. Sélectionnez un commutateur distribué pour le pool de réseaux, puis cliquez sur **Suivant**.
8. Passez les paramètres du pool de réseaux en revue et cliquez sur **Terminer**.

Étape suivante

Créez un réseau VDC d'organisation reposant sur un pool de réseaux ou associez le pool de réseaux à un VDC d'organisation et créez des réseaux vApp.

Créer un pool de réseaux reposant sur des groupes de ports vSphere

Pour enregistrer des groupes de ports vSphere pour une utilisation par vCloud Director, ajoutez un pool de réseaux reposant sur des groupes de ports. Contrairement aux autres types de pools de réseaux, un pool de réseaux reposant sur un groupe de ports ne nécessite pas de commutateur distribué vSphere et peut prendre en charge les groupes de ports associés à des commutateurs distribués tiers.

Attention Les groupes de ports doivent être isolés de tous les autres groupes de ports à la couche 2. Les groupes de ports doivent être isolés physiquement ou à l'aide de balises de VLAN. Une isolation incorrecte des groupes de ports peut entraîner une interruption du réseau.

Conditions préalables

Vérifiez qu'un ou plusieurs groupes de ports sont disponibles dans votre environnement vSphere. Les groupes de ports doivent être disponibles sur chaque hôte ESXi du cluster, et chaque groupe de ports doit utiliser un VLAN unique. Les groupes de ports avec ou sans jonction VLAN sont pris en charge.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Pools de réseaux**, puis sur **Nouveau**.
3. Entrez un nom et, éventuellement, une description pour le nouveau pool de réseaux, puis cliquez sur **Suivant**.
4. Sélectionnez **Dépendant d'un groupe de ports** et cliquez sur **Suivant**.
5. Sélectionnez une instance de vCenter Server pour fournir les groupes de ports qui seront utilisés par ce pool de réseaux, puis cliquez sur **Suivant**.
6. Sélectionnez un ou plusieurs groupes de ports et cliquez sur **Suivant**.

   Vous pouvez créer un réseau pour chaque groupe de ports.
7. Passez les paramètres du pool de réseaux en revue et cliquez sur **Terminer**.

Étape suivante

Créez un réseau VDC d'organisation reposant sur un pool de réseaux ou associez le pool de réseaux à un VDC d'organisation et créez des réseaux vApp.

Afficher les instances de vCenter Server

Vous pouvez afficher une liste des instances de vCenter Server sur tous les sites de votre installation de vCloud Director. Vous pouvez voir comment vCloud Director utilise chaque instance de vCenter Server.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**.

Résultats

Une liste de toutes les instances de vCenter Server attachées s'affiche. La liste contient les informations suivantes pour chaque instance de vCenter Server.

	Description
Nom	Nom de l'instance de vCenter Server dans vCloud Director.
État	L'état de l'instance de vCenter Server peut être normal, avertissement et critique.
État	Activé ou désactivé. Reportez-vous à Activer ou désactiver une instance de vCenter Server.
Connexion	Connectée ou non à vCloud Director. Reportez-vous à Reconnecter une instance de vCenter Server.

	Description
Hôte de VC	Nom de domaine complet de l'instance de vCenter Server.
Version	La version de vCenter Server.
Utilisation	Les instances dédiées de vCenter Server ont activé l'accès du locataire. Le fournisseur peut utiliser différents pools de ressources d'une instance partagée de vCenter Server sur plusieurs VDC fournisseur, puis allouer ces pools de ressources à différents locataires. Reportez-vous à la section Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys.
Santé du cluster	Agrégation de la santé de tous les clusters dans l'instance de vCenter Server. Lors de l'agrégation de la santé du cluster, la santé du cluster le moins sain s'affiche.
Clusters	Nombre de clusters dans l'instance de vCenter Server.
VM	Nombre de machines virtuelles dans l'instance de vCenter Server.
VM en cours d'exécution	Nombre de machines virtuelles en cours d'exécution dans l'instance de vCenter Server.
CPU	Quantité de CPU virtuel activement utilisée en pourcentage du CPU vCenter Server disponible total.
Mémoire	Quantité de mémoire virtuelle activement utilisée sous la forme d'un pourcentage de la mémoire vCenter Server totale disponible.
Stockage	Quantité de stockage virtuel activement utilisée en pourcentage de stockage vCenter Server total disponible.

Modifier les paramètres vCenter Server

Si les informations de connexion d'une instance de vCenter Server attachée sont modifiées, ou si vous souhaitez modifier son nom ou sa description dans vCloud Director, vous pouvez en modifier les paramètres.

Vous pouvez modifier les paramètres configurés lors de l'ajout de l'instance de vCenter Server. Reportez-vous à Ajouter l'instance de vCenter Server.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**, puis sur le nom de l'instance de vCenter Server que vous souhaitez modifier.
3. Dans le coin supérieur droit de la section **Infos vCenter**, cliquez sur **Modifier**.
4. Modifiez les paramètres de vCenter Server, puis cliquez sur **Enregistrer**.

Étape suivante

Si vous avez modifié les informations de connexion, vous devez Reconnecter une instance de vCenter Server.

Activer ou désactiver une instance de vCenter Server

Avant d'effectuer une opération de maintenance ou d'annuler l'enregistrement d'une instance de vCenter Server, vous devez désactiver l'instance de vCenter Server cible. Pour fournir ses ressources aux centres de données virtuels de vCloud Director, vous devez activer l'instance de vCenter Server.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**.
3. Cliquez sur le bouton radio en regard du nom de l'instance de vCenter Server cible, puis sur **Activer** ou **Désactiver**.
4. Pour confirmer, cliquez sur **OK**.

Reconnecter une instance de vCenter Server

Si une instance de vCenter Server apparaît déconnectée ou si vous avez modifié les paramètres de connexion, vous pouvez essayer de réinitialiser la connexion.

Note Lors de l'établissement de la nouvelle connexion, l'instance de vCenter Server n'est pas disponible pour l'exécution d'opérations.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**.
3. Cliquez sur le bouton radio en regard du nom de l'instance de vCenter Server cible, puis cliquez sur **Reconnecter**.
4. Pour confirmer, cliquez sur **OK**.

Actualiser une instance de vCenter Server

Pour mettre à jour les informations de la base de données vCloud Director sur les ressources sous-jacentes de vCenter Server, vous devez actualiser l'instance de vCenter Server.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le volet de gauche, cliquez sur **vCenter**.

3 Cliquez sur le bouton radio en regard du nom de l'instance de vCenter Server cible, puis cliquez sur **Actualiser**.

4 Pour confirmer, cliquez sur **OK**.

Actualiser les stratégies de stockage d'une instance de vCenter Server

Pour mettre à jour les informations de la base de données vCloud Director sur les stratégies de stockage de machine virtuelle dans l'environnement vSphere sous-jacent, vous devez actualiser les stratégies de stockage de l'instance de vCenter Server.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le volet de gauche, cliquez sur **vCenter**.

3 Cliquez sur le bouton radio en regard du nom de l'instance de vCenter Server cible, puis cliquez sur **Actualiser les stratégies**.

4 Pour confirmer, cliquez sur **OK**.

Annuler l'enregistrement d'une instance de vCenter Server

Pour cesser d'utiliser les ressources d'une instance de vCenter Server, vous pouvez supprimer cette instance de vCenter Server de votre installation de vCloud Director.

Conditions préalables

- Désactivez l'instance de vCenter Server. Reportez-vous à Activer ou désactiver une instance de vCenter Server.
- Supprimez tous les centres de données virtuels fournisseur qui utilisent des pools de ressources de cette instance de vCenter Server. Reportez-vous à Supprimer un centre de données virtuel fournisseur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le volet de gauche, cliquez sur **vCenter**.

3 Cliquez sur le bouton radio en regard du nom de l'instance de vCenter Server cible, puis cliquez sur **Désinscrire**.

4 Pour confirmer, cliquez sur **OK**.

Modifier les paramètres de NSX Manager

Si les informations de connexion d'une instance de NSX Manager enregistrée sont modifiées, ou si vous souhaitez modifier son nom ou sa description dans vCloud Director, vous pouvez en modifier les paramètres.

Vous pouvez modifier les paramètres configurés lors de l'ajout de l'instance de NSX Manager. Reportez-vous à (Facultatif) Ajouter l'instance de NSX Manager associée.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**, puis sur le nom de l'instance de vCenter Server associée à l'instance de NSX Manager cible.
3. Dans le coin supérieur droit de la section **Infos NSX-V Manager**, cliquez sur **Modifier**.
4. Modifiez le nom d'hôte et les informations d'identification de l'administrateur de NSX Manager, puis cliquez sur **Enregistrer**.
5. (Facultatif) Pour activer la mise en réseau entre centres de données virtuels pour les centres de données virtuels répondant de cette instance de vCenter Server, activez le bouton bascule, puis entrez les propriétés de la machine virtuelle de contrôle et un nom pour l'étendue du fournisseur réseau.

   Les propriétés de la machine virtuelle de contrôle sont utilisées pour déployer un dispositif sur l'instance de NSX Manager pour la mise en réseau entre centres de données virtuels des composants, comme un routeur universel.

Paramètre	Description
Chemin du pool de ressources	Chemin d'accès hiérarchique à un pool de ressources spécifique dans l'instance de vCenter Server, commençant par le cluster, *Cluster/Resource_Pool_Parent/Target_Resource* . Par exemple, **`TestbedCluster1/mgmt-rp`**. Vous pouvez également entrer l'ID de la référence d'objet géré du pool de ressources. Par exemple, **`resgroup-1476`**.
Nom de la banque de données	Nom de la banque de données permettant d'héberger les fichiers du dispositif. Par exemple, **`shared-disk-1`**.
Interface de gestion	Nom du réseau dans vCenter Server ou groupe de ports utilisé pour l'interface de gestion du DLR HA. Par exemple, **`TestbedPG1`**.
Étendue du fournisseur de réseau	Correspond au domaine d'erreur de réseau dans les topologies réseau des groupes de centres de données. Par exemple, **`boston-fault1`**. Pour plus d'informations sur la gestion des groupes entre centres de données virtuels, reportez-vous au *Guide du portail de locataires de vCloud Director*.

Modifier les paramètres de NSX-T Manager

Si les informations de connexion d'une instance de NSX-T Manager enregistrée sont modifiées, ou si vous souhaitez modifier son nom ou sa description dans vCloud Director, vous pouvez en modifier les paramètres.

Vous pouvez modifier les paramètres configurés lors de l'ajout de l'instance de vCenter Server. Reportez-vous à Enregistrer une instance de NSX-T Manager.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **NSX-T Manager**, puis sur le nom de l'instance de NSX-T Manager que vous souhaitez modifier.
3. Dans le coin supérieur droit de l'onglet **Général**, cliquez sur **Modifier**.
4. Modifiez les paramètres de NSX-T Manager, puis cliquez sur **Enregistrer**.

Supprimer une instance de NSX-T Manager

Pour cesser d'utiliser les ressources d'une instance de NSX-T Manager, vous pouvez supprimer cette instance de vCenter Server de votre installation de vCloud Director.

Conditions préalables

Supprimez tous les centres de données virtuels fournisseur qui utilisent des ressources de cette instance de NSX-T Manager. Reportez-vous à Supprimer un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **NSX-T Manager**.
3. Cliquez sur le bouton radio en regard du nom de l'instance de NSX-T Manager à supprimer, puis sur **Supprimer**.
4. Pour confirmer, cliquez sur **Supprimer**.

Configuration et gestion de déploiements multisite

La fonctionnalité multisite de vCloud Director permet à un fournisseur de services ou à un locataire de plusieurs installations (groupes de serveurs) vCloud Director géographiquement dispersées de gérer et de surveiller ces installations et leurs organisations en tant qu'entités uniques.

Lorsque vous associez deux sites vCloud Director, vous activez l'administration des sites en tant qu'entité unique. Vous permettez également aux organisations sur ces sites de former des associations entre elles. Lorsqu'une organisation est membre d'une association, les utilisateurs de l'organisation peuvent utiliser le vCloud Director Tenant Portal pour accéder aux ressources de l'organisation de n'importe quel site membre, bien que chaque organisation membre et ses ressources soient locales sur le site qu'elles occupent.

Note Vous devez utiliser vCloud API pour associer des sites. Lorsque deux sites ont été associés, vous pouvez utiliser vCloud API ou le vCloud Director Tenant Portal pour associer les organisations qui occupent ces sites. Consultez le *Guide de programmation de vCloud API pour fournisseurs de services* et le *Guide du portail de locataires de vCloud Director*.

Un site ou une organisation peut former un nombre illimité d'associations avec un homologue, mais chaque association inclut exactement deux membres. Chaque site ou organisation doit détenir sa propre clé privée. Les membres d'une association établissent une relation de confiance en échangeant des clés publiques, qui sont utilisées pour vérifier les demandes signées d'un membre à un autre.

Chaque site d'une association est défini par l'étendue d'un groupe de serveurs vCloud Director (un groupe de serveurs qui partagent une base de données vCloud Director). Chaque organisation dans une association occupe un site unique. L'administrateur d'organisation contrôle l'accès aux ressources par les utilisateurs et les groupes de l'organisation sur chaque site membre.

Objets site et associations de sites

Le processus d'installation ou de mise à niveau crée un objet `Site` qui représente le groupe de serveurs vCloud Director local. Un administrateur système dont l'autorité s'étend à plusieurs groupes de serveurs vCloud Director peut configurer ces groupes de serveurs comme une association de sites vCloud Director.

Associations d'organisations

Une fois l'association de sites effectuée, les administrateurs d'organisation sur n'importe quel site membre peuvent commencer à associer leurs organisations.

Note Vous ne pouvez pas associer une organisation `System` à une organisation de locataire. L'organisation `System` de tout site peut être associée uniquement à l'organisation `System` d'un autre site.

Identités d'utilisateurs et de groupes

Les associations de sites et d'organisations doivent convenir d'utiliser le même fournisseur d'identité (IDP). Les identités d'utilisateurs et de groupes pour toutes les organisations dans l'association doivent être gérées au moyen de ce fournisseur d'identité.

À l'exception de l'organisation système, qui doit utiliser le fournisseur d'identité intégré de vCloud Director, les associations sont libres de choisir le fournisseur d'identité qui leur convient le mieux.

Contrôle d'accès aux sites pour les utilisateurs et les groupes d'organisation

Les administrateurs d'organisation peuvent configurer leur fournisseur d'identité pour générer des jetons d'accès d'utilisateur ou de groupe qui sont valides sur tous les sites membres ou seulement sur un sous-ensemble des sites membres. Alors que les identités d'utilisateurs et de groupes doivent être les mêmes dans toutes les organisations membres, les droits des utilisateurs et des groupes sont limités par les rôles attribués à ces utilisateurs et groupes dans chaque organisation membre. L'attribution d'un rôle à un utilisateur ou un groupe se fait de manière locale à l'organisation membre, tout comme les rôles personnalisés que vous créez.

Conditions d'équilibrage de charge

Pour mettre efficacement en œuvre un déploiement multisite, vous devez configurer un équilibrage de charge qui répartit les demandes arrivant sur un point de terminaison institutionnel comme `https://vcloud.example.com` aux points de terminaison de chaque membre de l'association de sites (par exemple, `https://us.vcloud.example.com` et `https://uk.vcloud.example.com`). Si un site dispose d'une seule cellule, vous devez également configurer un équilibrage de charge qui répartit les demandes entrantes dans l'ensemble de ses cellules, afin qu'une demande à `https://us.vcloud.example.com` puisse être traitée par `https://cell1.us.vcloud.example.com` , `https://cell2.us.vcloud.example.com` et ainsi de suite.

État de membre de l'association

Une fois que vous avez créé une association de sites ou d'organisations, le système local récupère périodiquement l'état de chaque membre distant de l'association et actualise cet état dans la base de données du site local vCloud Director. Le statut du membre est visible dans l'élément `Status` d'un `SiteAssociationMember` ou `OrgAssociationMember`. Cet élément peut avoir une des trois valeurs suivantes :

ACTIVE

L'association a été établie par les deux parties et la communication avec la partie distante a réussi.

ASYMMETRIC

L'association a été établie sur le site local, mais le site distant n'a pas encore répondu.

UNREACHABLE

Une association a été créée par les deux parties, mais le site distant est actuellement inaccessible sur le réseau.

L'état de membre « signal de pulsation » s'exécute avec l'identité de l'utilisateur système multisite, un compte d'utilisateur local de vCloud Director créé dans l'organisation système pendant l'installation de vCloud Director. Bien que ce compte soit membre de l'organisation système, il ne dispose pas de droits d'administrateur système. Il n'a qu'un seul droit, `Multisite: System Operations`, qui lui donne l'autorisation d'effectuer une demande d'API vCloud qui récupère l'état du membre distant d'une association de sites.

Listes de ressources multisites

Si vous travaillez avec des déploiements de vCloud Director sur plusieurs emplacements, vous pouvez afficher des listes de ressources qui incluent des informations sur les objets de tous les sites connectés.

Pour faciliter la navigation dans vSphere et les ressources Cloud depuis Service Provider Admin Portal, à partir de la version 9.7, vCloud Director introduit les listes de ressources multisites. À partir de la version 10.0, vCloud Director prend en charge les listes de ressources multisites qui comprennent des organisations.

Vous pouvez accéder aux listes de ressources via les menus **Ressources vSphere** et **Ressources de Cloud**.

Vous pouvez accéder à des informations détaillées sur les objets des différents sites, ainsi que créer des objets sur le site local et sur les sites distants.

Les listes de ressources multisites vSphere sont prises en charge pour les instances de vCenter Server, les instances de NSX-T Manager, les pools de ressources, les banques de données, les hôtes, les commutateurs distribués, les groupes de ports, les éléments bloqués et les stratégies de stockage.

Les listes de ressources de Cloud multisites sont prises en charge pour les organisations, les VDC d'organisation, les modèles de VDC d'organisation, les VDC fournisseurs, les cellules de Cloud, les passerelles Edge, les réseaux externes, les pools de réseaux et les stratégies de dimensionnement de VM.

Gestion des centres de données virtuels fournisseur

4

Après avoir créé un centre de données virtuel fournisseur, vous pouvez modifier ses propriétés, le désactiver ou le supprimer et gérer ses stratégies de stockage et ses pools de ressources.

Pour créer un centre de données virtuel fournisseur, vous devez utiliser la Service Provider Admin Portal ou l'API vCloud. Pour plus d'informations sur l'utilisation du Service Provider Admin Portal, reportez-vous à la section Créer un centre de données virtuel fournisseur. Pour plus d'informations sur l'utilisation de l'API vCloud, reportez-vous au *Guide de programmation de vCloud API pour fournisseurs de services*.

Ce chapitre contient les rubriques suivantes :

- Activer ou désactiver un centre de données virtuel fournisseur
- Supprimer un centre de données virtuel fournisseur
- Modifier les paramètres généraux d'un centre de données virtuel fournisseur
- Fusionner les centres de données virtuels fournisseur
- Afficher les centres de données virtuels d'organisation d'un centre de données virtuel fournisseur
- Afficher les banques de données sur un centre de données virtuel fournisseur
- Afficher les réseaux externes sur un centre de données virtuel fournisseur
- Gestion des stratégies de stockage de machine virtuelle dans un centre de données virtuel fournisseur
- Gestion des pools de ressources dans un centre de données virtuel fournisseur
- Modifier les métadonnées d'un centre de données virtuel fournisseur

Activer ou désactiver un centre de données virtuel fournisseur

Pour désactiver tous les centres de données virtuels d'organisation qui utilisent les ressources d'un centre de données virtuel fournisseur, vous pouvez désactiver ce centre de données virtuel fournisseur. Vous ne pouvez pas créer de centres de données virtuels d'organisation qui utilisent les ressources d'un centre de données virtuel de fournisseur désactivé.

Les vApp en cours d'exécution et les machines virtuelles sous tension continuent à s'exécuter dans les centres de données virtuels d'organisation existants dépendant de ce centre de données virtuel fournisseur, mais vous ne pouvez ni créer ni démarrer d'autres vApp ou machines virtuelles.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.
3. Cliquez sur le bouton radio en regard du nom du centre de données virtuel fournisseur cible, puis sur **Désactiver** ou **Activer**.
4. Pour confirmer, cliquez sur **OK**.

Supprimer un centre de données virtuel fournisseur

Pour supprimer les ressources d'un centre de données virtuel fournisseur de vCloud Director, vous pouvez supprimer ce centre de données virtuel fournisseur.

Les ressources sous-jacentes dans vSphere ne sont pas affectées.

Conditions préalables

- Désactivez le centre de données virtuel fournisseur cible. Reportez-vous à Activer ou désactiver un centre de données virtuel fournisseur.
- Supprimez tous les centres de données virtuels d'organisation qui utilisent des ressources de ce centre de données virtuel fournisseur. Reportez-vous à Supprimer un centre de données virtuel d'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.
3. Cliquez sur le bouton radio en regard du nom du centre de données virtuel fournisseur à supprimer, puis sur **Supprimer**.
4. Pour confirmer, cliquez sur **OK**.

Modifier les paramètres généraux d'un centre de données virtuel fournisseur

Vous pouvez modifier le nom et la description d'un centre de données virtuel fournisseur. Si le pool de ressources de sauvegarde prend en charge une version de matériel virtuel plus élevée, vous pouvez mettre à niveau le matériel virtuel le plus élevé pris en charge par un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur que vous souhaitez modifier.
3. Sous l'onglet **Configurer > Général**, dans le coin supérieur droit, cliquez sur **Modifier**.
4. (Facultatif) Modifiez le nom et la description du centre de données virtuel fournisseur.
5. (Facultatif) Dans le menu déroulant, sélectionnez la version matérielle la plus élevée prise en charge par ce centre de données virtuel fournisseur, puis cliquez sur **Enregistrer**.

   La version la plus élevée que vous pouvez sélectionner est déterminée par les hôtes ESXi du pool de ressources dont dépend le centre de données virtuel fournisseur.

   Note Vous pouvez uniquement mettre à niveau la version matérielle prise en charge par un centre de données virtuel fournisseur. Vous ne pouvez pas la rétrograder. La version du matériel de machine virtuelle la plus haute prise en charge dans vCloud Director 10.0 est la version 14.
6. Cliquez sur **Enregistrer**.

Fusionner les centres de données virtuels fournisseur

Pour associer les ressources de deux centres de données virtuels fournisseur, vous pouvez fusionner ces centres de données virtuels fournisseur en un centre de données virtuel fournisseur unique.

Conditions préalables

- Les centres de données virtuels du fournisseur cible appartiennent au même centre de données vCenter Server.
- Les centres de données virtuels fournisseur cible ne contiennent que des centres de données virtuels d'organisation élastiques.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.
3. Cliquez sur le bouton radio en regard du nom du centre de données virtuel fournisseur à développer, puis sur **Fusionner**.
4. Cliquez sur le bouton radio en regard du nom du centre de données virtuel fournisseur avec lequel fusionner les ressources, puis sur **Fusionner**.

Afficher les centres de données virtuels d'organisation d'un centre de données virtuel fournisseur

Vous pouvez afficher la liste des centres de données virtuels d'organisation qui utilisent des ressources d'un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **VDC d'organisation**.

Résultats

La liste des centres de données virtuels d'organisation qui consomment les ressources de ce centre de données virtuel fournisseur s'affiche. Pour chaque VDC d'organisation, la liste inclut des informations sur l'état, le modèle d'allocation, l'organisation, l'instance de vCenter Server, le nombre de réseaux, le nombre de vApp, le nombre de stratégies de stockage et le nombre de pools de ressources.

Étape suivante

- Vous pouvez accéder à la vue du centre de données virtuel d'organisation dans le vCloud Director Tenant Portal en cliquant sur l'icône **contextuelle** (↗) en regard du nom du centre de données virtuel d'organisation cible.
- En cliquant sur le bouton radio en regard du nom d'un centre de données virtuel d'organisation, vous pouvez effectuer des opérations de gestion semblables aux opérations décrites dans Chapitre 6 Gestion des centres de données virtuels d'organisation.

Afficher les banques de données sur un centre de données virtuel fournisseur

Vous pouvez afficher des détails sur les banques de données qui fournissent la capacité de stockage à un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **Banque de données**.

   Une liste de toutes les banques de données du centre de données virtuel fournisseur s'affiche. La liste contient les informations suivantes pour chaque banque de données.

Titre	Description
Nom	Nom de la banque de données
État	Activé ou désactivé
Type	Type de système de fichiers que la banque de données utilise, VMFS (Virtual Machine File System) ou NFS (Network File System)
Utilisé	Espace de banque de données occupé par les fichiers de machine virtuelle, y compris les fichiers journaux, les snapshots et les disques virtuels. Lorsqu'une machine virtuelle est activée, l'espace de stockage utilisé inclut également des fichiers journaux.
Provisionnée	Espace de banque de données garanti pour les machines virtuelles. Si des machines virtuelles utilisent le provisionnement fin, une partie de l'espace provisionné peut ne pas être utilisée et d'autres machines virtuelles peuvent occuper l'espace inutilisé. Cette valeur peut être supérieure à la capacité de la banque de données réelle si le provisionnement fin est utilisé.
Stockage requis	Stockage provisionné utilisé uniquement par des objets vCloud Director sur la banque de données, y compris : ■ Machines virtuelles provisionnées dans vCloud Director ■ Éléments du catalogue (modèles et supports) ■ dispositifs NSX Edge ■ Exigences relatives à l'échange de mémoire utilisées et inutilisées pour les machines virtuelles Cette valeur n'inclut pas le stockage demandé par les machines virtuelles fantômes ou les disques intermédiaires dans une arborescence de clone lié.
vCenter	Instance de vCenter Server associée à la banque de données

Afficher les réseaux externes sur un centre de données virtuel fournisseur

Vous pouvez afficher la liste des réseaux externes accessibles à un centre de données virtuel fournisseur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.

3 Cliquez sur l'onglet **Réseaux externes**.

Résultats

Vous pouvez afficher la liste des réseaux externes disponibles avec des informations sur leurs paramètres CIDR de passerelle et l'utilisation du pool d'adresses IP.

Gestion des stratégies de stockage de machine virtuelle dans un centre de données virtuel fournisseur

Vous pouvez ajouter, activer, désactiver et supprimer des stratégies de stockage de machine virtuelle dans un centre de données virtuel fournisseur. Vous pouvez également ajouter, modifier et supprimer des métadonnées d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur.

Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel fournisseur

Vous pouvez ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel fournisseur, après quoi vous pouvez configurer des centres de données virtuels d'organisation dépendant de ce centre de données virtuel fournisseur pour prendre en charge la stratégie de stockage ajoutée.

Important vCloud Director ne prend pas en charge les stratégies de stockage de machine virtuelle pour les services de données basés sur un hôte, comme le chiffrement et Storage I/O Control.

Conditions préalables

- Votre administrateur vSphere a créé la stratégie de stockage de machine virtuelle cible. Pour plus d'informations sur la gestion basée sur une stratégie de stockage (SPBM, Storage Policy Based Management), reportez-vous à la documentation *Stockage vSphere*.
- Actualiser les stratégies de stockage d'une instance de vCenter Server.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Dans l'onglet **Stratégies de stockage**, cliquez sur **Ajouter**.
4. Sélectionnez une ou plusieurs stratégies de stockage à ajouter et cliquez sur **Ajouter**.

   Si vous sélectionnez * **(Tous)**, vCloud Director ajoute ou supprime des banques de données de manière dynamique à mesure qu'elles sont ajoutées aux clusters de banque de données du centre de données virtuel fournisseur ou supprimées de ceux-ci.

Étape suivante

Configurez les centres de données virtuels d'organisation dépendant du centre de données virtuel fournisseur pour prendre en charge la stratégie de stockage. Reportez-vous à Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel d'organisation.

Activer ou désactiver une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur

Après la désactivation d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur, ses centres de données virtuels d'organisation ne peuvent plus utiliser cette stratégie de stockage de machine virtuelle.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **Stratégies de stockage**.
4. Cliquez sur le bouton radio en regard de la stratégie de stockage de machine virtuelle cible, puis sur **Activer** ou **Désactiver**.
5. Pour confirmer, cliquez sur **OK**.

Supprimer une stratégie de stockage de machine virtuelle d'un centre de données virtuel fournisseur

Vous pouvez supprimer une stratégie de stockage de machine virtuelle d'un centre de données virtuel fournisseur.

Conditions préalables

Désactivez la stratégie de stockage de machine virtuelle cible. Reportez-vous à Activer ou désactiver une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **Stratégies de stockage**.
4. Cliquez sur le bouton radio en regard de la stratégie de stockage de machine virtuelle cible et cliquez sur **Supprimer**.
5. Pour confirmer, cliquez sur **Supprimer**.

Modifier les métadonnées d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel fournisseur

Vous pouvez ajouter, modifier et supprimer des métadonnées d'une stratégie de stockage dans un centre de données virtuel fournisseur.

En utilisant des métadonnées d'objet, vous pouvez associer des paires *nom=valeur* définies par l'utilisateur à une stratégie de stockage sur un centre de données virtuel fournisseur. Vous pouvez utiliser des métadonnées d'objet dans des expressions de filtre de requête d'API vCloud.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **Stratégies de stockage**.
4. Cliquez sur le bouton radio en regard de la stratégie de stockage de machine virtuelle cible, puis sur **Métadonnées**.
5. Cliquez sur **Modifier**.
6. (Facultatif) Pour ajouter une paire clé-valeur, cliquez sur **Ajouter**, entrez un nom et une valeur, puis sélectionnez un type pour la nouvelle paire clé-valeur.
7. (Facultatif) Pour modifier une paire clé-valeur, entrez un nouveau nom et une valeur, puis sélectionnez un nouveau type pour la paire clé-valeur.
8. (Facultatif) Pour supprimer une paire clé-valeur, à droite de la ligne correspondante, cliquez sur l'icône **Supprimer**.
9. Cliquez sur **Enregistrer** , puis sur **OK**.

Gestion des pools de ressources dans un centre de données virtuel fournisseur

Vous pouvez ajouter, activer, désactiver et détacher des pools de ressources secondaires dans un centre de données virtuel fournisseur. Vous ne pouvez pas désactiver ou détacher le pool de ressources principal dans un centre de données virtuel fournisseur.

Ajouter un pool de ressources à un centre de données virtuel fournisseur

Vous pouvez ajouter un ou plusieurs pools de ressources secondaires à un centre de données virtuel fournisseur, afin que ses centres de données virtuels Facturation à l'utilisation et Pool d'allocations puissent se développer.

Lorsqu'elles dépendent de plusieurs pools de ressources, les ressources de calcul peuvent s'étendre en fonction du nombre de machines virtuelles.

Vous pouvez ajouter des pools de ressources reposant sur des clusters vSphere, configurés de manière optimale pour héberger des dispositifs NSX Edge comportant des liaisons montantes VLAN. vCloud Director peut utiliser des métadonnées pour indiquer que le système doit placer des passerelles Edge de VDC d'organisation dans des pools de ressources dépendant de ces clusters. Pour plus d'informations, reportez-vous à l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/2151398.

Conditions préalables

Votre administrateur vSphere a créé le pool de ressources secondaire cible dans l'instance de vCenter Server dont dépend le pool de ressources principal du centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Dans l'onglet **Pools de ressources**, cliquez sur **Ajouter**.
4. Sélectionnez un ou plusieurs pools de ressources, puis cliquez sur **Ajouter**.

Résultats

vCloud Director ajoute le pool de ressources qui sera utilisé par le centre de données virtuel fournisseur, rendant élastiques tous les centres de données virtuels d'organisation Facturation à l'utilisation et Pool d'allocations dépendant du centre de données virtuel fournisseur.

vCloud Director ajoute également un pool de ressources de VDC système sous le nouveau pool de ressources. Ce pool de ressources est utilisé pour la création de ressources système, telles que des machines virtuelles NSX Edge et des machines virtuelles qui servent de modèle pour les clones liés.

Important Ne modifiez pas ou ne supprimez pas le pool de ressources de VDC système.

Activer ou désactiver un pool de ressources sur un centre de données virtuel fournisseur

Lorsque vous désactivez un pool de ressources, les ressources de mémoire et de calcul du pool de ressources ne sont plus accessibles au centre de données virtuel fournisseur.

Les processus déjà en cours ne cessent pas d'utiliser les ressources du pool de ressources désactivé.

Note Vous ne pouvez pas désactiver le pool de ressources principal dans un centre de données virtuel fournisseur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.

3 Cliquez sur l'onglet **Pools de ressources**.

4 Cliquez sur le bouton radio en regard du pool de ressources cible, puis sur **Activer** ou **Désactiver**.

5 Pour confirmer, cliquez sur **OK**.

Détacher un pool de ressources d'un centre de données virtuel fournisseur

Si un centre de données virtuel fournisseur contient plusieurs pools de ressources, vous pouvez détacher un pool de ressources secondaire du centre de données virtuel fournisseur. Vous ne pouvez pas détacher le pool de ressources principal du centre de données virtuel du fournisseur.

Conditions préalables

- Désactivez le pool de ressources cible sur le centre de données virtuel fournisseur. Reportez-vous à Activer ou désactiver un pool de ressources sur un centre de données virtuel fournisseur.
- Redéployez des réseaux qui sont affectés par le pool de ressources désactivé.
- Redéployez des passerelles Edge qui sont affectées par le pool de ressources désactivé.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.

3 Cliquez sur l'onglet **Pools de ressources**.

4 Cliquez sur le bouton radio situé en regard du pool de ressources cible, puis cliquez sur **Détacher**.

5 Pour confirmer, cliquez sur **OK**.

Modifier les métadonnées d'un centre de données virtuel fournisseur

Vous pouvez ajouter, modifier et supprimer des métadonnées pour un centre de données virtuel fournisseur.

En utilisant des métadonnées d'objets, vous pouvez associer des paires *nom=valeur* définies par l'utilisateur à un centre de données virtuel fournisseur. Vous pouvez utiliser des métadonnées d'objets dans les expressions de filtre de requête API vCloud.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Sous l'onglet **Configurer > Métadonnées**, dans le coin supérieur droit, cliquez sur **Modifier**.
4. (Facultatif) Pour ajouter une paire clé-valeur, cliquez sur **Ajouter**, entrez un nom et une valeur, puis sélectionnez un type pour la nouvelle paire clé-valeur.
5. (Facultatif) Pour modifier une paire clé-valeur, entrez un nouveau nom et une valeur, puis sélectionnez un nouveau type pour la paire clé-valeur.
6. (Facultatif) Pour supprimer une paire clé-valeur, à droite de la ligne correspondante, cliquez sur l'icône **Supprimer**.
7. Cliquez sur **Enregistrer** , puis sur **OK**.

Gestion d'organisations

5

vCloud Director Service Provider Admin Portal vous permet de créer, de configurer et de gérer les organisations vCloud Director.

Utilisez vCloud Director Service Provider Admin Portal pour gérer des organisations, définir des stratégies en vue de déterminer la façon dont les utilisateurs consomment les ressources allouées à une organisation, et gérer la publication et le partage des catalogues.

Ce chapitre contient les rubriques suivantes :

- Comprendre comment fonctionnent les baux
- Créer une organisation
- Configurer les catalogues d'une organisation
- Configurer les stratégies d'une organisation
- Migrer le stockage des locataires

Comprendre comment fonctionnent les baux

La création d'une organisation implique la spécification de baux. Les baux fournissent un certain niveau de contrôle sur les ressources de stockage et de calcul d'une organisation, en spécifiant la quantité de temps maximum d'exécution des vApp et de stockage de modèles de vApp.

L'objectif d'un bail de délai d'exécution est d'empêcher que des vApp inactifs consomment des ressources de calcul. Si, par exemple, un utilisateur démarre un vApp et part en congé sans l'arrêter, ce vApp continue de consommer des ressources.

Un bail de délai d'exécution commence lorsqu'un utilisateur démarre un vApp. Lors de l'expiration d'un bail de délai d'exécution, vCloud Director arrête le vApp.

L'objectif d'un bail de stockage est d'empêcher que des vApp et des modèles de vApp inutilisés consomment des ressources de stockage. Un bail de stockage de vApp commence lorsqu'un utilisateur arrête un vApp. Les baux de stockage n'affectent pas les vApp en cours d'exécution. Un bail de stockage de modèle de vApp commence lorsqu'un utilisateur ajoute le modèle de vApp à un vApp, ajoute le modèle de vApp à un espace de travail, télécharge, copie ou déplace le modèle de vApp.

Lors de l'expiration d'un bail de stockage, vCloud Director indique que le vApp ou le modèle de vApp a expiré, ou supprime le vApp ou le modèle de vApp, en fonction de la stratégie d'organisation que vous définissez.

Créer une organisation

Vous pouvez créer une organisation à partir de vCloud Director Service Provider Admin Portal.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**

   a Sur le panneau de gauche, sélectionnez **Organisations**.

   La liste des organisations existantes s'affiche dans une vue de grille.

2 Pour créer une organisation, cliquez sur le bouton **+Ajouter**.

   La boîte de dialogue **Nouvelle organisation** s'ouvre.

3 Entrez les valeurs suivantes.

Option	Description
Nom de l'organisation	Identifiant unique qui constitue l'URL permettant d'accéder au portail du locataire de l'organisation.
Nom complet de l'organisation	Nom complet de l'organisation.
Description	Description facultative de l'organisation.

4 Cliquez sur le bouton **Créer** pour terminer la création.

Configurer les catalogues d'une organisation

Vous pouvez configurer la manière dont une organisation partage ses catalogues de services.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**

   a Sur le panneau de gauche, sélectionnez **Organisations**.

   La liste des organisations existantes s'affiche dans une vue de grille.

2 Sélectionnez une organisation et, sous l'onglet **Configurer**, sélectionnez **Catalogue**.

3 Pour modifier les paramètres de partage et de publication, cliquez sur **Modifier**.

Option	Description
Partage	Permet aux administrateurs de l'organisation de partager les catalogues de celle-ci avec d'autres organisations appartenant à cette instance de vCloud Director. Si vous ne sélectionnez pas cette option, les administrateurs d'organisation peuvent toujours partager des catalogues dans l'organisation.
Autoriser la publication de catalogues externes	Permet aux administrateurs de l'organisation de publier des catalogues dans les organisations externes à cette instance de vCloud Director.
Autoriser l'abonnement à des catalogues externes	Permet aux administrateurs de l'organisation de s'abonner à des catalogues externes à cette instance de vCloud Director.

Configurer les stratégies d'une organisation

Les baux, les quotas et les limites contraignent les utilisateurs d'une organisation concernant la consommation des ressources de stockage et de traitement. Vous pouvez modifier ces paramètres pour empêcher des utilisateurs d'épuiser ou de monopoliser les ressources d'une organisation.

Conditions préalables

Reportez-vous à Comprendre comment fonctionnent les baux.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**

   a Sur le panneau de gauche, sélectionnez **Organisations**.

   La liste des organisations existantes s'affiche dans une vue de grille.

2 Sélectionnez une organisation, puis l'onglet **Stratégies**.

3 Pour modifier les baux, les quotas, les limites des ressources et les stratégies de mot de passe de l'organisation, cliquez sur **Modifier**.

4 Configurez des baux vApp avec les paramètres suivants.

Option	Description
Bail de délai d'exécution maximal	Durée d'exécution des vApp avant leur arrêt automatique.
Action en cas d'expiration du délai d'exécution	Mode de traitement des vApp qui ont expiré. L'interruption d'un vApp interrompt toutes ses machines virtuelles et conserve leur état actuel en écrivant la mémoire sur le disque. **Mettre hors tension** arrête immédiatement toutes ses machines virtuelles et ses vApp enfants.
Bail de stockage maximal	Délai de disponibilité des vApp arrêtés avant leur suppression automatique.
Nettoyage du stockage	Traitement des vApp après leur arrêt et leur suppression.

5 Configurez les modèles de baux de vApp avec les paramètres suivants.

Option	Description
Bail de stockage maximal	Délai de disponibilité des modèles de vApp avant leur suppression automatique.
Nettoyage du stockage	Traitement des modèles de vApp ayant expiré après leur suppression.

6 Configurez des quotas avec les paramètres suivants.

Option	Description
Quota de toutes les machines virtuelles	Nombre total de machines virtuelles disponibles qu'un utilisateur peut stocker dans cette organisation.
Quota de machines virtuelles en cours d'exécution	Nombre total de machines virtuelles qu'un utilisateur peut mettre sous tension dans cette organisation.

7 Configurez des limites avec les paramètres suivants.

Option	Description
Nombre d'opérations exigeantes en ressources par utilisateur	Tapez le nombre maximal d'opérations simultanées exigeantes en ressources par utilisateur ou sélectionnez **Hériter de la limite du système**.
Nombre d'opérations exigeantes en ressources à mettre en file d'attente par utilisateur	Tapez le nombre maximal d'opérations exigeantes en ressources à mettre en file d'attente par utilisateur ou sélectionnez **Hériter de la limite du système**.
Nombre d'opérations exigeantes en ressources par organisation	Tapez le nombre maximal d'opérations simultanées exigeantes en ressources par organisation ou sélectionnez **Hériter de la limite du système**.
Nombre d'opérations exigeantes en ressources à mettre en file d'attente par organisation	Tapez le nombre maximal d'opérations exigeantes en ressources à mettre en file d'attente par organisation ou sélectionnez **Hériter de la limite du système**.
Nombre de connexions simultanées par machine virtuelle	Tapez le nombre maximal de connexions de console simultanées par machine virtuelle ou sélectionnez **Hériter de la limite du système**.
Nombre de centres de données virtuels par organisation	Tapez le nombre maximal de centres de données virtuels d'organisation par organisation ou sélectionnez **Hériter du quota du système**.

8 Configurez des stratégies de mot de passe avec les paramètres suivants.

Option	Description
Verrouillage de compte activé	Activez le verrouillage du compte d'utilisateur après un nombre de tentatives de connexion non valides.
Connexions non valides avant le verrouillage	Nombre de tentatives de connexion non valides avant que le compte d'utilisateur soit verrouillé.
Intervalle de verrouillage de compte	Période pendant laquelle un compte d'utilisateur verrouillé ne peut pas se connecter.

Migrer le stockage des locataires

Vous pouvez migrer tous les vApp, les disques indépendants et les éléments de catalogue d'une ou de plusieurs organisations depuis une ou plusieurs banques de données vers d'autres banques de données.

Avant de désaffecter une banque de données, vous devez migrer tous les éléments stockés sur cette banque de données vers une nouvelle banque de données. Vous pouvez également migrer une organisation vers une nouvelle banque de données disposant d'une capacité de stockage supérieure ou qui utilise une technologie de stockage plus récente, telle que VMware vSAN.

Important La migration de stockage de locataire est une opération gourmande en ressources qui peut durer un long moment, en particulier lorsqu'il y a de nombreuses ressources à migrer. Pour plus d'informations sur la migration d'un stockage des locataires, consultez https://kb.vmware.com/kb/2151086.

Conditions préalables

- Déterminez les stratégies de stockage utilisées par les VDC d'organisation des organisations cibles. Reportez-vous à la section Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel d'organisation.
- Pour chaque stratégie de stockage contenant une banque de données source que vous souhaitez migrer, vérifiez qu'il existe au moins une banque de données de destination vers laquelle effectuer la migration. Vous pouvez créer des banques de données de destination ou utiliser celles qui existent déjà. Pour plus d'informations sur la détermination des banques de données dans les stratégies de stockage utilisées par les organisations cibles, reportez-vous à la documentation sur le *stockage vSphere*.

Procédure

1. Connectez-vous à vCloud Director Service Provider Admin Portal en tant qu'**administrateur système** ou avec un rôle disposant du droit **Organisation : Migrer le stockage des locataires**.
2. Démarrez l'assistant **Migrer le stockage des locataires**.
   - Sous **Ressources de Cloud**, sélectionnez **Organisations** et cliquez sur **Migrer le stockage des locataires**.
   - Sous **Ressources vSphere**, sélectionnez **Banques de données** et cliquez sur **Migrer le stockage des locataires**.
3. Sélectionnez une ou plusieurs organisations avec des éléments de stockage que vous souhaitez migrer, puis cliquez sur **Suivant**.
4. Sélectionnez une ou plusieurs banques de données sources à migrer, puis cliquez sur **Suivant**.

   L'assistant répertorie toutes les banques de données dans le système.
5. Sélectionnez une ou plusieurs banques de données de destination, puis cliquez sur **Suivant**.

6 Vérifiez la page **Prêt à terminer**, puis cliquez sur **Terminer** pour commencer la migration.

Gestion des centres de données virtuels d'organisation

6

Pour fournir des ressources à une organisation, vous créez un ou plusieurs centres de données virtuels d'organisation pour cette organisation. Après avoir créé un centre de données virtuel d'organisation, vous pouvez modifier ses propriétés, le désactiver ou le supprimer et gérer ses paramètres de modèle d'allocation, de stockage et de réseau.

Ce chapitre contient les rubriques suivantes :

- Compréhension des modèles d'allocation
- Présentation des stratégies de positionnement et de dimensionnement de machine virtuelle
- Créer un centre de données virtuel d'organisation
- Activer ou désactiver un centre de données virtuel d'organisation
- Supprimer un centre de données virtuel d'organisation
- Modifier le nom et la description d'un centre de données virtuel d'organisation
- Modifier les paramètres de modèle d'allocation d'un centre de données virtuel d'organisation
- Modification des paramètres de stockage d'un centre de données virtuel d'organisation
- Modifier les paramètres réseau d'un centre de données virtuel d'organisation
- Configuration de la mise en réseau intercentre de données virtuel
- Modifier les métadonnées d'un centre de données virtuel d'organisation
- Afficher les pools de ressources d'un centre de données virtuel d'organisation
- Gestion du pare-feu distribué dans un centre de données virtuel d'organisation

Compréhension des modèles d'allocation

Un modèle d'allocation détermine comment et quand les ressources de calcul et de mémoire du centre de données virtuel (VDC) fournisseur alloué sont attribuées au VDC d'organisation.

Le tableau suivant présente les paramètres de distribution des ressources de vSphere au niveau de la machine virtuelle ou du pool de ressources en fonction du modèle d'allocation de VDC d'organisation.

	Modèle d'allocation Flex	Modèle de pool d'allocation élastique	Modèle de pool d'allocation non élastique	Modèle de facturation à l'utilisation	Modèle de pool de réservation
Élastique	En fonction de la configuration du VDC d'organisation.	Oui	Non	Oui	Non
Vitesse du vCPU	Si une limite de CPU de machine virtuelle n'est pas définie dans une stratégie de dimensionnement de machine virtuelle, la vitesse de vCPU peut avoir un impact sur la limite de CPU de machine virtuelle dans le VDC.	Affecte le nombre de vCPU en cours d'exécution dans le VDC d'organisation.	Non applicable	Affecte la limite de CPU de machine virtuelle	Non applicable
Limite de CPU de pool de ressources	Limite de CPU de VDC d'organisation répartie en fonction du nombre de machines virtuelles dans le pool de ressources.	Allocation de CPU de VDC d'organisation	Allocation de CPU de VDC d'organisation	Illimité	Allocation de CPU de VDC d'organisation
Réservation de CPU du pool de ressources	La réservation de CPU de VDC d'organisation est répartie en fonction du nombre de vCPU dans le pool de ressources. La réservation de CPU du VDC d'organisation est égale à l'allocation du CPU du VDC d'organisation multipliée par la garantie de CPU.	Somme des machines virtuelles sous tension et correspondant à la garantie de CPU multipliée par la vitesse de vCPU, multiplié par le nombre de vCPU.	Allocation de CPU de VDC d'organisation multipliée par la garantie de CPU	Aucun, extensible	Allocation de CPU de VDC d'organisation
Limite de mémoire du pool de ressources	La limite de mémoire de VDC d'organisation est répartie en fonction du nombre de machines virtuelles dans le pool de ressources.	Illimité	Allocation de RAM de VDC d'organisation	Illimité	Allocation de RAM de VDC d'organisation
Réservation de mémoire du pool de ressources	La réservation de RAM de VDC d'organisation est répartie en fonction du nombre de machines virtuelles dans le pool de ressources. La réservation de RAM de VDC d'organisation est égale à l'allocation de RAM de VDC d'organisation multipliée par la garantie de RAM.	Somme de la garantie de RAM multipliée par la vRAM de toutes les machines virtuelles sous tension dans le pool de ressources. La réservation de RAM de pool de ressources est extensible.	Allocation de RAM de VDC d'organisation multipliée par la garantie de RAM	Aucun, extensible	Allocation de RAM de VDC d'organisation

	Modèle d'allocation Flex	Modèle de pool d'allocation élastique	Modèle de pool d'allocation non élastique	Modèle de facturation à l'utilisation	Modèle de pool de réservation
Limite de CPU de machine virtuelle	Basée sur la stratégie de dimensionnement de machine virtuelle de la machine virtuelle.	Illimité	Illimité	Vitesse de vCPU multipliée par le nombre de vCPU	Personnalisé
Réservation de CPU de machine virtuelle	Basée sur la stratégie de dimensionnement de machine virtuelle de la machine virtuelle.	0	0	Est égal à la vitesse de CPU multipliée par la vitesse de vCPU, multipliée par le nombre de vCPU.	Personnalisé
Limite de RAM de machine virtuelle	Basée sur la stratégie de dimensionnement de machine virtuelle de la machine virtuelle.	Illimité	Illimité	vRAM	Personnalisé
Réservation de RAM de machine virtuelle	Basée sur la stratégie de dimensionnement de machine virtuelle de la machine virtuelle.	0	Est égal à la vRAM multipliée par la garantie de RAM plus le surdébit de RAM.	Est égal à la vRAM multipliée par la garantie de RAM plus le surdébit de RAM.	Personnalisé

Conversion d'un modèle d'allocation de VDC hérité en un modèle d'allocation Flex

Vous ajoutez une stratégie de positionnement et de dimensionnement de machine virtuelle à un VDC avec un modèle de pool d'allocation élastique, un modèle de pool d'allocation non élastique, un modèle de facturation à l'utilisation ou un modèle de pool de réservation. Si la stratégie de positionnement ou de dimensionnement de machine virtuelle n'est pas compatible avec le modèle d'allocation de VDC existant, vous pouvez décider de convertir le VDC en VDC d'organisation Flex.

Conformité de la stratégie de machine virtuelle

La conversion d'un VDC hérité ne provoque pas de non-conformité de machine virtuelle. Si un administrateur modifie les valeurs de calcul de machine virtuelle ou l'appartenance à un groupe de machines virtuelles d'une machine virtuelle directement dans l'instance de vCenter Server, une machine virtuelle peut devenir non conforme à la stratégie de positionnement ou de dimensionnement de machine virtuelle attribuée. Une machine virtuelle peut également devenir non conforme si un utilisateur disposant des privilèges nécessaires modifie la réservation de la machine virtuelle et ses valeurs limites à l'aide de l'API vCloud. En présence d'une

machine virtuelle non conforme, l'interface utilisateur de vCloud Director Tenant Portal affiche un message d'avertissement. Le locataire peut voir des informations détaillées sur la cause de la non-conformité et peut rendre la machine virtuelle à nouveau conforme, ce qui réapplique les stratégies à la machine virtuelle.

Utilisation suggérée des modèles d'allocation

Chaque modèle d'allocation peut être utilisé pour différents niveaux de contrôle et de gestion des performances.

Le tableau suivant contient des informations sur l'utilisation suggérée de chaque modèle d'allocation.

Modèle d'allocation	Utilisation suggérée
Modèle d'allocation Flex	Avec le modèle d'allocation Flex, vous disposez d'un contrôle précis des performances au niveau de la charge de travail. Avec le modèle d'allocation Flex, les **administrateurs système** de vCloud Director peuvent gérer l'élasticité des VDC d'organisation spécifiques. Le modèle d'allocation Flex utilise la gestion des charges de travail basée sur des stratégies. Avec le modèle d'allocation Flex, les **fournisseurs de cloud** ont davantage de contrôle sur la capacité supplémentaire de mémoire dans un VDC d'organisation et peuvent appliquer une utilisation de fonctionnalité de pic stricte pour les locataires.
Modèle d'allocation de pool d'allocation	Utilisez le modèle d'allocation de pool d'allocation pour les charges de travail durables et stables, où les locataires s'abonnent à une consommation de ressources de calcul fixe et les **fournisseurs de cloud** peuvent prévoir et gérer la capacité des ressources de calcul. Le modèle d'allocation de pool d'allocation est optimal pour les charges de travail ayant des exigences de performance différentes. Avec le modèle d'allocation de pool d'allocation, toutes les charges de travail partagent les ressources allouées à partir des pools de ressources de vCenter Server. Que vous activiez ou désactiviez l'élasticité, les locataires reçoivent une quantité limitée de ressources de calcul. Avec le modèle d'allocation de pool d'allocation, les **fournisseurs de cloud** activent ou désactivent l'élasticité au niveau du système et le paramètre s'applique à tous les VDC d'organisation du pool d'allocation. Si vous utilisez l'allocation de pool d'allocation non élastique, le VDC d'organisation pré-réserve le pool de ressources de VDC et les locataires peuvent surcharger les vCPU mais ne peuvent pas surcharger la mémoire. Si vous utilisez l'allocation de pool élastique, le VDC d'organisation ne pré-réserve aucune ressource de calcul et la capacité peut s'étendre sur plusieurs clusters. Les fournisseurs de Cloud gèrent la surcharge des ressources de calcul physiques et les locataires ne peuvent pas surcharger les vCPU ni la mémoire.

Modèle d'allocation	Utilisation suggérée
Facturation à l'utilisation	Utilisez le modèle de facturation à l'utilisation lorsque vous n'avez pas à allouer de ressources de calcul dans vCenter Server au préalable. La réservation, la limite et les parts sont appliquées à chaque charge de travail que les locataires déploient dans le VDC. Avec le modèle d'allocation de facturation à l'utilisation, chaque charge de travail dans le VDC d'organisation reçoit le même pourcentage des ressources de calcul configurées. Pour vCloud Director, la vitesse de CPU de chaque vCPU pour chaque charge de travail est identique et vous pouvez uniquement définir la vitesse du CPU au niveau du VDC d'organisation. Du point de vue des performances, étant donné que vous ne pouvez pas modifier les paramètres de réservation de charges de travail individuelles, chaque charge de travail reçoit la même préférence. Le modèle d'allocation de facturation à l'utilisation est optimal pour les locataires qui nécessitent que des charges de travail ayant différentes exigences de performances s'exécutent dans le même VDC d'organisation. En raison de l'élasticité, le modèle de facturation à l'utilisation convient aux charges de travail génériques à durée de vie courte qui font partie d'applications de mise à l'échelle automatique. Avec la facturation à l'utilisation, les locataires peuvent faire correspondre les pics de demande en ressources de calcul au sein d'un VDC d'organisation.
Pool de réservation	Utilisez le modèle d'allocation de pool de réservation lorsque vous avez besoin d'un contrôle précis sur les performances des charges de travail qui s'exécutent dans le VDC d'organisation. Du point de vue du **fournisseur de cloud**, le modèle d'allocation de pool de réservation nécessite une allocation préalable de toutes les ressources de calcul dans vCenter Server. Le modèle d'allocation de pool de réservation n'est pas élastique. Le modèle d'allocation de pool de réservation est optimal pour les charges de travail qui s'exécutent sur du matériel dédié à un locataire spécifique. Dans ce cas, les utilisateurs locataires peuvent gérer l'utilisation et la surcharge des ressources de calcul.

Modèle d'allocation Flex

À partir de vCloud Director 9.7, les **administrateurs système** peuvent créer des centres de données virtuels (VDC) d'organisation à l'aide du modèle d'allocation Flex. Avec la combinaison de stratégies d'allocation Flex et de dimensionnement de machine virtuelle, les **administrateurs système** peuvent contrôler la consommation de CPU et de RAM à la fois sur le VDC et sur les machines virtuelles spécifiques. Le modèle d'allocation Flex prend en charge toutes les configurations d'allocation disponibles dans les modèles d'allocation existants.

Dans vCloud Director 10.0, tous les VDC d'organisation non-Flex peuvent être convertis en VDC Flex.

Lors de la création d'un VDC d'organisation Flex, les **administrateurs système** contrôlent les paramètres suivants du VDC d'organisation :

Paramètre	Description
Élasticité	Activez ou désactivez la fonctionnalité de pool élastique.
Inclure la capacité supplémentaire de mémoire de VM	Incluez ou excluez la surcharge de mémoire dans ce VDC. Lorsque cette propriété est définie sur true, il est possible que vous ne puissiez pas utiliser la capacité totale du VDC, car la surcharge de mémoire de chaque machine virtuelle sous tension est également puisée dans la capacité disponible du VDC. Lorsque cette valeur est définie sur false, la surcharge de mémoire provient du VDC fournisseur et non de la capacité allouée du VDC.

Paramètre	Description
Allocation de processeur	Quantité de CPU allouée à ce VDC en MHz ou en GHz. L'allocation de CPU définit la capacité de CPU du VDC. Le CPU total utilisé par toutes les machines virtuelles exécutées dans le VDC ne peut pas dépasser cette valeur.
Limite de CPU	La limite de CPU définit le quota de CPU d'un VDC. Dans la plupart des cas, la limite de CPU est égale à la capacité allouée de CPU du VDC. Parfois, il peut être nécessaire de ne pas allouer de CPU au VDC, comme dans le modèle de facturation à l'utilisation. Dans ce cas, vous devez définir un quota sur la consommation de CPU globale en définissant l'allocation de CPU sur zéro et la limite de CPU sur une valeur différente de zéro. Vous pouvez également utiliser ce paramètre pour autoriser un quota de CPU illimité. Si ce nombre est défini sur illimité, les pools de ressources sur lesquels le VDC repose dans l'instance de vCenter Server obtiennent un nombre illimité de CPU.
Ressources de processeur garanties	Pourcentage d'allocation de CPU physiquement réservé au VDC.
Vitesse du vCPU	Vitesse de CPU virtuel par défaut pour les machines virtuelles dans le VDC.
Allocation de mémoire	Quantité de mémoire allouée à ce VDC en Mo ou Go. Ce paramètre définit la capacité totale de mémoire du VDC. La capacité totale de mémoire configurée par toutes les machines virtuelles exécutées dans le VDC ne peut pas dépasser cette valeur.
Ressources de mémoire garanties	Pourcentage d'allocation de mémoire physiquement réservée au VDC.
Nombre maximum de machines virtuelles	Nombre maximal de machines virtuelles dans le VDC.

En tant qu'**administrateur système de vCloud Director**, vous pouvez configurer un VDC d'organisation Flex pour qu'il soit élastique ou non élastique. Lorsque la fonctionnalité de pool élastique est activée sur les VDC d'organisation Flex, le VDC d'organisation s'étend et utilise tous les pools de ressources associés à son VDC fournisseur. Dans vCloud Director 9.7, si vous convertissez un VDC d'organisation non élastique en un VDC d'organisation élastique, vous ne pouvez pas reconvertir le même VDC d'organisation en un VDC non élastique.

Le modèle d'allocation Flex prend en charge les fonctionnalités des stratégies de dimensionnement de machine virtuelle sans les contraintes dont les autres modèles d'allocation font l'objet. Dans le modèle d'allocation Flex, l'allocation des ressources de calcul de la machine virtuelle dépend des stratégies de dimensionnement de machine virtuelle. Si vous ne définissez pas de stratégie de dimensionnement de machine virtuelle pour un VDC d'organisation, l'allocation des ressources de calcul dépend du modèle d'allocation de VDC d'organisation. À l'aide de la combinaison du modèle d'allocation Flex et des stratégies de dimensionnement de machine virtuelle d'organisation, un VDC d'organisation unique peut accueillir les machines virtuelles qui utilisent la configuration commune pour tous les autres modèles d'allocation. Pour plus d'informations, reportez-vous à la section Présentation des stratégies de positionnement et de dimensionnement de machine virtuelle .

Pour créer un VDC d'organisation Flex, vous pouvez utiliser le vCloud Director Service Provider Admin Portal ou l'API vCloud. Pour plus d'informations sur l'API vCloud, reportez-vous à la section *Guide de programmation de vCloud API pour fournisseurs de services*.

Modèle d'allocation de pool d'allocation

Avec le modèle d'allocation de pool d'allocation, un pourcentage des ressources que vous allouez à partir du centre de données virtuel (VDC, Virtual Data Center) fournisseur est attribué au VDC d'organisation. Vous pouvez définir le pourcentage pour le CPU et la mémoire. Ce pourcentage s'appelle facteur de pourcentage garanti et permet de surcharger des ressources.

En tant qu'administrateur système, vous pouvez configurer des VDC d'organisation de pool d'allocation pour qu'ils soient élastiques ou non élastiques. L'élasticité est un paramètre global qui affecte tous les VDC d'organisation à pool d'allocation. Reportez-vous à la section Modifier des paramètres système généraux.

Par défaut, un pool d'allocation élastique est activé pour les VDC d'organisation à pool d'allocation. Sur les systèmes mis à niveau à partir de vCloud Director 5.1, dans lesquels les VDC d'organisation à pool d'allocation comportent des machines virtuelles réparties sur plusieurs pools de ressources, le pool d'allocation élastique est activé par défaut.

Lorsque la fonctionnalité de pool d'allocation élastique est activée dans les VDC à pool d'allocation, le VDC d'organisation occupe et utilise tous les pools de ressources associés à son VDC fournisseur. Par conséquent, la fréquence du processeur virtuel est maintenant un paramètre obligatoire d'un pool d'allocations.

Définissez la fréquence de vCPU et le facteur de pourcentage garanti de sorte qu'un nombre suffisant de machines virtuelles puisse être déployé dans le VDC d'organisation sans que le CPU constitue un goulot d'étranglement.

Lors de la création d'une machine virtuelle, le moteur de placement place cette dernière dans un pool de ressources VDC fournisseur qui répond le mieux à ses besoins. Un pool de sous-ressources est créé pour ce VDC d'organisation sous le pool de ressources du VDC fournisseur et la machine virtuelle est placée sous le pool de sous-ressources.

Lors de l'activation de la machine virtuelle, le moteur de placement vérifie le pool de ressources du VDC fournisseur pour déterminer s'il dispose toujours de la capacité nécessaire à la mise sous tension de la machine virtuelle. Si tel n'est pas le cas, le moteur de placement transfère la machine virtuelle vers un pool de ressources VDC fournisseur disposant des ressources suffisantes pour exécuter la machine virtuelle. Un pool de sous-ressources est créé pour le VDC d'organisation s'il n'en existe pas.

Le pool de sous-ressources est configuré avec suffisamment de ressources pour exécuter la nouvelle machine virtuelle. La réservation de mémoire du pool de sous-ressources augmente de la taille de mémoire configurée de la machine virtuelle multipliée par le facteur de pourcentage garanti pour le VDC d'organisation. La réservation de CPU des pools de sous-ressources augmente du nombre de vCPU (vCPU) configuré pour les machines virtuelles multiplié par les vCPU spécifiés au niveau du VDC d'organisation, multiplié par le facteur de pourcentage garanti de processeur défini au niveau du VDC d'organisation. Si la fonctionnalité de pool d'allocation élastique est activée, la limite de mémoire du pool de sous-ressources augmente de la taille de mémoire configurée de la machine virtuelle, et la limite de CPU du pool de sous-ressources

augmente du nombre de vCPU configuré sur la machine virtuelle multiplié par la fréquence du vCPU spécifiée au niveau du VDC d'organisation. La machine virtuelle est reconfigurée pour définir sur zéro sa réservation de mémoire et de CPU et le moteur de placement des machines virtuelles la place dans un pool de ressources de VDC fournisseur.

Avec le modèle d'allocation de pool d'allocation élastique, les limites sont surveillées et gérées uniquement par vCloud Director. Si la fonctionnalité élastique est désactivée, la limite de pool de ressources est également définie.

Grâce au modèle de pool d'allocations, une machine virtuelle peut tirer parti des ressources d'une autre machine virtuelle inactive appartenant au même groupe de sous-ressources. Ce modèle permet de tirer parti des nouvelles ressources ajoutées au VDC fournisseur.

Dans de rares cas, une machine virtuelle passe du pool de ressources auquel elle était attribuée à sa création à un pool de ressources différent lors de l'activation à cause d'un manque de ressources sur le pool de ressources d'origine. Cela peut impliquer un faible coût pour déplacer les fichiers de disque de machine virtuelle vers un nouveau pool de ressources.

Lorsque la fonctionnalité de pool d'allocation élastique est désactivée, le comportement des VDC d'organisation à pool d'allocation est semblable au modèle de pool d'allocation de vCloud Director 1.5. Dans ce modèle, la fréquence du vCPU n'est pas configurable. La surcharge est contrôlée en définissant le pourcentage de ressources garanti.

Par défaut, dans un VDC de pool d'allocation, les machines virtuelles obtiennent leurs paramètres de réservation, de limite et de partage à partir des paramètres du VDC. Pour créer ou reconfigurer une machine virtuelle avec les paramètres d'allocation de ressources personnalisés pour le CPU et la mémoire, vous pouvez utiliser l'API vCloud. Reportez-vous à la section *Guide de programmation de vCloud API pour fournisseurs de services*.

Modèle d'allocation de facturation à l'utilisation

Dans le modèle d'allocation de facturation à l'utilisation, les ressources ne sont attribuées que lorsque les utilisateurs créent des vApp dans le VDC d'organisation. Vous pouvez spécifier un pourcentage de ressources à garantir, ce qui vous permet de surcharger des ressources. Vous pouvez rendre élastique un VDC d'organisation Facturation à l'utilisation en ajoutant plusieurs pools de ressources à son VDC fournisseur.

Les ressources attribuées à l'organisation sont appliquées au niveau de la machine virtuelle.

Lorsqu'une machine virtuelle est sous tension, si le pool de ressources d'origine ne peut pas accueillir la machine virtuelle, le moteur de placement vérifie le pool de ressources et attribue la machine virtuelle à un autre pool de ressources. Si aucun pool de sous-ressources n'est disponible pour le pool de ressources, vCloud Director en crée un avec une limite infinie et un débit de zéro. Le débit de la machine virtuelle est défini sur sa limite multipliée par ses ressources attribuées et le moteur de placement de machines virtuelles place la machine virtuelle dans un pool de ressources de VDC fournisseur.

Le modèle Facturation à l'utilisation offre l'avantage de pouvoir utiliser les nouvelles ressources ajoutées au VDC fournisseur.

Dans de rares cas, une machine virtuelle passe du pool de ressources auquel elle était attribuée à sa création à un pool de ressources différent lors de l'activation à cause d'un manque de ressources sur le pool de ressources d'origine. Cela peut impliquer un faible coût pour déplacer les fichiers de disque de machine virtuelle vers un nouveau pool de ressources.

Dans le modèle Facturation à l'utilisation, aucune ressource n'est réservée à l'avance ; une machine virtuelle peut donc ne pas parvenir à mettre sous tension s'il n'y a pas suffisamment de ressources. Des machines virtuelles fonctionnant sous ce modèle ne peuvent pas tirer parti des ressources des machines virtuelles inactives sur le même pool de sous-ressources, car les ressources sont définies au niveau de la machine virtuelle.

Par défaut, dans un VDC Facturation à l'utilisation, les machines virtuelles obtiennent leurs paramètres de réservation, de limite et de partage à partir des paramètres du VDC. Pour créer ou reconfigurer une machine virtuelle avec les paramètres d'allocation de ressources personnalisés pour le CPU et la mémoire, vous pouvez utiliser l'API vCloud. Reportez-vous au *Guide de programmation de vCloud API pour fournisseurs de services*.

Modèle d'allocation de pool de réservation

Avec le modèle d'allocation de pool de réservation, toutes les ressources que vous allouez sont immédiatement attribuées au VDC d'organisation. Les utilisateurs au sein de l'organisation peuvent contrôler la surcharge en spécifiant des paramètres de réservation, de limite et de priorité pour des machines virtuelles individuelles.

Comme ce modèle ne contient qu'un seul pool de ressources et qu'un seul pool de sous-ressources, le moteur de placement ne réattribue pas le pool de ressources d'une machine virtuelle lorsqu'elle est activée. Le débit et la limite de la machine virtuelle ne sont pas modifiés.

Avec le modèle Pool de réservation, des sources sont toujours disponibles lorsqu'elles sont nécessaires. Ce modèle offre également un contrôle très fin sur le débit, la limite et les partages de la machine virtuelle, ce qui peut permettre d'optimiser l'utilisation des ressources réservées si vous les prévoyez avec soin. Pour plus d'informations sur la configuration des paramètres d'allocation de ressources de machine virtuelle dans les VDC de pool de réservation, reportez-vous au *vCloud Air - Guide de l'utilisateur de Virtual Private Cloud OnDemand*.

Dans ce modèle, la réservation est toujours effectuée au niveau du cluster principal. Si la quantité de ressources est insuffisante pour créer un VDC d'organisation dans le cluster principal, la création de ce dernier échoue.

Les autres limites de ce modèle sont qu'il n'est pas élastique et que les utilisateurs de l'organisation peuvent définir des partages, des débits et des limites non optimaux sur les machines virtuelles, ce qui entraîne une sous-utilisation des ressources.

Présentation des stratégies de positionnement et de dimensionnement de machine virtuelle

Vous pouvez contrôler l'allocation et le positionnement des ressources de machine virtuelle (VM) sur un cluster ou un hôte spécifique à l'aide de stratégies de dimensionnement et de positionnement de machine virtuelle.

vCloud Director 10.0 introduit les concepts de stratégie de positionnement de machine virtuelle et de stratégie de dimensionnement de machine virtuelle.

Les vCloud Director **administrateurs système** créent et gèrent des stratégies de dimensionnement de machine virtuelle à un niveau global et peuvent publier des stratégies individuelles dans un ou plusieurs VDC d'organisation. Les stratégies de positionnement de machine virtuelle sont créées et gérées pour chaque VDC fournisseur, car une stratégie de positionnement de machine virtuelle est limitée au niveau du VDC fournisseur. Lorsque vous publiez une stratégie sur un VDC d'organisation, la stratégie devient disponible pour les utilisateurs dans l'organisation. Lors de la création et de la gestion de machines virtuelles dans le VDC d'organisation, les locataires peuvent attribuer les stratégies disponibles aux machines virtuelles. Les locataires et les utilisateurs du VDC d'organisation ne peuvent pas accéder à la configuration spécifique d'une stratégie de positionnement ou de dimensionnement de machine virtuelle.

Les stratégies de positionnement ou de dimensionnement de machine virtuelle constituent un mécanisme qui permet aux fournisseurs de cloud de définir et d'offrir des niveaux de service différenciés (par exemple, un profil gourmand en CPU ou un profil à forte utilisation de mémoire). Si vous publiez plusieurs stratégies de positionnement ou de dimensionnement de machine virtuelle sur un VDC d'organisation, les utilisateurs de locataire peuvent sélectionner entre toutes les stratégies personnalisées et la stratégie par défaut lors de la création et de la gestion des machines virtuelles dans le VDC d'organisation. La stratégie système par défaut est générée automatiquement pour chaque VDC. Les **administrateurs système** peuvent supprimer la stratégie système par défaut dans le VDC et marquer une autre stratégie personnalisée comme stratégie par défaut. La stratégie par défaut ne définit aucune valeur et autorise toutes les configurations de machine virtuelle.

Stratégie de positionnement de machine virtuelle

Une stratégie de positionnement de machine virtuelle définit le placement d'une machine virtuelle sur un hôte ou un groupe d'hôtes. Il s'agit d'un mécanisme destiné aux **administrateurs de fournisseurs de cloud** permettant de créer un groupe d'hôtes nommé au sein d'un VDC fournisseur. Le groupe d'hôtes nommé est un sous-ensemble des hôtes dans les clusters de VDC fournisseur qui peuvent être sélectionnés en fonction de critères tels que les niveaux de performance ou les licences. Une stratégie de positionnement de machine virtuelle définit des règles d'affinité machine virtuelle-hôte qui affectent directement le positionnement des charges de travail de locataire. Les administrateurs définissent ou exposent des groupes d'hôtes nommés en utilisant des groupes de machines virtuelles dans vCenter Server. Un groupe de machines virtuelles a une affinité directe avec un groupe d'hôtes et représente celui-ci.

Vous définissez la stratégie de positionnement de machine virtuelle au niveau du VDC fournisseur. Une stratégie de positionnement de machine virtuelle inclut les attributs suivants :

- Nom (doit être unique dans le VDC fournisseur)
- Description
- Ensemble d'un ou de plusieurs groupes de machines virtuelles sélectionnés dans les clusters sous-jacents du VDC fournisseur. Vous pouvez sélectionner un groupe de machines virtuelles par cluster

Une stratégie de positionnement de machine virtuelle est facultative lors de la création d'une machine virtuelle et un locataire ne peut attribuer qu'une seule stratégie de positionnement de machine virtuelle à une machine virtuelle.

Lorsqu'un locataire crée une machine virtuelle dans le VDC d'organisation et sélectionne la stratégie de positionnement de machine virtuelle, vCloud Director ajoute la machine virtuelle au groupe de machines virtuelles référencé dans la stratégie. Par conséquent, vCloud Director crée la machine virtuelle sur l'hôte approprié.

Une stratégie de positionnement de machine virtuelle peut avoir zéro ou un groupe de machines virtuelles issu de chaque cluster. Par exemple, la stratégie de calcul de positionnement de machine virtuelle *oracle_license* peut comprendre les groupes de machines virtuelles *oracle_license1* et *oracle_license2*, où le groupe de machines virtuelles *oracle_license1* appartient au cluster *oracle_cluster1* et le groupe de machines virtuelles *oracle_license2* appartient au cluster *oracle_cluster2*.

Lorsque vous attribuez une stratégie de positionnement de machine virtuelle à une machine virtuelle, le moteur de positionnement ajoute cette machine virtuelle au groupe de machines virtuelles correspondant dans le cluster sur lequel il réside. Par exemple, si vous choisissez de déployer une machine virtuelle sur un cluster *oracle_cluster1* et d'attribuer la stratégie de positionnement de machine virtuelle *oracle_license* à cette machine virtuelle, le moteur de positionnement ajoute la machine virtuelle au groupe de machines virtuelles *oracle_license1*.

Stratégie de dimensionnement de machine virtuelle

Une stratégie de dimensionnement de machine virtuelle définit l'allocation des ressources de calcul pour les machines virtuelles au sein d'un VDC d'organisation. L'allocation des ressources de calcul inclut l'allocation de CPU et de mémoire, les réservations, les limites et les parts.

Avec les stratégies de dimensionnement de machines virtuelles, les vCloud Director **administrateurs système** peuvent contrôler les aspects suivants de la consommation des ressources de calcul au niveau de la machine virtuelle :

- Nombre de vCPU et vitesse d'horloge de vCPU
- Quantité de mémoire allouée à la machine virtuelle.
- Mémoire et réservation de CPU, limite et parts
- Configurations supplémentaires.

Le paramètre d'API `extraConfigs` représente un mappage entre une clé et des paires de valeurs qui sont appliquées en tant que valeurs de configuration supplémentaires sur une machine virtuelle. Vous pouvez créer une stratégie avec des configurations supplémentaires uniquement au moyen de vCloud API. Les configurations supplémentaires existantes s'affichent dans l'interface utilisateur du Service Provider Admin Portal sous **Configurations supplémentaires** dans la vue détaillée de stratégie de dimensionnement de machine virtuelle.

Vous définissez les stratégies de dimensionnement de machine virtuelle à un niveau global. Pour plus d'informations sur les attributs de stratégie de dimensionnement de machine virtuelle, reportez-vous à la section Attributs des stratégies de dimensionnement de machine virtuelle.

vCloud Director génère une stratégie de dimensionnement de machine virtuelle par défaut pour tous les VDC. La stratégie de dimensionnement de machine virtuelle par défaut ne contient qu'un nom et une description, et tous les attributs de stratégie restants sont vides.

Vous pouvez également définir une autre stratégie de dimensionnement de machine virtuelle comme stratégie par défaut pour un VDC d'organisation. La stratégie de dimensionnement de machine virtuelle par défaut contrôle l'allocation et la consommation des ressources des machines virtuelles que les locataires créent dans le VDC d'organisation, sauf si un locataire attribue une autre stratégie de dimensionnement de machine virtuelle spécifique à la machine virtuelle.

Pour limiter le nombre maximal de ressources de calcul que les locataires peuvent allouer à des machines virtuelles spécifiques au sein d'un VDC d'organisation, les fournisseurs de cloud peuvent définir une stratégie de dimensionnement de machine virtuelle maximale. Lorsqu'elle est attribuée à un VDC d'organisation, la stratégie de dimensionnement de machine virtuelle maximale agit comme une limite supérieure pour la configuration des ressources de calcul de toutes les machines virtuelles dans le VDC d'organisation. La stratégie de dimensionnement de machine virtuelle maximale n'est pas disponible pour les utilisateurs de locataire lors de la création d'une machine virtuelle. Lorsque vous définissez une stratégie de dimensionnement de machine virtuelle comme stratégie maximale, vCloud Director copie en interne le contenu de la stratégie et utilise le contenu copié comme stratégie de dimensionnement de machine virtuelle maximale. Par conséquent, le VDC d'organisation ne dépend pas de la stratégie de dimensionnement de machine virtuelle initialement utilisée.

À l'aide de stratégies de dimensionnement de machine virtuelle, les fournisseurs de cloud peuvent limiter la consommation des ressources de calcul pour toutes les machines virtuelles d'un VDC d'organisation à, par exemple, trois tailles prédéfinies (telles que *Petite taille*, *Taille moyenne* et *Grande taille*). Le workflow est le suivant.

1 Un **administrateur système** crée trois stratégies de dimensionnement de machine virtuelle avec les attributs suivants :

Nom	Attributs
Petite taille	■ Description : stratégie de machine virtuelle de petite taille ■ Nom : Petite taille ■ Mémoire : 1024 ■ Nombre de vCPU : 1
Taille moyenne	■ Description : stratégie de machine virtuelle de taille moyenne ■ Nom : Taille moyenne ■ Mémoire : 2048 ■ Nombre de vCPU : 2
Grande taille	■ Description : stratégie de machine virtuelle de grande taille ■ Nom : Grande taille ■ Mémoire : 4096 ■ Nombre de vCPU : 4

2 Publiez les nouvelles stratégies de dimensionnement de machine virtuelle sur un VDC d'organisation.

3 Si vous le souhaitez, définissez l'une des stratégies de dimensionnement de machine virtuelle comme stratégie de dimensionnement de machine virtuelle par défaut pour le VDC d'organisation.

Les opérations de stratégie disponibles pour les fournisseurs de cloud sont les suivantes :

- Pour définir le placement d'une machine virtuelle sur un hôte ou un groupe d'hôtes, créez une stratégie de positionnement. Reportez-vous à Créer une stratégie de positionnement de VM.
- Pour contrôler l'allocation des ressources de calcul physique pour les charges de travail des locataires, créez une stratégie de dimensionnement. Reportez-vous à la section Créer une stratégie de dimensionnement de machine virtuelle.
- Publiez une stratégie de positionnement ou une stratégie de dimensionnement de machine virtuelle sur un ou plusieurs VDC d'organisation. Reportez-vous à Ajouter une stratégie de positionnement de machine virtuelle à un VDC d'organisation
- Définir une stratégie de positionnement de machine virtuelle ou de dimensionnement de machine virtuelle comme valeur par défaut.
- Modifier une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle. Vous pouvez uniquement modifier le nom et la description de la stratégie dans l'interface utilisateur de vCloud Director.

- Annuler la publication d'une stratégie de positionnement de machine virtuelle ou d'une stratégie de dimensionnement de machine virtuelle à partir d'un VDC d'organisation.
- Supprimer une stratégie de positionnement de machine virtuelle ou une stratégie de dimensionnement de machine virtuelle. Reportez-vous à Supprimer une stratégie de positionnement de machine virtuelle et à Supprimer une stratégie de dimensionnement de machine virtuelle.

Les utilisateurs disposant du droit **ORG_VDC_MANAGE_COMPUTE_POLICIES** peuvent créer, mettre à jour et publier des stratégies de positionnement de machine virtuelle ou de dimensionnement de machine virtuelle .

Le tableau suivant répertorie les opérations de stratégie de dimensionnement de machine virtuelle ou de positionnement de machine virtuelle pour les utilisateurs de locataire.

Tableau 6-1. Opérations de stratégie de dimensionnement de machine virtuelle et de stratégie de positionnement de machine virtuelle pour les utilisateurs de locataire

Opération	Description
Attribuez une stratégie à une machine virtuelle pendant la création d'une machine virtuelle.	Les utilisateurs de locataire autorisés à créer des machines virtuelles dans un VDC d'organisation peuvent éventuellement attribuer des stratégies de dimensionnement de machine virtuelle et de positionnement de machine virtuelle à des machines virtuelles en utilisant le vCloud Director Tenant Portal. Par conséquent, les paramètres définis dans la stratégie de dimensionnement de machine virtuelle contrôlent la consommation de CPU et de mémoire de la machine virtuelle. L'attribution d'une stratégie de positionnement ou de dimensionnement de machine virtuelle n'est pas requise pour les locataires lors de la création d'une machine virtuelle. Si un locataire ne sélectionne pas explicitement une stratégie de dimensionnement de machine virtuelle à attribuer à une machine virtuelle, le dimensionnement de machine virtuelle par défaut est appliqué à la machine virtuelle. Si vous ne créez pas de stratégie de positionnement de machine virtuelle, l'option de stratégie de positionnement de machine virtuelle n'est pas visible par les locataires. Si le locataire sélectionne une stratégie de positionnement incluant des informations de dimensionnement, l'option de stratégie de dimensionnement de machine virtuelle devient masquée pour le locataire. Vous pouvez créer une stratégie de positionnement de machine virtuelle avec des informations de dimensionnement uniquement à l'aide de vCloud API. S'il n'existe qu'une seule stratégie de dimensionnement de machine virtuelle, l'option de stratégie de dimensionnement de machine virtuelle n'est pas visible par les locataires. Lorsque l'**administrateur système** définit les attributs **Nombre de vCPU**, **Cœurs par socket** et **Mémoire** dans une stratégie de dimensionnement de machine virtuelle, si un locataire sélectionne la stratégie, ces valeurs sont affichées, mais ne sont pas modifiables.
Attribuez une stratégie à une machine virtuelle existante.	Les utilisateurs de locataire autorisés à gérer des machines virtuelles dans un VDC d'organisation peuvent attribuer ou modifier les stratégies de dimensionnement de machine virtuelle et de positionnement de machine virtuelle d'une machine virtuelle existante à l'aide du vCloud Director Tenant Portal. Lorsqu'un locataire modifie la stratégie de positionnement de machine virtuelle, la machine virtuelle se déplace vers un nouvel hôte conformément à la règle d'affinité machine virtuelle/hôte définie dans la nouvelle stratégie de positionnement de machine virtuelle. Lorsqu'un locataire modifie une stratégie de dimensionnement de machine virtuelle, le système reconfigure la machine virtuelle pour consommer des ressources de calcul telles que spécifiées dans la nouvelle stratégie de dimensionnement de machine virtuelle.

Le workflow d'utilisation des stratégies de positionnement de machine virtuelle et de dimensionnement de machine virtuelle est le suivant.

1 Un **administrateur système** crée une ou plusieurs stratégies de positionnement de machine virtuelle. Reportez-vous à Créer une stratégie de positionnement de VM.

2 Un **administrateur système** crée une ou plusieurs stratégies de dimensionnement de machine virtuelle. Reportez-vous à Créer une stratégie de dimensionnement de machine virtuelle.

   Le nom d'une stratégie de dimensionnement de machine virtuelle est unique dans un site vCloud Director. Le nom d'une stratégie de positionnement de machine virtuelle est unique dans la portée du VDC fournisseur de la stratégie.

3 Un **administrateur système** publie les stratégies de positionnement de machine virtuelle et de dimensionnement de machine virtuelle sur un ou plusieurs VDC d'organisation. Reportez-vous à la section Ajouter une stratégie de positionnement de machine virtuelle à un VDC d'organisation.

   La publication d'une stratégie de positionnement de machine virtuelle la rend disponible pour les utilisateurs de locataire dans les VDC d'organisation lors de la création et de la modification de machine virtuelle.

4 Lors de la création ou de la mise à jour d'une machine virtuelle, les locataires peuvent utiliser l'API vCloud ou vCloud Director Tenant Portal pour attribuer une stratégie de dimensionnement de machine virtuelle et une stratégie de positionnement de machine virtuelle à une machine virtuelle.

Attributs des stratégies de dimensionnement de machine virtuelle

Lorsque vous créez une stratégie de dimensionnement de machine virtuelle (VM), vous pouvez spécifier un sous-ensemble de tous les attributs disponibles. Le seul attribut obligatoire est le nom de la stratégie de dimensionnement de machine virtuelle.

Il existe deux types de paramètres dans une stratégie de dimensionnement de machine virtuelle.

- Configuration de dimensionnement de machine virtuelle individuelle : vous préconfigurez la RAM, le nombre de vCPU et les cœurs spécifiés par socket pour les machines virtuelles sous la stratégie actuelle.
- Contraintes relatives au nombre maximal de ressources : vous préconfigurez une limite pour la consommation de mémoire et de CPU par une seule machine virtuelle sous la stratégie actuelle.

Le tableau suivant répertorie tous les attributs que vous pouvez définir dans une stratégie de dimensionnement de machine virtuelle.

Tableau 6-2. Attributs de stratégie de calcul de VDC

Attribut de stratégie de calcul de VDC	Paramètre API	Description
Name	name	Paramètre obligatoire utilisé comme identifiant pour la stratégie de dimensionnement de machine virtuelle.
Description	description	Représente une brève description de la stratégie de dimensionnement de machine virtuelle.
vCPU Speed	cpuSpeed	Définit la vitesse de vCPU d'un cœur en MHz ou GHz.
vCPU Count	cpuCount	Définit le nombre de vCPU configurés pour une machine virtuelle. Il s'agit d'une configuration matérielle de machine virtuelle. Lorsqu'un locataire attribue la stratégie de dimensionnement de machine virtuelle à une machine virtuelle, ce nombre devient le nombre configuré de vCPU pour la machine virtuelle.

Tableau 6-2. Attributs de stratégie de calcul de VDC (suite)

Attribut de stratégie de calcul de VDC	Paramètre API	Description
Cores Per Socket	coresPerSocket	Nombre de cœurs par socket pour une machine virtuelle. Il s'agit d'une configuration matérielle de machine virtuelle. Le nombre de vCPU qui est défini dans la stratégie de dimensionnement de machine virtuelle doit être divisible par le nombre de cœurs par socket. Si le nombre de vCPU n'est pas divisible par le nombre de cœurs par socket, le nombre de cœurs par socket devient non valide.
CPU Reservation Guarantee	cpuReservationGuarantee	Définit la quantité réservée de ressources de CPU d'une machine virtuelle. La quantité de CPU allouée pour une machine virtuelle est égale au nombre de vCPU multiplié par la vitesse du vCPU en MHz. La valeur des attributs est comprise entre 0 et un. La valeur de la garantie de réservation de CPU nulle ne définit aucune réservation de CPU. La valeur 1 définit 100 % de CPU réservé.
CPU Limit	cpuLimit	Définit la limite de CPU en MHz ou GHz pour une machine virtuelle. Si elle n'est pas définie dans la stratégie de calcul de VDC, la limite de CPU est égale à la vitesse de vCPU multipliée par le nombre de vCPU.
CPU Shares	cpuShares	Définit le nombre de parts de CPU d'une machine virtuelle. Les parts définissent l'importance relative d'une machine virtuelle dans un centre de données de données virtuel. Si une machine virtuelle possède deux fois plus de parts de CPU qu'une autre machine virtuelle, elle est autorisée à consommer le double de CPU lorsque ces deux machines virtuelles sont en compétition pour les ressources. Si cet attribut n'est pas défini dans la stratégie de calcul de VDC, les partages normaux sont appliqués à la machine virtuelle.
Memory	memory	Définit la mémoire configurée pour une machine virtuelle en Mo ou en Go. Il s'agit d'une configuration matérielle de machine virtuelle. Lorsqu'un locataire attribue la stratégie de dimensionnement de machine virtuelle à une machine virtuelle, celle-ci reçoit la quantité de mémoire définie par cet attribut.
Memory Reservation Guarantee	memoryReservationGuarantee	Définit la quantité de mémoire réservée qui est configurée pour une machine virtuelle. La valeur des plages d'attributs se situe entre 0 et 100 %.
Memory Limit	memoryLimit	Définit la limite de mémoire en Mo ou en Go pour une machine virtuelle. Si elle n'est pas définie dans la stratégie de dimensionnement de machine virtuelle, la limite de mémoire est égale à la mémoire allouée pour la machine virtuelle.

Tableau 6-2. Attributs de stratégie de calcul de VDC (suite)

Attribut de stratégie de calcul de VDC	Paramètre API	Description
Memory Shares	memoryShares	Définit le nombre de parts de mémoire pour une machine virtuelle. Les parts définissent l'importance relative d'une machine virtuelle dans un centre de données de données virtuel. Si une machine virtuelle possède deux fois plus de parts de mémoire qu'une autre machine virtuelle, elle est autorisée à consommer le double de mémoire lorsque ces deux machines virtuelles sont en compétition pour les ressources. Si cet attribut n'est pas défini dans la stratégie de calcul de VDC, les partages normaux sont appliqués à la machine virtuelle.
Extra Configurations	extraConfigs	Représente un mappage entre une clé et des paires de valeurs qui sont appliquées en tant que valeurs de configuration supplémentaires sur une machine virtuelle. Vous pouvez créer une stratégie avec des configurations supplémentaires uniquement via l'API vCloud. Les configurations supplémentaires existantes s'affichent dans l'interface utilisateur de Service Provider Admin Portal sous **Configurations supplémentaires** dans la vue de stratégie de dimensionnement de machine virtuelle détaillée.

Créer une stratégie de positionnement de VM

Une stratégie de positionnement de machine virtuelle est une stratégie de calcul de VDC qui contient une référence à une stratégie de VDC fournisseur. Vous pouvez utiliser une stratégie de positionnement de machine virtuelle pour définir le placement d'une machine virtuelle sur un hôte spécifique, un groupe d'hôtes ou un cluster.

Conditions préalables

- Vérifiez que vous disposez d'au moins un VDC fournisseur dans votre environnement.
- Vérifiez que vous disposez d'au moins un groupe de machines virtuelles dans votre environnement.

  Un groupe de machines virtuelles est un ensemble de machines virtuelles que vous pouvez lier à un groupe d'hôtes avec des affinités positives ou négatives. À l'aide d'une règle d'affinité positive, vous pouvez placer un groupe de machines virtuelles sur un hôte spécifique. La règle d'anti-affinité ou d'affinité négative place un groupe de machines virtuelles sur différents hôtes, ce qui empêche l'échec simultané de toutes les machines virtuelles en cas d'échec d'un seul hôte. Vous pouvez créer un groupe de machines virtuelles via l'interface utilisateur de vCenter Server ou l'API vCloud Director.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.
3. Sélectionnez un VDC fournisseur dans la liste.

4 Cliquez sur l'onglet **Stratégies de placement de VM**, puis sur **Nouveau**.

5 (Facultatif) Sur la page **Quelle est la stratégie de positionnement de VM** de l'Assistant, cochez la case pour arrêter d'afficher les informations sur la stratégie de positionnement de machine virtuelle.

6 Cliquez sur **Suivant**.

7 Entrez un nom pour la stratégie de positionnement de machine virtuelle et, éventuellement, une description.

8 Sélectionnez les groupes de machines virtuelles ou les groupes de machines virtuelles logiques auxquels vous souhaitez lier la machine virtuelle et cliquez sur **Suivant**.

   Lorsque vous sélectionnez plusieurs groupes logiques, si un locataire applique cette stratégie à une machine virtuelle, celle-ci devient membre de tous les groupes de machines virtuelles inclus dans les groupes de machines virtuelles logiques sélectionnés. La machine virtuelle est conditionnée par une combinaison de toutes les affinités qui s'appliquent aux machines virtuelles de ces groupes.

   Vous pouvez créer un groupe de machines virtuelles logiques en ligne en sélectionnant un groupe de machines virtuelles par cluster. Ce groupe de machines virtuelles logiques n'a pas de nom et ne peut être utilisé que pour la stratégie de positionnement de machine virtuelle sélectionnée.

9 Vérifiez les paramètres de la stratégie de positionnement de machine virtuelle et cliquez sur **Terminer**.

Étape suivante

- Créer une stratégie de dimensionnement de machine virtuelle.
- Ajouter une stratégie de positionnement de machine virtuelle à un VDC d'organisation.

Ajouter une stratégie de positionnement de machine virtuelle à un VDC d'organisation

Lorsque vous créez une stratégie de positionnement de machine virtuelle, elle n'est pas visible par les locataires. Vous pouvez publier des stratégies de positionnement de machine virtuelle dans un VDC d'organisation pour les rendre disponibles pour les locataires.

La publication d'une stratégie de positionnement de machine virtuelle sur un VDC d'organisation rend la stratégie visible par les locataires. Le locataire peut sélectionner la stratégie lors de la création d'une machine virtuelle autonome ou d'une machine virtuelle à partir d'un modèle, de la modification d'une machine virtuelle, de l'ajout d'une machine virtuelle à un vApp et de la création d'un vApp à partir d'un modèle de vApp. Vous ne pouvez pas supprimer une stratégie de positionnement de machine virtuelle disponible pour les locataires.

Conditions préalables

- Vérifiez que vous disposez d'au moins un VDC d'organisation dans votre environnement. Reportez-vous à Créer un centre de données virtuel d'organisation.

- Vérifiez que vous disposez d'au moins une stratégie de positionnement de machine virtuelle. Reportez-vous à Créer une stratégie de positionnement de VM.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Sélectionnez un VDC d'organisation et cliquez sur l'onglet **Stratégies de positionnement de VM**.
4. Cliquez sur **Ajouter**.
5. Sélectionnez les stratégies de positionnement de machine virtuelle que vous souhaitez ajouter au VDC d'organisation, puis cliquez sur **OK**.

Étape suivante

- Sélectionnez une stratégie et cliquez sur **Supprimer** pour annuler la publication de la stratégie.
- Sélectionnez une stratégie de positionnement de machine virtuelle, puis cliquez sur **Définir comme valeur par défaut** pour que cette stratégie s'affiche comme choix par défaut pour les locataires pendant la création d'une machine virtuelle et d'un vApp, ainsi que pendant la modification d'une machine virtuelle. Si plusieurs stratégies de positionnement de machine virtuelle sont publiées pour un VDC d'organisation, le locataire peut sélectionner une stratégie différente de la stratégie par défaut.

Supprimer une stratégie de positionnement de machine virtuelle

Si une stratégie de positionnement de machine virtuelle n'est pas publiée pour les locataires, vous pouvez la supprimer du VDC fournisseur.

Conditions préalables

- Vérifiez que vous disposez d'au moins une stratégie de positionnement de machine virtuelle dans votre environnement.
- Vérifiez que la stratégie de positionnement de machine virtuelle n'est pas ajoutée à un VDC d'organisation. Vous ne pouvez pas supprimer les stratégies de positionnement de machine virtuelle disponibles pour les locataires.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**.
3. Sélectionnez un VDC fournisseur dans la liste.
4. Cliquez sur l'onglet **Stratégies de positionnement de VM** et sélectionnez une stratégie de positionnement de machine virtuelle.

5 Cliquez sur **Supprimer**.

Créer une stratégie de dimensionnement de machine virtuelle

Vous pouvez créer une stratégie de dimensionnement de machine virtuelle pour rendre disponible aux locataires des contraintes de consommation de CPU et de mémoire prédéfinies qu'ils peuvent appliquer à des machines virtuelles individuelles dans un VDC d'organisation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Stratégies de dimensionnement de VM**.

3 Cliquez sur **Nouveau**.

4 Entrez un nom pour la stratégie de dimensionnement de machine virtuelle et, éventuellement, une description.

5 Cliquez sur **Suivant**.

6 Sur la page **CPU**, sélectionnez les paramètres d'allocation de CPU que vous souhaitez appliquer à la stratégie et cliquez sur **Suivant**.

7 Sélectionnez les paramètres d'allocation de mémoire que vous souhaitez appliquer à la stratégie et cliquez sur **Suivant**.

8 Vérifiez les paramètres de la stratégie de dimensionnement de machine virtuelle et cliquez sur **Terminer**.

Étape suivante

- Après avoir créé une stratégie de dimensionnement de machine virtuelle, vous pouvez uniquement modifier le nom et la description de la stratégie de dimensionnement de machine virtuelle. Reportez-vous à la section Modifier une stratégie de dimensionnement de machine virtuelle.
- Ajouter une stratégie de dimensionnement de machine virtuelle à un VDC d'organisation.
- Créer une stratégie de positionnement de VM.

Ajouter une stratégie de dimensionnement de machine virtuelle à un VDC d'organisation

Lorsque vous créez une stratégie de dimensionnement de machine virtuelle, elle n'est pas visible par les locataires. Vous pouvez publier une stratégie de dimensionnement de machine virtuelle dans un VDC d'organisation pour la rendre disponible pour les locataires.

La publication d'une stratégie de dimensionnement de machine virtuelle sur un VDC d'organisation rend la stratégie visible par les locataires. Le locataire peut sélectionner la stratégie lors de la création d'une machine virtuelle autonome ou d'une machine virtuelle à partir d'un modèle, de la modification d'une machine virtuelle, de l'ajout d'une machine virtuelle à un vApp et de la création d'un vApp à partir d'un modèle de vApp. Vous ne pouvez pas supprimer une stratégie de dimensionnement de machine virtuelle disponible pour les locataires.

Conditions préalables

- Vérifiez que vous disposez d'au moins un VDC d'organisation dans votre environnement. Reportez-vous à la section Créer un centre de données virtuel d'organisation.
- Vérifiez que vous disposez d'au moins une stratégie de dimensionnement de machine virtuelle. Reportez-vous à la section Créer une stratégie de dimensionnement de machine virtuelle.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Sélectionnez un VDC d'organisation et cliquez sur l'onglet **Stratégies de dimensionnement de VM**.
4. Cliquez sur **Ajouter**.
5. Sélectionnez les stratégies de dimensionnement de machine virtuelle que vous souhaitez ajouter au VDC d'organisation, puis cliquez sur **OK**.

Étape suivante

- Sélectionnez une stratégie et cliquez sur **Supprimer** pour annuler la publication de la stratégie.
- Sélectionnez une stratégie de dimensionnement de machine virtuelle et cliquez sur **Définir comme valeur par défaut** pour que cette stratégie s'affiche comme choix par défaut pour les locataires pendant la création d'une machine virtuelle et d'un vApp ainsi que pendant la modification d'une machine virtuelle. Si plusieurs stratégies de dimensionnement de machine virtuelle sont publiées pour un VDC d'organisation, le locataire peut sélectionner une stratégie différente de la stratégie par défaut.

Modifier une stratégie de dimensionnement de machine virtuelle

Après avoir créé une stratégie de dimensionnement de machine virtuelle, vous pouvez uniquement modifier son nom et sa description. La modification des paramètres de CPU et de mémoire n'est pas prise en charge.

Conditions préalables

- Vérifiez que vous disposez d'au moins un VDC d'organisation dans votre environnement. Reportez-vous à Créer un centre de données virtuel d'organisation.
- Vérifiez que vous disposez d'au moins une stratégie de dimensionnement de machine virtuelle. Reportez-vous à Créer une stratégie de dimensionnement de machine virtuelle.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Stratégies de dimensionnement de VM**.
3. Cliquez sur le nom de la stratégie de dimensionnement de machine virtuelle que vous souhaitez modifier.
4. Pour modifier le nom et la description de la stratégie, cliquez sur **Modifier**.
5. Cliquez sur **Enregistrer**.

Étape suivante

Ajouter une stratégie de dimensionnement de machine virtuelle à un VDC d'organisation

Supprimer une stratégie de dimensionnement de machine virtuelle

Vous pouvez supprimer des stratégies de dimensionnement de machine virtuelle qui ne sont pas publiées pour les locataires.

Conditions préalables

- Vérifiez que vous disposez d'au moins une stratégie de dimensionnement de machine virtuelle dans votre environnement.
- Vérifiez que la stratégie de dimensionnement de machine virtuelle n'est pas ajoutée à un VDC d'organisation. Vous ne pouvez pas supprimer les stratégies de dimensionnement de machine virtuelle disponibles pour les locataires.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Stratégies de dimensionnement de VM**.
3. Sélectionnez une stratégie de dimensionnement de machine virtuelle et cliquez sur **Supprimer**.

Créer un centre de données virtuel d'organisation

Pour allouer des ressources à une organisation, vous devez créer un centre de données virtuel d'organisation. Un centre de données virtuel d'organisation obtient ses ressources d'un centre

de données virtuel fournisseur. Une organisation peut posséder plusieurs centres de données virtuels d'organisation.

Conditions préalables

Créez un centre de données virtuel fournisseur. Reportez-vous à Créer un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC d'organisation**, puis sur **Nouveau**.
3. Entrez un nom et, éventuellement, une description pour le nouveau centre de données virtuel d'organisation.
4. (Facultatif) Pour désactiver le nouveau centre de données virtuel d'organisation lors de la création, désactivez le bouton bascule **Activer le VDC d'organisation**.

   Les utilisateurs ne peuvent pas déployer de vApp sur un centre de données virtuel d'organisation désactivé.
5. Cliquez sur **Suivant**.
6. Sélectionnez le bouton radio situé en regard du nom de l'organisation à laquelle vous souhaitez ajouter ce centre de données virtuel, puis cliquez sur **Suivant**.
7. Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel fournisseur à partir duquel vous souhaitez que le centre de données virtuel d'organisation obtienne des ressources de calcul et de stockage, puis cliquez sur **Suivant**.

   La liste du centre de données virtuel fournisseur affiche tous les centres de données virtuels fournisseurs activés sur le site avec des informations sur les ressources disponibles. La liste des réseaux affiche des informations sur les réseaux disponibles pour le centre de données virtuel fournisseur sélectionné.
8. Sélectionnez un modèle d'allocation pour ce centre de données virtuel d'organisation, puis cliquez sur **Suivant**.

Option	Description
Pool d'allocation	Un pourcentage des ressources que vous allouez depuis le centre de données virtuel fournisseur est attribué au centre de données virtuel d'organisation. Vous pouvez définir le pourcentage pour le processeur et la mémoire.
Facturation à l'utilisation	Les ressources sont attribuées uniquement lorsque les utilisateurs créent des vApp dans le centre de données virtuel d'organisation.

Option	Description
Pool de réservation	Toutes les ressources que vous allouez sont immédiatement attribuées au centre de données virtuel d'organisation.
Flex	Vous pouvez contrôler la consommation des ressources à la fois sur le VDC et sur les machines virtuelles spécifiques. Le modèle d'allocation Flex prend en charge les fonctionnalités des stratégies de calcul de VDC d'organisation. Le modèle d'allocation Flex prend en charge toutes les configurations d'allocation disponibles dans les autres modèles d'allocation.

9 Configurez les paramètres d'allocation du modèle d'allocation que vous avez sélectionné, puis cliquez sur **Suivant**.

Option	Description	Modèle d'allocation
Élasticité	Activez ou désactivez la fonctionnalité de pool élastique. Un VDC d'organisation élastique s'étend à tous les pools de ressources associés à son VDC fournisseur et les utilise.	Flex
Inclure la capacité supplémentaire de mémoire de VM	Incluez ou excluez la capacité supplémentaire de mémoire.	Flex
Allocation de processeur	La quantité maximale de CPU que vous souhaitez allouer aux machines virtuelles exécutées dans ce centre de données virtuel d'organisation.	■ Pool d'allocation ■ Pool de réservation ■ Flex
Permettre aux ressources de CPU de dépasser	Pour fournir des ressources de CPU illimitées au centre de données virtuel d'organisation, activez ce bouton radio.	Pool de réservation
Quota de processeur	La quantité maximale de consommation de CPU pour ce centre de données virtuel d'organisation.	■ Facturation à l'utilisation ■ Flex
Ressources de CPU garanties	Le pourcentage de ressources de CPU que vous souhaitez garantir à une machine virtuelle exécutée dans ce centre de données virtuel d'organisation. Vous pouvez contrôler la surcharge des ressources de CPU en garantissant moins de 100 %. Pour un modèle d'allocation de pool d'allocation, le pourcentage garanti détermine également le pourcentage d'allocation de CPU validé pour le centre de données virtuel d'organisation.	■ Pool d'allocation ■ Facturation à l'utilisation ■ Flex
Vitesse du vCPU	La vitesse du vCPU. Cette vitesse en GHz par vCPU est affectée aux machines virtuelles exécutées dans le centre de données virtuel d'organisation.	■ Facturation à l'utilisation ■ Flex
Allocation de mémoire	La quantité maximale de mémoire que vous souhaitez allouer aux machines virtuelles exécutées dans le centre de données virtuel d'organisation.	■ Pool d'allocation ■ Pool de réservation
Quota de mémoire	La quantité maximale de consommation de mémoire pour ce centre de données virtuel d'organisation.	■ Facturation à l'utilisation ■ Flex

Option	Description	Modèle d'allocation
Ressources de mémoire garanties	Le pourcentage de ressources de mémoire que vous souhaitez garantir aux machines virtuelles exécutées dans le centre de données virtuel d'organisation. Vous pouvez surcharger des ressources en garantissant moins de 100 %. Pour un modèle d'allocation de pool d'allocation, le pourcentage garanti détermine également le pourcentage d'allocation de mémoire validé pour le centre de données virtuel d'organisation.	■ Pool d'allocation ■ Facturation à l'utilisation ■ Flex
Nombre maximal de VM	Le nombre maximal de machines virtuelles pouvant exister dans le centre de données virtuel d'organisation.	■ Pool d'allocation ■ Facturation à l'utilisation ■ Pool de réservation ■ Flex

10 Configurez les paramètres de stockage de ce centre de données virtuel d'organisation, puis cliquez sur **Suivant**.

La liste contient les stratégies de stockage activées sur le centre de données virtuel fournisseur source.

a Cochez les cases correspondant à une ou plusieurs stratégies de stockage que vous souhaitez ajouter à ce centre de données virtuel d'organisation.

b (Facultatif) Pour limiter la capacité de stockage allouée à une stratégie de stockage sélectionnée, sélectionnez **Limité** dans le menu déroulant de la cellule **Type d'allocation**, puis entrez la capacité maximale dans la cellule **Stockage alloué**.

c (Facultatif) Pour modifier la stratégie de stockage par défaut, dans le menu déroulant **Stratégie d'instanciation par défaut**, sélectionnez la stratégie de stockage par défaut cible.

vCloud Director utilise la stratégie de stockage par défaut pour toutes les opérations de provisionnement de machines virtuelles dans lesquelles la stratégie de stockage n'est pas spécifiée au niveau de la machine virtuelle ou du modèle de vApp.

d (Facultatif) Pour activer le provisionnement dynamique pour les machines virtuelles dans le centre de données virtuel d'organisation, activez le commutateur **Provisionnement dynamique**.

e (Facultatif) Pour désactiver le provisionnement rapide pour les machines virtuelles dans le centre de données virtuel d'organisation, désactivez le commutateur **Provisionnement rapide**.

11 Configurez les paramètres de pool de réseaux de ce centre de données virtuel d'organisation, puis cliquez sur **Suivant**.

vCloud Director utilise le pool de réseaux pour créer des réseaux vApp et des réseaux de centre de données virtuel d'organisation internes.

- Pour ignorer l'ajout d'un pool de réseaux à ce stade, désactivez le commutateur **Utiliser le pool de réseaux**.

- Pour configurer un pool de réseaux, sélectionnez le bouton radio situé en regard du nom du pool de réseaux cible, puis entrez le quota de ce centre de données virtuel d'organisation.

  Le quota est le nombre maximal de réseaux provisionnés dans le centre de données virtuel d'organisation dépendant de ce pool de réseaux. Il ne doit pas dépasser le nombre de réseaux disponibles pour le pool de réseaux sélectionné.

12 Vérifiez la page **Prêt à terminer** et cliquez sur **Terminer**.

Activer ou désactiver un centre de données virtuel d'organisation

Pour empêcher des machines virtuelles et des vApp supplémentaires d'utiliser des ressources de calcul et de stockage à partir d'un centre de données virtuel d'organisation, vous pouvez désactiver ce centre de données virtuel d'organisation. Les vApp en cours d'exécution et les machines virtuelles sous tension continuent à s'exécuter, mais vous ne pouvez ni créer ni démarrer d'autres vApp ou machines virtuelles.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Désactiver** ou **Activer**.

4 Pour confirmer, cliquez sur **OK**.

Supprimer un centre de données virtuel d'organisation

Pour supprimer toutes les ressources d'un centre de données virtuel fournisseur d'une organisation, vous pouvez supprimer ce centre de données virtuel d'organisation. Les ressources demeurent inchangées dans le centre de données virtuel fournisseur source.

Important Cette opération supprime définitivement le centre de données virtuel d'organisation et toutes ses machines virtuelles, vApp, réseaux de centre de données virtuel d'organisation et passerelles Edge.

Conditions préalables

Si vous souhaitez conserver certaines machines virtuelles, vApp, modèles de vApp ou fichiers de support qui appartiennent au centre de données virtuel d'organisation cible, déplacez-les vers un autre centre de données virtuel d'organisation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation à supprimer, puis cliquez sur **Supprimer**.

4 Si ce centre de données virtuel d'organisation contient des ressources (par exemple, des machines virtuelles, des vApp, des réseaux de centre de données virtuel d'organisation et des passerelles Edge), pour confirmer leur suppression, cochez la case associée à chaque type de ressource.

5 Pour confirmer, cliquez sur **Supprimer**.

Modifier le nom et la description d'un centre de données virtuel d'organisation

À mesure que votre installation de vCloud Director s'étend, vous souhaiterez peut-être attribuer un nom ou une description plus significatifs à un centre de données virtuel d'organisation existant.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Sous l'onglet **Général**, dans le coin supérieur droit, cliquez sur **Modifier**.

4 Entrez un nouveau nom et une nouvelle description, puis cliquez sur **Enregistrer**.

Modifier les paramètres de modèle d'allocation d'un centre de données virtuel d'organisation

Vous ne pouvez pas changer le modèle d'allocation d'un centre de données virtuel d'organisation, mais vous pouvez changer les paramètres d'allocation du modèle d'allocation que vous avez spécifié lors de la création du centre de données virtuel d'organisation.

Vous pouvez modifier les paramètres d'allocation du modèle d'allocation que vous avez configuré lors de la création du centre de données virtuel d'organisation. Reportez-vous à Étape 9.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Sous l'onglet **Allocation**, dans le coin supérieur droit, cliquez sur **Modifier**.

4 Modifiez les paramètres de modèle d'allocation, puis cliquez sur **Enregistrer**.

Modification des paramètres de stockage d'un centre de données virtuel d'organisation

Vous pouvez modifier les paramètres de stockage que vous avez configurés lors de la création du centre de données virtuel d'organisation.

Modifier les paramètres de provisionnement de machine virtuelle d'un centre de données virtuel d'organisation

Vous pouvez modifier les paramètres de provisionnement dynamique et de provisionnement rapide de machines virtuelles que vous avez configurés lors de la création du centre de données virtuel d'organisation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Dans l'onglet **Stockage**, dans le coin supérieur droit, cliquez sur **Modifier**.

4 (Facultatif) Modifiez le paramètre de provisionnement dynamique.

- Pour désactiver le provisionnement dynamique des machines virtuelles dans le centre de données virtuel d'organisation, désactivez l'option **Provisionnement dynamique**.
- Pour activer le provisionnement dynamique des machines virtuelles dans le centre de données virtuel d'organisation, activez l'option **Provisionnement dynamique**.

5 (Facultatif) Modifiez le paramètre de provisionnement rapide.

- Pour activer le provisionnement rapide des machines virtuelles dans le centre de données virtuel d'organisation, activez l'option **Provisionnement rapide**.
- Pour désactiver le provisionnement rapide pour les machines virtuelles dans le centre de données virtuel d'organisation, désactivez le commutateur **Provisionnement rapide**.

6 Cliquez sur **Modifier**.

Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel d'organisation

Vous pouvez configurer un centre de données virtuel d'organisation pour qu'il prenne en charge une stratégie de stockage de machine virtuelle que vous avez précédemment ajoutée au centre de données virtuel fournisseur sous-jacent.

Conditions préalables

Vous avez ajouté la stratégie de stockage de machine virtuelle cible au centre de données virtuel fournisseur source. Reportez-vous à Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.
3. Cliquez sur l'onglet **Stockage**, puis sur **Ajouter**.

   Vous pouvez voir une liste des stratégies de stockage supplémentaires disponibles dans le centre de données virtuel du fournisseur source.
4. Cochez la case de l'une ou plusieurs stratégies de stockage à ajouter, puis cliquez sur **Ajouter**.

Modifier la stratégie de stockage par défaut sur un centre de données virtuel d'organisation

Vous pouvez modifier la stratégie de stockage par défaut que vous avez configurée lors de la création d'un centre de données virtuel d'organisation.

vCloud Director utilise la stratégie de stockage par défaut pour toutes les opérations de provisionnement de machines virtuelles dans lesquelles la stratégie de stockage n'est pas spécifiée au niveau de la machine virtuelle ou du modèle de vApp.

Conditions préalables

- La stratégie de stockage par défaut cible est ajoutée au centre de données virtuel d'organisation. Reportez-vous à Ajouter une stratégie de stockage de machine virtuelle à un centre de données virtuel d'organisation.
- La stratégie de stockage par défaut cible est activée sur le centre de données virtuel d'organisation. Reportez-vous à Activer ou désactiver une stratégie de stockage dans un centre de données virtuel d'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Cliquez sur l'onglet **Stockage**.

4 Cliquez sur le bouton radio situé en regard du nom de la stratégie de stockage par défaut cible, puis sur **Définir comme valeur par défaut**.

5 Pour confirmer, cliquez sur **OK**.

Modifier la limite d'une stratégie de stockage sur un centre de données virtuel d'organisation

Vous pouvez changer la limite de capacité de stockage allouée que vous avez configurée pour une stratégie de stockage lors de la création d'un centre de données virtuel d'organisation.

Vous pouvez définir la capacité de stockage allouée comme étant illimitée ou configurer une quantité maximale de capacité de stockage allouée pour une stratégie de stockage sur un centre de données virtuel d'organisation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Cliquez sur l'onglet **Stockage**.

4 Cliquez sur le bouton radio situé en regard du nom de stratégie de stockage cible, puis cliquez sur **Modifier la limite**.

5 Configurez le paramètre de limite pour cette stratégie de stockage.

- Pour définir une limite, sélectionnez le bouton radio supérieur, puis entrez la quantité maximale de ressources de stockage pour cette stratégie de stockage sur ce centre de données virtuel d'organisation.
- Pour ne définir aucune limite, sélectionnez le bouton radio **Illimité**.

6 Cliquez sur **Modifier**.

Modifier les métadonnées d'une stratégie de stockage de machine virtuelle dans un centre de données virtuel d'organisation

Vous pouvez ajouter, modifier et supprimer des métadonnées d'une stratégie de stockage dans un centre de données virtuel d'organisation.

En utilisant des métadonnées d'objets, vous pouvez associer des paires *nom=valeur* définies par l'utilisateur à une stratégie de stockage sur un centre de données virtuel d'organisation. Vous pouvez utiliser des métadonnées d'objets dans les expressions de filtre de requête API vCloud.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.
3. Cliquez sur l'onglet **Stockage**.
4. Cliquez sur le bouton radio situé en regard du nom de stratégie de stockage cible, puis cliquez sur **Métadonnées**.
5. Cliquez sur **Modifier**.
6. (Facultatif) Pour ajouter une paire clé-valeur, cliquez sur **Ajouter**, entrez un nom et une valeur, puis sélectionnez un type pour la nouvelle paire clé-valeur.
7. (Facultatif) Pour modifier une paire clé-valeur, entrez un nouveau nom et une valeur, puis sélectionnez un nouveau type pour la paire clé-valeur.
8. (Facultatif) Pour supprimer une paire clé-valeur, à droite de la ligne correspondante, cliquez sur l'icône **Supprimer**.
9. Cliquez sur **Enregistrer** , puis sur **OK**.

Activer ou désactiver une stratégie de stockage dans un centre de données virtuel d'organisation

Pour empêcher d'autres vApp et machines virtuelles d'utiliser une stratégie de stockage dans un centre de données virtuel d'organisation, vous pouvez désactiver cette stratégie de stockage dans le centre de données virtuel d'organisation. Les vApp en cours d'exécution et les machines virtuelles sous tension continuent à s'exécuter, mais vous ne pouvez ni créer ni démarrer d'autres vApp ou machines virtuelles sur cette stratégie de stockage.

Vous ne pouvez pas désactiver la stratégie de stockage par défaut.

Conditions préalables

Si vous souhaitez désactiver la stratégie de stockage par défaut, Modifier la stratégie de stockage par défaut sur un centre de données virtuel d'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.
3. Cliquez sur l'onglet **Stockage**.
4. Cliquez sur le bouton radio situé en regard du nom de la stratégie de stockage cible, puis sur **Activer** ou **Désactiver**.
5. Pour confirmer, cliquez sur **OK**.

Supprimer une stratégie de stockage d'un centre de données virtuel d'organisation

Pour empêcher un centre de données virtuel d'organisation d'utiliser une stratégie de stockage, vous pouvez supprimer cette stratégie de stockage du centre de données virtuel d'organisation. Les vApp en cours d'exécution et les machines virtuelles sous tension continuent à s'exécuter, mais vous ne pouvez ni créer ni démarrer d'autres vApp ou machines virtuelles sur cette stratégie de stockage.

Conditions préalables

Désactivez la stratégie de stockage que vous souhaitez supprimer. Reportez-vous à Activer ou désactiver une stratégie de stockage dans un centre de données virtuel d'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.
3. Cliquez sur l'onglet **Stockage**.
4. Cliquez sur le bouton radio situé en regard du nom de stratégie de stockage cible, puis cliquez sur **Supprimer**.
5. Pour confirmer, cliquez sur **Supprimer**.

Modifier les paramètres réseau d'un centre de données virtuel d'organisation

Vous pouvez modifier le pool de réseaux à partir duquel les nouveaux réseaux sont provisionnés dans un centre de données virtuel d'organisation. Vous pouvez également activer les centres de données virtuels d'organisation pour qu'ils remplissent les conditions requises pour la mise en réseau intercentre de données virtuel.

Un pool de réseaux est un groupe de réseaux non différenciés, qui sert à créer des réseaux vApp, des réseaux VDC d'organisation acheminés et des réseaux VDC d'organisation internes. Vous pouvez modifier le pool de réseaux pour les nouveaux réseaux. Les réseaux existants continuent d'utiliser les anciens pools de réseaux.

Avec les centres de données virtuels d'organisation activés pour la mise en réseau intercentre de données virtuel, les utilisateurs de l'organisation disposant des droits appropriés peuvent créer des groupes de centres de données et des réseaux de couche 2 étirés dans ces groupes.

Conditions préalables

Si vous souhaitez activer la mise en réseau inter-VDC pour un centre de données virtuel d'organisation, vérifiez que vous avez configuré Cross-vCenter NSX sur le centre de données virtuel fournisseur dont il dépend.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Sous l'onglet **Pool de réseaux**, dans le coin supérieur droit, cliquez sur **Modifier**.

   Vous pouvez voir le nombre de réseaux utilisés par le centre de données virtuel d'organisation.

4 (Facultatif) Configurez les paramètres du pool de réseaux pour ce centre de données virtuel d'organisation.

   - Si vous ne souhaitez pas configurer de pool de réseaux pour ce centre de données virtuel d'organisation, désactivez le bouton bascule **Utiliser un pool de réseaux**.
   - Si vous souhaitez configurer un pool de réseaux pour ce centre de données virtuel d'organisation, procédez comme suit :

     a Activez le bouton bascule **Utiliser le pool de réseaux**.

       Vous pouvez voir une liste des pools de réseaux disponibles accompagnés d'informations sur leur utilisation, les réseaux disponibles et leur capacité.

     b Sélectionnez le bouton radio en regard du nom du pool de ressources cible.

     c Configurez le quota pour ce pool de réseaux dans ce centre de données virtuel d'organisation.

       Le quota est le nombre maximal de réseaux provisionnés. Il ne doit pas dépasser le nombre de réseaux disponibles pour le pool de réseaux sélectionné.

5 Pour activer la mise en réseau intercentre de données virtuel pour ce centre de données virtuel d'organisation, activez le bouton bascule **Mise en réseau inter-VDC**.

6 Cliquez sur **Enregistrer**.

Résultats

Dans le portail de locataires de vCloud Director, les centres de données virtuels activés pour la mise en réseau intercentre de données virtuel s'affichent dans la liste des centres de données pour la création d'un groupe de centres de données. Pour plus d'informations sur la création de groupes de centres de données, consultez le *Guide du portail de locataires de vCloud Director*.

Configuration de la mise en réseau intercentre de données virtuel

La fonctionnalité de mise en réseau intercentre de données virtuel permet aux organisations qui ont des centres de données virtuels reposant sur plusieurs instances de vCenter Server d'étirer les réseaux de couche 2 sur quatre centres de données virtuels au maximum. La mise en réseau

intercentre de données virtuel dépend d'une instance de Cross-vCenter NSX et peut s'étendre sur plusieurs sites vCloud Director.

La mise en réseau entre centres de données virtuels nécessite NSX Data Center for vSphere.

Avec la mise en réseau entre centres de données virtuels, les organisations peuvent regrouper jusqu'à quatre centres de données virtuels et configurer des sorties et des réseaux étirés de couche 2 dans chaque groupe.

Les centres de données virtuels d'organisation figurant dans le groupe peuvent appartenir à différents sites vCloud Director. Reportez-vous à la section Configuration et gestion de déploiements multisite.

Les organisations peuvent utiliser la mise en réseau intercentre de données virtuel pour mettre en œuvre des solutions de haute disponibilité ou des architectures de systèmes distribués, dans lesquelles une application peut être distribuée sur plusieurs centres de données virtuels ou sites.

L'**administrateur système** doit configurer l'environnement Cross-vCenter NSX sous-jacent, les serveurs vCloud Director et activer la mise en réseau intercentre de données virtuel pour chaque centre de données virtuel.

1 Configurez une des instances de NSX Manager comme instance principale de NSX Manager. Consultez le *Guide d'installation de Cross-vCenter NSX*.
   a Déployez le cluster NSX sur l'instance principale de NSX Manager.
   b Préparez les hôtes ESXi sur l'instance principale de NSX Manager.
   c Configurez VXLAN à partir de l'instance principale de NSX Manager.
   d Attribuez le rôle principal à l'instance de NSX Manager.
   e Créez un pool pour les adresses IP de segment de la zone de transport universelle.
   f Ajoutez une zone de transport universelle.
2 Configurez le reste des instances de NSX Manager en tant qu'instances secondaires de NSX Manager. Consultez le *Guide d'installation de Cross-vCenter NSX*.
   a Préparez les hôtes ESXi sur chaque instance secondaire de NSX Manager.
   b Configurez VXLAN à partir de chaque instance secondaire de NSX Manager.
   c Attribuez le rôle secondaire à chaque instance de NSX Manager.
   d Connectez les clusters ESXi à la zone de transport universelle.
3 Configurez les propriétés de machine virtuelle de contrôle pour chaque instance de NSX Manager. Reportez-vous au Modifier les paramètres de NSX Manager.

4 Créez un pool de réseaux reposant sur VXLAN à l'aide d'une zone de transport de type universel à partir de n'importe quelle instance de vCenter Server. Reportez-vous à Créez un pool de réseaux reposant sur une zone de transport NSX Data Center for vSphere..

Note Pour les déploiements multisites, vous devez créer un pool de réseaux reposant sur VXLAN dans chaque site vCloud Director.

5 Activez la mise en réseau intercentre de données virtuel sur chaque de centre de données virtuel d'organisation. Reportez-vous au Modifier les paramètres réseau d'un centre de données virtuel d'organisation.

6 Si l'organisation comprend des centres de données virtuels multisites, vérifiez que les ID d'installation des sites vCloud Director sont différents. Si des sites vCloud Director sont configurés avec le même ID d'installation, reportez-vous à la section Régénération d'adresses MAC pour les réseaux étirés multisite dans le *Guide d'installation, de configuration et de mise à niveau de vCloud Director*.

L'**administrateur d'organisation** peut désormais créer et configurer des groupes de centres de données, des sorties et des réseaux étirés. Pour plus d'informations sur la gestion de la mise en réseau intercentre de données virtuel, consultez le *Guide du portail de locataires de vCloud Director*.

Modifier les métadonnées d'un centre de données virtuel d'organisation

Vous pouvez ajouter, modifier et supprimer des métadonnées pour un centre de données virtuel d'organisation.

En utilisant des métadonnées d'objets, vous pouvez associer des paires *nom=valeur* à un centre de données virtuel d'organisation. Vous pouvez utiliser des métadonnées d'objets dans les expressions de filtre de requête API vCloud.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Cliquez sur l'onglet **Métadonnées**.

4 Cliquez sur **Modifier**.

5 (Facultatif) Pour ajouter une paire clé-valeur, cliquez sur **Ajouter**, entrez un nom et une valeur, puis sélectionnez un type pour la nouvelle paire clé-valeur.

6 (Facultatif) Pour modifier une paire clé-valeur, entrez un nouveau nom et une valeur, puis sélectionnez un nouveau type pour la paire clé-valeur.

7 (Facultatif) Pour supprimer une paire clé-valeur, à droite de la ligne correspondante, cliquez sur l'icône **Supprimer**.

8 Cliquez sur **Enregistrer** , puis sur **OK**.

Afficher les pools de ressources d'un centre de données virtuel d'organisation

Vous pouvez afficher la liste des pools de ressources vCenter Server utilisés par un centre de données virtuel d'organisation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**, puis cliquez sur le nom du centre de données virtuel d'organisation cible.

3 Cliquez sur l'onglet **Pools de ressources**.

Résultats

Un tableau s'affiche contenant les pools de ressources utilisés par le centre de données virtuel d'organisation et l'instance de vCenter Server à laquelle appartient chaque pool de ressources.

Gestion du pare-feu distribué dans un centre de données virtuel d'organisation

Pour fournir une sécurité réseau de couche 3 et de couche 2 dans un centre de données virtuel d'organisation, vous pouvez activer et créer des règles pour le pare-feu distribué dans ce centre de données virtuel d'organisation. Avec les règles de pare-feu distribué, vous pouvez protéger le trafic circulant entre les machines virtuelles dans un centre de données virtuel d'organisation.

vCloud Director prend en charge les services de pare-feu distribué sur les centres de données virtuels d'organisation reposant sur NSX Data Center for vSphere.

Pour créer les règles de pare-feu distribué, vous pouvez utiliser divers objets de regroupement et groupes de sécurité. Reportez-vous à Personnaliser le regroupement d'objets et Utilisation des groupes de sécurité.

Pour plus d'informations sur la protection du trafic entrant et sortant sur une passerelle Edge, reportez-vous à Gestion d'un pare-feu de passerelle Edge NSX Data Center for vSphere.

Activer le pare-feu distribué dans un centre de données virtuel d'organisation

Pour pouvoir gérer les paramètres de pare-feu distribué dans un centre de données virtuel d'organisation, vous devez activer le pare-feu distribué dans ce centre de données virtuel d'organisation.

vCloud Director prend en charge les services de pare-feu distribué sur les centres de données virtuels d'organisation reposant sur NSX Data Center for vSphere.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.
4. Dans l'onglet **Pare-feu distribué > Général**, activez le bouton radio **Activer le pare-feu distribué**.

Résultats

Vous pouvez voir les règles de pare-feu distribué par défaut, qui autorisent tout le trafic de couche 3 et de couche 2 à passer par le centre de données virtuel d'organisation.

- Dans l'onglet **Pare-feu distribué > Général**, vous pouvez voir la règle de pare-feu distribué par défaut pour le trafic de couche 3, nommée Règle autoriser par défaut.
- Dans l'onglet **Pare-feu distribué > Ethernet**, vous pouvez voir la règle de pare-feu distribué par défaut du trafic de couche 2, nommée Règle autoriser par défaut.

Ajouter une règle de pare-feu distribué

Commencez par ajouter des règles de Distributed Firewall à l'échelle du centre de données virtuel de l'organisation. Vous pouvez ensuite réduire l'étendue à laquelle vous souhaitez appliquer la règle. Le pare-feu distribué vous permet d'ajouter plusieurs objets aux niveaux source et destination pour chaque règle ce qui contribue à réduire le nombre de règles de pare-feu à ajouter.

Pour plus d'informations sur les services et les groupes de services prédéfinis que vous pouvez utiliser dans une règle, consultez Afficher les services disponibles pour les règles de pare-feu et Afficher les groupes de services disponibles pour les règles de pare-feu.

Conditions préalables

- Activer le pare-feu distribué dans un centre de données virtuel d'organisation
- Si vous souhaitez utiliser un ensemble d'adresses IP comme source ou destination dans une règle, Créer un ensemble d'adresses IP à utiliser dans les règles de pare-feu et la configuration du relais DHCP.
- Si vous souhaitez utiliser un ensemble d'adresses MAC comme source ou destination dans une règle, Créer un ensemble d'adresses MAC à utiliser dans les règles de pare-feu.
- Si vous souhaitez utiliser un groupe de sécurité comme source ou destination dans une règle, Créer un groupe de sécurité.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Sélectionnez le type de règle que vous souhaitez créer. Vous pouvez créer une règle générale ou une règle Ethernet.

   Les règles de la couche 3 (L3) sont configurées dans l'onglet **Général**. Les règles de la couche 2 (L2) sont configurées dans l'onglet **Ethernet**.

5 Pour ajouter une règle sous une règle existante dans le tableau du pare-feu, cliquez sur la ligne existante, puis cliquez sur le bouton **Créer** ( ).

   Une ligne destinée à la nouvelle règle est ajoutée sous la règle sélectionnée ; par défaut, elle se voit attribuer n'importe quelle destination, n'importe quel service et l'action **Autoriser**. Si la règle Autoriser définie par défaut par le système est l'unique règle du tableau du pare-feu, la nouvelle règle est ajoutée au-dessus de la règle par défaut.

6 Cliquez dans la cellule **Nom** et entrez un nom.

7 Cliquez dans la cellule **Source** et utilisez les icônes désormais visibles pour sélectionner la source à ajouter à la règle :

Action	Description
Cliquez sur l'icône IP	Applicable aux règles définies dans l'onglet **Général**. Saisissez la valeur source que vous souhaitez utiliser. Les valeurs valides sont une adresse IP, CIDR, une plage d'adresses IP ou le mot clé **tous**. Le pare-feu distribué prend uniquement en charge le format IPv4.
Cliquez sur l'icône +	Utilisez l'icône **+** pour spécifier la source sous la forme d'un objet autre qu'une adresse IP spécifique : ■ Utilisez la fenêtre **Sélectionner des objets** pour ajouter des objets qui correspondent à vos sélections et cliquez sur **Conserver** pour les ajouter à la règle. ■ Pour exclure une source de la règle, ajoutez-la à cette règle à l'aide de la fenêtre **Sélectionner des objets**, puis sélectionnez l'icône d'exclusion pour exclure cette source de cette règle. Lorsque l'exclusion est sélectionnée sur la source, la règle est appliquée au trafic provenant de toutes les sources à l'exception de celle que vous avez exclue. Lorsque l'exclusion n'est pas sélectionnée, la règle s'applique au trafic provenant de la source que vous avez spécifiée dans la fenêtre **Sélectionner des objets**

8 Cliquez sur la cellule **Destination** et effectuez l'une des actions suivantes :

Action	Description
Cliquez sur l'icône IP	Applicable aux règles définies dans l'onglet **Général**. Saisissez la valeur de destination que vous souhaitez utiliser. Les valeurs valides sont une adresse IP, un routage CIDR, une plage d'adresses IP ou le mot clé **tous**. Le pare-feu distribué prend uniquement en charge le format IPv4.
Cliquez sur l'icône +	Utilisez l'icône **+** pour spécifier la source sous la forme d'un objet autre qu'une adresse IP spécifique : ■ Utilisez la fenêtre **Sélectionner des objets** pour ajouter des objets qui correspondent à vos sélections et cliquez sur **Conserver** pour les ajouter à la règle. ■ Pour exclure une source de la règle, ajoutez-la à cette règle à l'aide de la fenêtre Sélectionner des objets, puis sélectionnez l'icône d'exclusion pour exclure cette source de cette règle. Lorsque l'exclusion est sélectionnée sur la source, la règle est appliquée au trafic provenant de toutes les sources à l'exception de celle que vous avez exclue. Lorsque l'exclusion n'est pas sélectionnée, la règle s'applique au trafic provenant de la source que vous avez spécifiée dans la fenêtre **Sélectionner des objets**

9 Cliquez sur la cellule **Service** de la nouvelle règle et effectuez l'une des actions suivantes :

Action	Description
Cliquez sur l'icône IP	Pour spécifier le service en tant que combinaison port-protocole : a Sélectionnez le protocole de service. b Tapez les numéros de port pour les ports source et destination, ou spécifiez **tous**, puis cliquez sur **Conserver**.
Cliquez sur l'icône +	Pour sélectionner un service prédéfini ou un groupe de services, ou en définir un nouveau : a Sélectionnez un ou plusieurs objets et ajoutez-les au filtre. b Cliquez sur **Conserver**.

10 Dans la cellule **Action** de la nouvelle règle, configurez l'action de la règle.

Option	Description
Autoriser	Autorise le trafic depuis ou vers les sources, les destinations et les services spécifiés.
Refuser	Bloque le trafic depuis ou vers les sources, les destinations et les services spécifiés.

11 Dans la cellule **Direction** de la nouvelle règle, indiquez si la règle s'applique au trafic entrant, sortant ou aux deux.

12 S'il s'agit d'une règle de l'onglet **Général**, dans la cellule **Type de paquet** de la nouvelle règle, sélectionnez le type de paquet **Tous**, **IPV4** ou **IPV6**.

13 Sélectionnez la cellule **Appliqué à** et utilisez l'icône **+** pour définir la portée de l'objet auquel s'applique cette règle.

Note Si la règle contient des machines virtuelles dans les cellules **Source** et **Destination**, vous devez ajouter les machines virtuelles source et de destination à l'option **Appliqué à** de la règle pour que celle-ci fonctionne correctement.

14 Cliquez sur **Enregistrer les modifications**.

Modifier une règle de pare-feu distribué

Dans un environnement vCloud Director, pour modifier une règle de pare-feu distribué existante d'un centre de données virtuel d'organisation, utilisez l'écran **Pare-feu distribué**.

Pour plus d'informations sur les paramètres disponibles pour les différentes cellules d'une règle, reportez-vous à la section Ajouter une règle de pare-feu distribué.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Les actions suivantes vous permettent de gérer les règles de pare-feu distribué :

- Pour désactiver une règle, cliquez sur la coche verte dans la cellule **N°**.

  La coche verte prend l'aspect d'une icône rouge de désactivation. Si la règle est désactivée et que vous souhaitez l'activer, cliquez sur l'icône rouge de désactivation.

- Pour modifier le nom d'une règle, double-cliquez dans la cellule **Nom** et saisissez le nouveau nom.

- Pour modifier les paramètres d'une règle (par exemple, les paramètres de source ou d'action), sélectionnez la cellule appropriée et utilisez les contrôles affichés.

- Pour supprimer une règle, sélectionnez-la, puis cliquez sur le bouton **Supprimer** ( ) situé au-dessus du tableau de règles.

- Pour déplacer une règle vers le haut ou vers le bas dans le tableau des règles, sélectionnez la règle et cliquez sur la flèche vers le haut ou sur la flèche vers le bas au-dessus du tableau des règles.

5 Cliquez sur **Enregistrer les modifications**.

Personnaliser le regroupement d'objets

Le logiciel NSX de votre environnement vCloud Director vous offre la possibilité de définir des ensembles et des groupes de certaines entités, que vous pouvez ensuite utiliser pour spécifier d'autres configurations relatives au réseau, comme pour les règles de pare-feu.

Créer un ensemble d'adresses IP à utiliser dans les règles de pare-feu et la configuration du relais DHCP

Un ensemble d'adresses IP est un groupe d'adresses IP que vous pouvez créer au niveau d'un centre de données virtuel d'organisation. Vous pouvez utiliser un ensemble d'adresses IP comme source ou destination dans une règle de pare-feu ou dans une configuration de relais DHCP.

Créez un ensemble d'adresses IP à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres des services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Ensembles d'adresses IP**.

Les ensembles d'adresses IP qui sont déjà définis sont affichés dans cet écran.

3 Pour ajouter un ensemble d'adresses IP, cliquez sur le bouton **Créer** (+).

4 Entrez un nom et, éventuellement, une description de l'ensemble d'adresses IP, ainsi que les adresses IP à inclure dans l'ensemble.

5 Pour enregistrer cet ensemble d'adresses IP, cliquez sur **Conserver**.

Résultats

Le nouvel ensemble d'adresses IP peut être sélectionné en tant que source ou destination dans les règles de pare-feu ou dans les configurations du relais DHCP.

Créer un ensemble d'adresses MAC à utiliser dans les règles de pare-feu

Un ensemble d'adresses MAC est un groupe d'adresses MAC que vous pouvez créer au niveau d'un centre de données virtuel d'organisation. Vous pouvez utiliser un ensemble d'adresses MAC comme source ou destination dans une règle de pare-feu.

Vous créez un ensemble d'adresses MAC à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Ensembles d'adresses MAC**.

Les ensembles d'adresses MAC qui sont déjà définis sont affichés dans cet écran.

3 Pour ajouter un ensemble d'adresses MAC, cliquez sur le bouton **Créer** (+).

4 Entrez un nom pour l'ensemble, une description facultative et les adresses MAC à inclure dans l'ensemble.

5 Pour enregistrer l'ensemble d'adresses MAC, cliquez sur **Conserver**.

Résultats

Le nouvel ensemble d'adresses MAC peut être sélectionné en tant que source ou destination dans les règles de pare-feu.

Afficher les services disponibles pour les règles de pare-feu

Vous pouvez afficher la liste des groupes de services utilisables dans les règles de pare-feu. Dans ce contexte, un service est une combinaison port-protocole.

Vous pouvez afficher les services disponibles à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Services**.

Résultats

Les services disponibles sont affichés sur l'écran.

Afficher les groupes de services disponibles pour les règles de pare-feu

Vous pouvez afficher la liste des groupes de services pouvant être utilisés dans les règles de pare-feu. Dans ce contexte, un service est une combinaison port-protocole et un groupe de services est un groupe de services ou d'autres groupes de services.

Vous pouvez afficher les groupes de services disponibles à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez dans l'onglet **Groupes de services**.

Résultats

Les groupes de services disponibles s'affichent sur l'écran. La colonne Description affiche les services qui sont regroupés dans chaque groupe de services.

Utilisation des groupes de sécurité

Un groupe de sécurité est un ensemble de ressources ou un regroupement d'objets, tels que des machines virtuelles, des réseaux de centres de données virtuels d'organisation ou des balises de sécurité.

Les groupes de sécurité peuvent avoir des critères d'appartenance dynamique basés sur les balises de sécurité, le nom de la machine virtuelle, le nom du système d'exploitation invité de machine virtuelle ou le nom d'hôte invité de machine virtuelle. Par exemple, toutes les machines virtuelles qui possèdent la balise de sécurité « web » sont automatiquement ajoutées à un groupe de sécurité spécifique destiné à des serveurs Web. Après la création d'un groupe de sécurité, une stratégie de sécurité est appliquée à ce groupe.

Créer un groupe de sécurité

Vous pouvez créer des groupes de sécurité définis par l'utilisateur.

Conditions préalables

Si vous souhaitez utiliser des balises de sécurité avec des groupes de sécurité, Créer et attribuer des balises de sécurité.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Cliquez sur l'onglet **Regroupement d'objets > Groupes de sécurité**.

5 Cliquez sur le bouton **Créer** ( ).

6 Entrez le nom et la description (facultative) du groupe de sécurité.

La description s'affiche dans la liste des groupes de sécurité, de sorte que l'ajout d'une description significative peut faciliter l'identification du groupe de sécurité en un coup d'œil.

7 (Facultatif) Ajouter un ensemble de membres dynamique.

a Sous Ensembles de membres dynamiques, cliquez sur le bouton **Ajouter** ( ).

b Indiquez si vous voulez obtenir une correspondance de **N'importe lequel** ou **Tous** les critères de votre instruction.

c Entrer le premier objet à faire correspondre.

Les options sont **Balise de sécurité**, **Nom du système d'exploitation invité de machine virtuelle**, **Nom de la machine virtuelle** et **Nom d'hôte invité de machine virtuelle**.

d Sélectionnez un opérateur, tel que **Contient**, **Commence par** ou **Se termine par**.

e Entrez une valeur.

f (Facultatif) Pour ajouter une autre instruction, utilisez un opérateur booléen **Et** ou **Ou**.

8 (Facultatif) Inclure les membres.

a Dans le menu déroulant **Parcourir les objets de type**, sélectionnez le type des objets, par exemple **Machines virtuelles**, **Réseaux VDC d'organisation**, **Ensembles d'adresses IP**, **Ensembles d'adresses MAC** ou **Balises de sécurité**.

b Pour inclure un objet dans la liste Inclure les membres, sélectionnez l'objet dans le panneau de gauche et déplacez-le vers le panneau de droite en cliquant sur la flèche droite.

9 (Facultatif) Exclure les membres.

a Dans le menu déroulant **Parcourir les objets de type**, sélectionnez le type des objets, par exemple **Machines virtuelles**, **Réseaux VDC d'organisation**, **Ensembles d'adresses IP**, **Ensembles d'adresses MAC** ou **Balises de sécurité**.

b Pour inclure un objet dans la liste Exclure les membres, sélectionnez l'objet dans le panneau de gauche et déplacez-le vers le panneau de droite en cliquant sur la flèche droite.

10 Cliquez sur **Conserver** pour conserver vos modifications.

L'exécution de l'opération peut prendre quelques instants.

Résultats

Le groupe de sécurité peut désormais être utilisé dans des règles, telles que celles de pare-feu.

Modifier un groupe de sécurité

Vous pouvez modifier les groupes de sécurité définis par l'utilisateur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.
4. Cliquez sur l'onglet **Regroupement d'objets > Groupes de sécurité**.
5. Sélectionnez le groupe de sécurité que vous souhaitez modifier.

   Les détails relatifs au groupe de sécurité s'affichent sous la liste des groupes de sécurité.
6. (Facultatif) Modifiez le nom et la description du groupe de sécurité.
7. (Facultatif) Ajouter un ensemble de membres dynamique.
   a. Sous **Ensembles de membres dynamiques**, cliquez sur le bouton **Ajouter** (+).
   b. Indiquez si vous voulez obtenir une correspondance de **N'importe lequel** ou **Tous** les critères de votre instruction.
   c. Entrer le premier objet à faire correspondre.

      Les options sont **Balise de sécurité**, **Nom du système d'exploitation invité de machine virtuelle**, **Nom de la machine virtuelle** et **Nom d'hôte invité de machine virtuelle**.
   d. Sélectionnez un opérateur, tel que **Contient**, **Commence par** ou **Se termine par**.
   e. Entrez une valeur.
   f. (Facultatif) Pour ajouter une autre instruction, utilisez un opérateur booléen **Et** ou **Ou**.
8. (Facultatif) Modifiez un ensemble de membres dynamiques en cliquant sur l'icône **Modifier** (⚙) en regard de l'ensemble de membres que vous souhaitez modifier.
   a. Apportez les modifications nécessaires à l'ensemble de membres dynamiques.
   b. Cliquez sur **OK**.
9. (Facultatif) Supprimez un ensemble de membres dynamiques en cliquant sur l'icône **Supprimer** (✖) en regard de l'ensemble de membres que vous souhaitez supprimer.

10 (Facultatif) Modifiez la liste des membres inclus en cliquant sur l'icône **Modifier** (⚙) en regard de la liste Inclure les membres.

   a Dans le menu déroulant **Parcourir les objets de type**, sélectionnez le type des objets, par exemple **Machines virtuelles**, **Réseaux VDC d'organisation**, **Ensembles d'adresses IP**, **Ensembles d'adresses MAC** ou **Balises de sécurité**.

   b Pour inclure un objet dans la liste Inclure les membres, sélectionnez l'objet dans le panneau de gauche et déplacez-le vers le panneau de droite en cliquant sur la flèche droite.

   c Pour exclure un objet de la liste Inclure les membres, sélectionnez l'objet dans le panneau de droite et déplacez-le vers le panneau de gauche en cliquant sur la flèche gauche.

11 (Facultatif) Modifiez la liste des membres exclus en cliquant sur l'icône **Modifier** (⚙) en regard de la liste Exclure les membres.

   a Dans le menu déroulant **Parcourir les objets de type**, sélectionnez le type des objets, par exemple **Machines virtuelles**, **Réseaux VDC d'organisation**, **Ensembles d'adresses IP**, **Ensembles d'adresses MAC** ou **Balises de sécurité**.

   b Pour inclure un objet dans la liste Exclure les membres, sélectionnez l'objet dans le panneau de gauche et déplacez-le vers le panneau de droite en cliquant sur la flèche droite.

   c Pour exclure un objet de la liste Exclure les membres, sélectionnez l'objet dans le panneau de droite et déplacez-le vers le panneau de gauche en cliquant sur la flèche gauche.

12 Cliquez sur **Enregistrer les modifications**.

   Les modifications apportées au groupe de sécurité sont enregistrées.

Supprimer un groupe de sécurité

Vous pouvez supprimer un groupe de sécurité défini par l'utilisateur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Cliquez sur l'onglet **Regroupement d'objets > Groupes de sécurité**.

5 Sélectionnez le groupe de sécurité que vous souhaitez supprimer.

6 Cliquez sur le bouton **Supprimer** (✖).

7 Pour confirmer la suppression, cliquez sur **OK**.

Résultats

Le groupe de sécurité est supprimé.

Utilisation des balises de sécurité

Les balises de sécurité sont des étiquettes qui peuvent être associées à une machine virtuelle ou un groupe de machines virtuelles. Les balises de sécurité sont conçues pour être utilisées avec des groupes de sécurité. Une fois que vous avez créé les balises de sécurité, vous les associez à un groupe de sécurité qui peut être utilisé dans des règles de pare-feu. Vous pouvez créer, modifier ou attribuer une balise de sécurité définie par l'utilisateur. Vous pouvez également afficher les machines virtuelles ou les groupes de sécurité pour lesquels une balise de sécurité particulière est appliquée.

Un cas d'utilisation courant des balises de sécurité consiste à regrouper les objets dynamiquement afin de simplifier les règles de pare-feu. Par exemple, vous pouvez créer plusieurs balises de sécurité différentes en fonction du type d'activité que vous prévoyez sur une machine virtuelle donnée. Vous créez une balise de sécurité pour les serveurs de base de données et une autre pour les serveurs de messagerie. Ensuite, vous appliquez la balise appropriée aux machines virtuelles qui hébergent des serveurs de base de données ou des serveurs de messagerie. Par la suite, vous pouvez attribuer la balise à un groupe de sécurité et écrire une règle de pare-feu par rapport à ce groupe, appliquant différents paramètres de sécurité selon que la machine virtuelle exécute un serveur de base de données ou un serveur de messagerie. Plus tard, si vous modifiez les fonctionnalités de la machine virtuelle, vous pouvez supprimer cette dernière de la balise de sécurité au lieu de modifier la règle de pare-feu.

Créer et attribuer des balises de sécurité

Vous pouvez créer une balise de sécurité et l'attribuer à une machine virtuelle ou à un groupe de machines virtuelles.

Créez une balise de sécurité et attribuez-la à une machine virtuelle ou à un groupe de machines virtuelles.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.
4. Cliquez sur l'onglet **Balises de sécurité**.
5. Cliquez sur le bouton **Créer** ( ) et entrez un nom pour la balise de sécurité.
6. (Facultatif) Entrez une description pour la balise de sécurité.

7 (Facultatif) Attribuez la balise de sécurité à une machine virtuelle ou à un groupe de machines virtuelles.

   Dans le menu déroulant **Parcourir les objets de type**, l'option **Machines virtuelles** est sélectionnée par défaut.

   a Sélectionnez une machine virtuelle dans le panneau de gauche.

   b Attribuez la balise de sécurité à la machine virtuelle sélectionnée en cliquant sur la flèche droite.

      La machine virtuelle se déplace vers le panneau de droite et la balise de sécurité lui est attribuée.

8 Une fois que vous avez terminé l'attribution de la balise aux machines virtuelles sélectionnées, cliquez sur **Conserver**.

Résultats

La balise de sécurité est créée et est attribuée, le cas échéant, aux machines virtuelles sélectionnées.

Étape suivante

Les balises de sécurité sont conçues pour fonctionner avec un groupe de sécurité. Pour plus d'informations sur la création de groupes de sécurité, reportez-vous à la section Créer un groupe de sécurité.

Modifier l'attribution de balises de sécurité

Après avoir créé une balise de sécurité, vous pouvez l'attribuer manuellement à des machines virtuelles. Vous pouvez également modifier une balise de sécurité pour supprimer la balise des machines virtuelles auxquelles vous l'avez déjà attribuée.

Si vous avez créé des balises de sécurité, vous pouvez les attribuer à des machines virtuelles. Vous pouvez utiliser des balises de sécurité afin de regrouper des machines virtuelles pour l'écriture des règles de pare-feu. Par exemple, vous pouvez attribuer une balise de sécurité à un groupe de machines virtuelles contenant des données sensibles.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Cliquez sur l'onglet **Balises de sécurité**.

5 Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez modifier, puis cliquez sur le bouton **Modifier** ( ).

6 Sélectionnez les machines virtuelles dans le panneau de gauche et attribuez-leur la balise de sécurité en cliquant sur la flèche droite.

   La balise de sécurité est attribuée aux machines virtuelles du panneau de droite.

7 Sélectionnez les machines virtuelles dans le panneau de droite et supprimez leur balise en cliquant sur la flèche gauche.

   La balise de sécurité n'est pas attribuée aux machines virtuelles du panneau de gauche.

8 Lorsque vous avez terminé l'ajout de vos modifications, cliquez sur **Conserver**.

Résultats

La balise de sécurité est attribuée aux machines virtuelles sélectionnées.

Étape suivante

Les balises de sécurité sont conçues pour fonctionner avec un groupe de sécurité. Pour plus d'informations sur la création de groupes de sécurité, reportez-vous à la section Créer un groupe de sécurité.

Afficher les balises de sécurité appliquées

Vous pouvez afficher les balises de sécurité appliquées à des machines virtuelles dans votre environnement. Vous pouvez également afficher les balises de sécurité appliquées aux groupes de sécurité dans votre environnement.

Conditions préalables

Une balise de sécurité doit avoir été créée et appliquée à une machine virtuelle ou à un groupe de sécurité.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Affichez les étiquettes attribuées à partir de l'onglet **Balises de sécurité**.

   a Dans l'onglet **Balises de sécurité**, sélectionnez la balise de sécurité pour laquelle vous souhaitez voir des attributions, puis cliquez sur l'icône **Modifier**.

   b Dans la section **Attribuer/annuler l'attribution des VM**, vous pouvez voir la liste de machines virtuelles attribuées à la balise de sécurité.

   c Cliquez sur **Ignorer**.

5 Affichez les étiquettes attribuées à partir de l'onglet **Groupes de sécurité**.

   a Cliquez dans l'onglet **Regroupement d'objets**, puis cliquez sur **Groupes de sécurité**.

   b Sélectionnez un groupe de sécurité.

   c Dans la liste sous **Inclure les membres**, vous pouvez voir la balise de sécurité attribuée à un groupe de sécurité.

Résultats

Vous pouvez afficher les balises de sécurité existantes et les machines virtuelles et groupes de sécurité associés. De cette manière, vous pouvez déterminer une stratégie pour la création de règles de pare-feu basées sur des balises de sécurité et des groupes de sécurité.

Modifier une balise de sécurité

Vous pouvez modifier une balise de sécurité définie par l'utilisateur.

Si vous modifiez l'environnement ou la fonction d'une machine virtuelle, vous voudrez peut-être également utiliser une balise de sécurité différente pour que les règles de pare-feu soient correctes pour la nouvelle configuration de la machine. Par exemple, si vous disposez d'une machine virtuelle sur laquelle vous ne stockez plus de données sensibles, vous voudrez peut-être attribuer une balise de sécurité différente afin que les règles de pare-feu qui s'appliquent aux données sensibles ne s'appliquent plus à la machine virtuelle.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **VDC d'organisation**.

3 Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.

4 Cliquez sur l'onglet **Balises de sécurité**.

5 Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez modifier.

6 Cliquez sur le bouton **Modifier** ( ).

7 Modifiez le nom et la description de la balise de sécurité.

8 Attribuez la balise aux machines virtuelles que vous sélectionnez ou supprimez l'attribution.

9 Pour enregistrer les modifications, cliquez sur **Conserver**.

Étape suivante

Si vous modifiez une balise de sécurité, vous devez également modifier le groupe de sécurité ou les règles de pare-feu associés. Pour plus d'informations sur les groupes de sécurité, reportez-vous à la section Utilisation des groupes de sécurité.

.

Supprimer une balise de sécurité

Vous pouvez supprimer une balise de sécurité définie par l'utilisateur.

Vous pouvez vouloir supprimer une balise de sécurité si la fonction ou l'environnement de la machine virtuelle sont modifiés. Par exemple, si vous disposez d'une balise de sécurité pour les bases de données Oracle, mais que vous décidez d'utiliser un serveur de base de données différent, vous pouvez supprimer la balise de sécurité afin que les règles de pare-feu qui s'appliquent aux bases de données Oracle ne soient plus exécutées pour la machine virtuelle.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **VDC d'organisation**.
3. Cliquez sur le bouton radio situé en regard du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**.
4. Cliquez sur l'onglet **Balises de sécurité**.
5. Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez supprimer.
6. Cliquez sur le bouton **Supprimer** ( ).
7. Pour confirmer la suppression, cliquez sur **OK**.

Résultats

La balise de sécurité est supprimée.

Étape suivante

Si vous supprimez une balise de sécurité, vous devez également modifier un groupe de sécurité ou des règles de pare-feu associés. Pour plus d'informations sur les groupes de sécurité, reportez-vous à la section Utilisation des groupes de sécurité.

Gestion de passerelles Edge NSX Data Center for vSphere 7

Une passerelle Edge NSX Data Center for vSphere fournit à un réseau de centre de données virtuel d'organisation routé la connectivité aux réseaux externes et peut fournir des services tels que l'équilibrage de charge, la traduction d'adresse réseau et un pare-feu. vCloud Director prend en charge les passerelles Edge IPv4 et IPv6.

À partir de vCloud Director 9.7, la charge de travail de calcul et la charge de travail de mise en réseau sont isolées en utilisant différents pools de ressources et stratégies de stockage de vSphere. Les passerelles Edge résident sur des clusters Edge que vous devez auparavant créer. Reportez-vous à Utilisation des clusters Edge.

Vous pouvez migrer des passerelles Edge héritées vers les clusters Edge correspondants en redéployant ces passerelles Edge. Reportez-vous à Redéployer une passerelle Edge.

Important À partir de la version 9.7, vCloud Director prend uniquement en charge les passerelles Edge avancées. Vous devez convertir une passerelle Edge non avancée héritée en une passerelle avancée. Reportez-vous à https://kb.vmware.com/kb/66767.

Ce chapitre contient les rubriques suivantes :

- Utilisation des clusters Edge
- Ajouter une passerelle Edge NSX Data Center for vSphere
- Configuration des services de passerelle Edge NSX Data Center for vSphere
- Afficher l'utilisation des réseaux et les allocations IP sur une passerelle Edge
- Modification des propriétés de la passerelle Edge
- Redéployer une passerelle Edge
- Supprimer une passerelle Edge
- Statistiques et journaux pour une passerelle Edge
- Activer l'accès de ligne de commande SSH à une passerelle Edge

Utilisation des clusters Edge

Pour isoler les charges de travail de calcul des charges de travail de mise en réseau, vCloud Director 9.7 introduit l'objet de cluster Edge. Un cluster Edge se compose d'un pool de ressources vSphere et d'une stratégie de stockage qui sont utilisées uniquement pour les passerelles Edge de VDC d'organisation. Les centres de données virtuels fournisseur ne peuvent pas utiliser les ressources dédiées aux clusters Edge, et les clusters Edge ne peuvent pas utiliser les ressources dédiées aux centres de données virtuels fournisseur.

Les clusters Edge fournissent un domaine de diffusion L2 dédié, ce qui réduit les prolifération VLAN et garantit la sécurité et l'isolation du réseau. Par exemple, le cluster Edge peut contenir des VLAN supplémentaires pour l'appairage avec des routeurs physiques.

Vous pouvez créer un nombre quelconque de clusters Edge. Vous pouvez attribuer un cluster Edge à un VDC d'organisation en tant que cluster Edge principal ou secondaire.

- Le cluster Edge principal d'un VDC d'organisation est utilisé pour le dispositif Edge principal d'une passerelle Edge de VDC d'organisation.
- Le cluster Edge secondaire d'un VDC d'organisation est utilisé pour le dispositif Edge en veille lorsqu'une passerelle Edge est en mode HA.

Différents VDC d'organisation peuvent partager des clusters Edge ou disposer de leurs propres clusters Edge dédiés.

La version vCloud Director 9.7 rend obsolète l'ancien processus d'utilisation des métadonnées pour contrôler le placement de la passerelle Edge. Reportez-vous à https://kb.vmware.com/kb/2151398.

Vous pouvez migrer des passerelles Edge héritées vers des clusters Edge récemment créés en redéployant ces passerelles Edge. Reportez-vous à Redéployer une passerelle Edge.

Préparation de votre environnement pour un cluster Edge

1 Dans vSphere, créez le pool de ressources pour le cluster Edge cible.

   Si un centre de données virtuel d'organisation utilise un pool de réseaux VLAN, le pool de réseaux VLAN et le cluster Edge de ce centre de données virtuel d'organisation doivent résider sur le même commutateur distribué vSphere.

2 Si un centre de données virtuel d'organisation utilise un pool de réseaux VXLAN, dans NSX, ajoutez le cluster Edge à la zone de transport VXLAN, puis synchronisez le pool de réseaux VXLAN dans vCloud Director.

3 Dans vSphere, créez le profil de stockage du cluster Edge.

Création et gestion de clusters Edge

Après avoir préparé votre environnement, pour créer et gérer des clusters Edge, vous devez utiliser les méthodes `EdgeClusters` vCloud OpenAPI. Reportez-vous à *Démarrage de vCloud OpenAPI* sur https://code.vmware.com.

L'affichage des clusters Edge nécessite le droit **Affichage de cluster Edge**. La création, la mise à jour et la suppression de clusters Edge nécessitent le droit **Gestion de cluster Edge**.

Lorsque vous créez un cluster Edge, vous spécifiez le nom, le pool de ressources vSphere et le nom du profil de stockage.

Après avoir créé un cluster Edge, vous pouvez modifier son nom et sa description. Après avoir supprimé ou déplacé ses passerelles Edge, vous pouvez supprimer un cluster Edge.

Attribution d'un cluster Edge à un VDC d'organisation

Après avoir créé un cluster Edge, vous pouvez attribuer ce cluster Edge à un VDC d'organisation en mettant à jour le profil réseau du VDC d'organisation. Vous pouvez attribuer un cluster Edge à un VDC d'organisation en tant que cluster Edge principal ou secondaire.

Si vous n'attribuez pas de cluster Edge secondaire, le dispositif Edge en veille d'une passerelle Edge en mode HA est déployé sur le cluster Edge principal mais sur un hôte différent de l'hôte exécutant le dispositif Edge principal.

Pour mettre à jour, afficher ou supprimer des profils de réseau VDC d'organisation, vous devez utiliser les méthodes `VdcNetworkProfile` vCloud OpenAPI. Reportez-vous à *Démarrage de vCloud OpenAPI* sur https://code.vmware.com.

Considérations :

- Les clusters Edge principal et secondaire doivent résider sur le même commutateur distribué vSphere.
- Si le VDC d'organisation utilise un pool de réseaux VXLAN, la zone de transport NSX doit couvrir les clusters de calcul et Edge.
- Si le VDC d'organisation utilise un pool de réseaux VLAN, les clusters Edge et les clusters de calcul doivent se trouver sur le même commutateur distribué vSphere.

Si vous mettez à nouveau à jour le cluster Edge principal ou secondaire d'un VDC d'organisation, pour déplacer une passerelle Edge existante vers le nouveau cluster, vous devez redéployer cette passerelle Edge. Reportez-vous à Redéployer une passerelle Edge.

Ajouter une passerelle Edge NSX Data Center for vSphere

Une passerelle Edge NSX Data Center for vSphere fournit à un réseau VDC d'organisation routé la connectivité aux réseaux externes et peut fournir des services, tels que l'équilibrage de charge, la traduction d'adresses réseau et un pare-feu.

À partir de vCloud Director 9.7, les passerelles Edge NSX Data Center for vSphere sont déployées sur des clusters Edge que vous avez précédemment créés et attribués au VDC d'organisation.

Vous pouvez ajouter une passerelle Edge IPv4 ou IPv6 qui se connecte à un ou plusieurs réseaux externes.

Note Les passerelles Edge IPv6 prennent en charge des services limités. Les passerelles Edge IPv6 prennent en charge les pare-feu Edge, les pare-feu distribués et le routage statique.

Conditions préalables

- Pour plus d'informations sur la configuration système requise pour le déploiement d'une passerelle Edge NSX Data Center for vSphere, reportez-vous au *Guide d'administration de NSX*.
- Si vous souhaitez déployer la passerelle Edge sur un cluster Edge dédié, créez et attribuez un cluster Edge au centre de données virtuel d'organisation. Reportez-vous à Utilisation des clusters Edge.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **Passerelles Edge**, puis sur **Nouveau**.
3. Sélectionnez le centre de données virtuel d'organisation reposant sur NSX-V sur lequel vous souhaitez créer la passerelle Edge, puis cliquez sur **Suivant**.
4. Entrez un nom et, éventuellement, une description pour la nouvelle passerelle Edge.
5. Activez ou laissez inactif chacun de ces paramètres généraux correspondant à la passerelle Edge.

Paramètre général	Description
Routage distribué	Configure la passerelle Edge pour fournir un routage logique distribué.
Mode FIPS	Configure la passerelle Edge pour utiliser le mode FIPS NSX.
Haute disponibilité	Active le basculement automatique vers une passerelle Edge de sauvegarde.

6. Sélectionnez la configuration de la passerelle Edge pour vos ressources système, puis cliquez sur **Suivant**.

Configuration	Description
Compacte	Requiert moins de ressources de mémoire et de calcul.
Grande	Fournit une plus grande capacité et des performances plus importantes que la configuration Compacte. Les configurations Grande et Extra grande offrent des fonctions de sécurité identiques.
Extra grande	À utiliser pour les environnements bénéficiant d'un équilibrage de charge avec un grand nombre de sessions simultanées.
Quadruple	À utiliser pour les environnements à débit élevé. Nécessite un débit de connexion élevé.

7 Sélectionnez un ou plusieurs sous-réseaux parmi les réseaux externes auxquels la passerelle Edge peut se connecter, puis cliquez sur **Suivant**.

   Si vous avez attribué un cluster Edge au VDC d'organisation, la liste affichée contient les réseaux externes accessibles à ce cluster Edge.

8 (Facultatif) Configurez un réseau en tant que passerelle par défaut.

   a Activez le bouton bascule **Configurer la passerelle par défaut**.

   b Cliquez sur la case d'option en regard du nom du réseau externe cible, puis sur celle en regard de l'adresse IP cible.

   c (Facultatif) Activez le bouton bascule **Utiliser la passerelle par défaut pour le relais DNS**.

9 Cliquez sur **Suivant**.

10 Activez ou laissez inactif chacun de ces paramètres avancés correspondant à la passerelle Edge, puis cliquez sur **Suivant**.

Paramètre avancé	Description
Paramètres IP	Vous pouvez entrer manuellement une adresse IP pour chaque sous-réseau de la passerelle Edge.
Sous-allouer des pools d'IP	Vous pouvez sous-allouer plusieurs pools d'adresses IP statiques à partir des pools d'adresses IP disponibles de chaque réseau externe sur la passerelle Edge.
Limites de débit	Vous pouvez configurer les limites de débit entrant et sortant pour chaque réseau externe sur la passerelle Edge.

11 (Facultatif) Si vous avez activé un ou plusieurs paramètres avancés à l'Étape étape 10, configurez chaque paramètre activé.

Paramètre avancé	Étapes
Paramètres IP	Pour chaque réseau de la passerelle Edge, dans la cellule **Adresses IP**, entrez une adresse IP, puis cliquez sur **Suivant**. Si vous n'entrez pas d'adresse IP pour un réseau, le système attribue une adresse IP arbitraire à ce réseau.
Sous-allouer des pools d'IP	1 Cliquez sur la case d'option en regard du nom d'un réseau externe, puis sur **Modifier**. Vous pouvez voir les pools d'adresses IP disponibles pour ce réseau externe et les pools d'adresses IP sous-alloués actuels, s'ils ont été configurés. 2 Modifiez les pools d'adresses IP sous-alloués pour ce réseau externe et cliquez sur **Enregistrer**. Vous pouvez ajouter des adresses IP et des plages à partir des plages de pools d'adresses IP disponibles. 3 Cliquez sur **Enregistrer**. Le système associe des plages d'adresses IP qui se chevauchent. 4 Cliquez sur **Suivant**. **Note** L'allocation d'adresses IP à une passerelle Edge est un processus par lequel le fournisseur attribue la propriété d'adresses IP à la passerelle. vCloud Director configure automatiquement l'interface de passerelle appropriée avec les adresses secondaires pendant le processus d'allocation. Si l'une des adresses IP est utilisée en dehors de vCloud Director, cela peut entraîner des conflits d'adresse IP.
Limites de débit	Pour chaque réseau externe sur la passerelle Edge, activez le bouton bascule **Activer**, entrez les limites dans les cellules **Taux entrant** et **Taux sortant**, puis cliquez sur **Suivant**.

12 Vérifiez la page **Prêt à terminer** et cliquez sur **Terminer**.

Configuration des services de passerelle Edge NSX Data Center for vSphere

Vous pouvez configurer des services, tels que DHCP, un pare-feu, la traduction d'adresses réseau (NAT) et un VPN sur une passerelle Edge.

Gestion d'un pare-feu de passerelle Edge NSX Data Center for vSphere

Pour protéger le trafic entrant et sortant sur une passerelle Edge, vous pouvez créer et gérer des règles de pare-feu sur cette passerelle Edge.

Pour plus d'informations sur la protection du trafic circulant entre les machines virtuelles dans un centre de données virtuel d'organisation, reportez-vous à Gestion du pare-feu distribué dans un centre de données virtuel d'organisation.

Les règles créées sur l'écran du pare-feu distribué pour lesquelles une passerelle Edge avancée est spécifiée dans la colonne Appliqué à ne s'affichent pas sur l'écran du pare-feu pour cette passerelle Edge avancée.

Les règles de pare-feu d'une passerelle Edge sont affichées dans l'écran **Pare-feu** et sont appliquées dans l'ordre suivant :

1 Règles internes, également appelées règles à montage automatique. Ces règles internes permettent le passage du trafic de contrôle des services de passerelle Edge.

2 Règles définies par l'utilisateur.

3 Règle par défaut.

Les paramètres de la règle par défaut s'appliquent au trafic qui ne correspond à aucune règle de pare-feu définie par l'utilisateur. La règle par défaut s'affiche au bas des règles sur l'écran du pare-feu.

Dans le portail de locataires, utilisez le bouton **Activer** sur l'écran des règles de pare-feu de la passerelle Edge pour désactiver ou activer un pare-feu de passerelle Edge.

Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere

L'onglet **Pare-feu** de la passerelle Edge vous permet d'ajouter des règles de pare-feu pour cette passerelle Edge. Vous pouvez ajouter plusieurs interfaces NSX Edge et groupes d'adresses IP en tant que source et destination pour les règles de pare-feu.

Le fait de spécifier **interne** pour la source ou la destination d'une règle indique le trafic pour tous les sous-réseaux sur les groupes de ports connectés à la passerelle NSX Edge. Si vous sélectionnez **interne** en tant que source, la règle est automatiquement mise à jour lorsque de nouvelles interfaces internes sont configurées sur la passerelle NSX.

Note Les règles de pare-feu de la passerelle Edge appliquées aux interfaces internes ne fonctionnent pas lorsque la passerelle Edge est configurée pour un routage dynamique.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Si l'écran **Règles de pare-feu** n'est pas visible, cliquez sur l'onglet **Pare-feu**.

3 Pour ajouter une règle sous une règle existante dans le tableau de règles du pare-feu, cliquez sur la ligne existante, puis cliquez sur le bouton **Créer**.

   Une ligne destinée à la nouvelle règle est ajoutée sous la règle sélectionnée ; par défaut, elle se voit attribuer n'importe quelle destination, n'importe quel service et l'action **Autoriser**. Si la règle définie par défaut par le système est l'unique règle du tableau du pare-feu, la nouvelle règle est ajoutée au-dessus de la règle par défaut.

4 Cliquez dans la cellule **Nom** et entrez un nom.

5 Cliquez dans la cellule **Source** et utilisez les icônes désormais visibles pour sélectionner la source à ajouter à la règle :

Option	Description
Cliquez sur l'icône IP	Saisissez la valeur source que vous souhaitez utiliser. Les valeurs valides sont une adresse IP, CIDR, une plage d'adresses IP ou le mot clé **tous**. Le pare-feu de la passerelle Edge prend en charge les formats IPv4 et IPv6.
Cliquez sur l'icône +	Utilisez l'icône **+** pour spécifier la source sous la forme d'un objet autre qu'une adresse IP spécifique : ■ Utilisez la fenêtre **Sélectionner des objets** pour ajouter des objets qui correspondent à vos sélections et cliquez sur **Conserver** pour les ajouter à la règle. ■ Pour exclure une source de la règle, ajoutez-la à cette règle à l'aide de la fenêtre **Sélectionner des objets**, puis sélectionnez l'icône d'exclusion pour exclure cette source de cette règle. Lorsque l'exclusion est sélectionnée sur la source, la règle est appliquée au trafic provenant de toutes les sources à l'exception de celle que vous avez exclue. Lorsque l'exclusion n'est pas sélectionnée, la règle s'applique au trafic provenant de la source que vous avez spécifiée dans la fenêtre **Sélectionner des objets**

6 Cliquez sur la cellule **Destination** et sélectionnez l'une des options suivantes :

Option	Description
Cliquez sur l'icône IP	Saisissez la valeur de destination que vous souhaitez utiliser. Les valeurs valides sont une adresse IP, CIDR, une plage d'adresses IP ou le mot clé **tous**. Le pare-feu de la passerelle Edge prend en charge les formats IPv4 et IPv6.
Cliquez sur l'icône +	Utilisez l'icône **+** pour spécifier la source sous la forme d'un objet autre qu'une adresse IP spécifique : ■ Utilisez la fenêtre **Sélectionner des objets** pour ajouter des objets qui correspondent à vos sélections et cliquez sur **Conserver** pour les ajouter à la règle. ■ Pour exclure une source de la règle, ajoutez-la à cette règle à l'aide de la fenêtre Sélectionner des objets, puis sélectionnez l'icône d'exclusion pour exclure cette source de cette règle. Lorsque l'exclusion est sélectionnée sur la source, la règle est appliquée au trafic provenant de toutes les sources à l'exception de celle que vous avez exclue. Lorsque l'exclusion n'est pas sélectionnée, la règle s'applique au trafic provenant de la source que vous avez spécifiée dans la fenêtre **Sélectionner des objets**

7 Cliquez sur la cellule **Service** de la nouvelle règle et cliquez sur l'icône **+** pour spécifier le service en tant que combinaison port-protocole :

a Sélectionnez le protocole de service.

b Tapez les numéros de port pour les ports source et de destination, ou spécifiez **tous**.

c Cliquez sur **Conserver**.

8 Dans la cellule **Action** de la nouvelle règle, configurez l'action de la règle.

Option	Description
Accepter	Autorise le trafic depuis ou vers les sources, les destinations et les services spécifiés.
Refuser	Bloque le trafic depuis ou vers les sources, les destinations et les services spécifiés.

9 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

Modifier les règles de pare-feu de la passerelle Edge NSX Data Center for vSphere

Seules les règles de pare-feu définies par l'utilisateur qui ont été ajoutées à une passerelle Edge peuvent être modifiées et supprimées. Vous ne pouvez pas modifier ou supprimer une règle générée automatiquement ni une règle par défaut, sauf lorsque vous modifiez le paramètre d'action de la règle par défaut. Vous pouvez modifier l'ordre de priorité des règles définies par l'utilisateur.

Pour plus d'informations sur les paramètres disponibles pour les différentes cellules d'une règle, reportez-vous à la section Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **Pare-feu**.

3 Gérez les règles de pare-feu.

   - Pour désactiver une règle, cliquez sur la coche verte dans la cellule **N°**. La coche verte prend l'aspect d'une icône rouge de désactivation. Si la règle est désactivée et que vous souhaitez l'activer, cliquez sur l'icône rouge de désactivation.
   - Pour modifier le nom d'une règle, double-cliquez dans la cellule **Nom** et saisissez le nouveau nom.
   - Pour modifier les paramètres d'une règle (par exemple, les paramètres de source ou d'action), sélectionnez la cellule appropriée et utilisez les contrôles affichés.
   - Pour supprimer une règle, sélectionnez-la et cliquez sur le bouton **Supprimer** situé au-dessus du tableau de règles.
   - Pour masquer les règles générées par le système, utilisez le bouton **Afficher uniquement les règles définies par l'utilisateur**.
   - Pour déplacer une règle vers le haut ou vers le bas dans le tableau des règles, sélectionnez la règle et cliquez sur la flèche vers le haut ou sur la flèche vers le bas au-dessus du tableau des règles.

4 Cliquez sur **Enregistrer les modifications**.

Appliquer les paramètres du serveur Syslog à une passerelle Edge NSX Data Center for vSphere

Si vous avez activé la journalisation pour une ou plusieurs règles de pare-feu de passerelle Edge, la passerelle Edge se connecte au serveur syslog. Si vous avez créé une passerelle Edge avant la configuration initiale du serveur syslog ou si vous avez changé les paramètres du serveur syslog, vous devez synchroniser les paramètres du serveur syslog pour cette passerelle Edge.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

3 Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Synchroniser Syslog**.

4 Pour confirmer, cliquez sur **OK**.

Gestion du protocole DHCP de la passerelle Edge NSX Data Center for vSphere

Vous configurez vos passerelles Edge pour fournir des services de protocole de configuration dynamique d'hôte (DHCP) aux machines virtuelles connectées aux réseaux de centre de données virtuel d'organisation associés.

Comme l'explique la documentation sur NSX, une passerelle Edge NSX inclut des capacités de pooling d'adresses IP, d'allocation d'adresses IP statiques de type « Une à une » et de configuration de serveur DNS externe. La liaison d'adresse IP statique se base sur l'ID d'objet géré et l'ID d'interface de la machine virtuelle cliente faisant la demande.

Le service DHCP pour une passerelle NSX Edge :

- Écoute sur l'interface interne de la passerelle Edge pour la découverte DHCP.
- Utilise l'adresse IP de l'interface interne de la passerelle Edge en tant qu'adresse de passerelle par défaut pour tous les clients.
- Utilise les valeurs de masque de sous-réseau et de diffusion de l'interface interne pour le réseau conteneur.

Dans les situations suivantes, vous devez redémarrer le service DHCP sur les machines virtuelles clientes dont les adresses IP sont attribuées par le DHCP :

- Vous avez modifié ou supprimé un pool DHCP, la passerelle par défaut ou le serveur DNS.
- Vous avez modifié l'adresse IP interne de l'instance de passerelle Edge.

Note Si les paramètres DNS d'une passerelle Edge sur laquelle le DHCP est activé sont modifiés, la passerelle Edge peut cesser de fournir des services DHCP. Si cette situation se produit, utilisez le bouton **État du service DHCP** de l'écran Pools DHCP pour désactiver, puis réactiver DHCP sur la passerelle Edge. Reportez-vous à Ajouter un pool d'adresses IP DHCP.

Ajouter un pool d'adresses IP DHCP

Vous pouvez configurer les pools d'adresses IP requis pour un service DHCP de passerelle Edge NSX Data Center for vSphere. DHCP automatise l'attribution d'adresses IP aux machines virtuelles connectées aux réseaux de centre de données virtuel d'organisation.

Comme cela est décrit dans la documentation sur l'*administration de NSX*, le service DHCP nécessite un pool d'adresses IP. Un pool d'adresses IP est une plage séquentielle d'adresses IP au sein du réseau. Une adresse IP de ce pool est attribuée aux machines virtuelles protégées par la passerelle Edge qui n'ont pas d'adresse liée. Il ne peut pas y avoir d'intersection entre les plages de pools d'adresses IP. Ainsi, une adresse IP donnée ne peut appartenir qu'à un seul pool d'adresses IP.

Note Au moins un pool d'adresses IP DHCP doit être configuré pour que l'état du service DHCP soit activé.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **DHCP > Pools**.

3 Si le service DHCP n'est pas actuellement activé, activez le bouton bascule **État du service DHCP**.

   Note Après l'activation du bouton bascule **État du service DHCP**, ajoutez au moins un pool d'adresses IP DHCP avant d'enregistrer les modifications. Si aucun pool d'adresses IP DHCP ne figure dans l'écran et que vous activez le bouton bascule **État du service DHCP**, puis enregistrez les modifications, l'écran s'affiche avec le bouton bascule désactivé.

4 Sous Pools DHCP, cliquez sur le bouton **Créer** (+), spécifiez les détails du pool DHCP et cliquez sur **Conserver**.

Option	Description
Plage d'adresses IP	Saisissez une plage d'adresses IP.
Nom de domaine	Nom de domaine du serveur DNS.
Configurer automatiquement le DNS	Activez ce bouton bascule pour utiliser la configuration du service DNS pour la liaison DNS de ce pool d'adresses IP. S'il est activé, le **Serveur de noms principal** et le **Serveur de noms secondaire** sont définis sur **Auto**.
Serveur de noms principal	Si vous n'activez pas **Configurer automatiquement le DNS**, tapez l'adresse IP de votre serveur DNS principal. Cette adresse IP est utilisée pour la résolution de noms d'hôte en adresses IP.

Option	Description
Serveur de noms secondaire	Si vous n'activez pas **Configurer automatiquement le DNS**, tapez l'adresse IP de votre serveur DNS secondaire. Cette adresse IP est utilisée pour la résolution de noms d'hôte en adresses IP.
Passerelle par défaut	Entrez l'adresse de la passerelle par défaut. Si vous n'indiquez pas l'adresse IP de la passerelle par défaut, c'est l'interface interne de l'instance de la passerelle Edge qui est adoptée comme passerelle par défaut.
Masque de sous-réseau	Tapez le masque de sous-réseau de l'interface de passerelle Edge.
Le bail n'expire jamais	Activez ce bouton bascule pour que les adresses IP attribuées à partir de ce pool soient liées indéfiniment aux machines virtuelles auxquelles elles sont attribuées. Lorsque vous sélectionnez cette option, **Durée de bail** est définie sur l'infini.
Durée de bail (en secondes)	Durée (en secondes) pendant laquelle les adresses IP attribuées par DHCP sont allouées aux clients. La durée du bail par défaut est d'un jour (86 400 secondes). **Note** Vous ne pouvez pas spécifier de durée de bail lorsque vous sélectionnez **Le bail n'expire jamais**.

5 Cliquez sur **Enregistrer les modifications**.

Résultats

vCloud Director met à jour la passerelle Edge pour qu'elle fournisse des services DHCP.

Ajouter des liaisons DHCP

Si vous avez des services s'exécutant sur une machine virtuelle et ne voulez pas que l'adresse IP soit modifiée, vous pouvez lier l'adresse MAC des machines virtuelles à leur adresse IP. L'adresse IP que vous liez ne doit pas chevaucher un pool d'adresses IP DHCP.

Conditions préalables

Vous disposez des adresses MAC des machines virtuelles pour lesquelles vous souhaitez définir des liaisons.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Dans l'onglet **Liaisons > DHCP**, cliquez sur le bouton **Créer** ( ), indiquez les détails de la liaison, puis cliquez sur **Conserver**.

Option	Description
Adresse MAC	Tapez l'adresse MAC de la machine virtuelle que vous souhaitez lier à l'adresse IP.
Nom de l'hôte	Tapez le nom d'hôte que vous souhaitez définir pour cette machine virtuelle lorsque celle-ci demande un bail DHCP.
Adresse IP	Tapez l'adresse IP que vous souhaitez lier à l'adresse MAC.
Masque de sous-réseau	Tapez le masque de sous-réseau de l'interface de passerelle Edge.
Nom de domaine	Entrez le nom de domaine du serveur DNS.
Configurer automatiquement le DNS	Activez ce bouton bascule pour utiliser la configuration du service DNS pour cette liaison DNS. S'il est activé, le **Serveur de noms principal** et le **Serveur de noms secondaire** sont définis sur **Auto**.
Serveur de noms principal	Si vous ne sélectionnez pas **Configurer automatiquement le DNS**, tapez l'adresse IP de votre serveur DNS principal. Cette adresse IP est utilisée pour la résolution de noms d'hôte en adresses IP.
Serveur de noms secondaire	Si vous ne sélectionnez pas **Configurer automatiquement le DNS**, tapez l'adresse IP de votre serveur DNS secondaire. Cette adresse IP est utilisée pour la résolution de noms d'hôte en adresses IP.
Passerelle par défaut	Entrez l'adresse de la passerelle par défaut. Si vous n'indiquez pas l'adresse IP de la passerelle par défaut, c'est l'interface interne de l'instance de la passerelle Edge qui est adoptée comme passerelle par défaut.
Le bail n'expire jamais	Activez ce bouton bascule pour garder l'adresse IP liée indéfiniment à cette adresse MAC. Lorsque vous sélectionnez cette option, **Durée de bail** est définie sur l'infini.
Durée de bail (en secondes)	Durée (en secondes) pendant laquelle les adresses IP attribuées par DHCP sont allouées aux clients. La durée du bail par défaut est d'un jour (86 400 secondes). **Note** Vous ne pouvez pas spécifier de durée de bail lorsque vous sélectionnez **Le bail n'expire jamais**.

3 Cliquez sur **Enregistrer les modifications**.

Configuration du relais DHCP pour les passerelles Edge NSX Data Center for vSphere

La capacité de relais DHCP fournie par NSX dans votre environnement vCloud Director vous permet d'exploiter votre infrastructure DHCP existante à partir de votre environnement vCloud Director sans interruption de la gestion des adresses IP dans votre infrastructure DHCP existante. Les messages DHCP sont relayés des machines virtuelles vers les serveurs DHCP désignés dans

votre infrastructure DHCP physique, ce qui permet aux adresses IP contrôlées par le logiciel NSX de continuer à être synchronisées avec les adresses IP dans le reste de vos environnements contrôlés par DHCP.

La configuration de relais DHCP d'une passerelle Edge peut répertorier plusieurs serveurs DHCP. Des demandes sont envoyées à tous les serveurs répertoriés. Pendant le relais de la demande DHCP à partir de machines virtuelles, la passerelle Edge ajoute une adresse IP de passerelle à la demande. Le serveur DHCP externe utilise cette adresse de passerelle pour faire correspondre un pool et allouer une adresse IP à la demande. L'adresse de la passerelle doit appartenir à un sous-réseau de l'interface de la passerelle Edge.

Vous pouvez spécifier un serveur DHCP différent pour chaque passerelle Edge et configurer plusieurs serveurs DHCP sur chaque passerelle Edge pour prendre en charge plusieurs domaines IP.

Note

- Le relais DHCP ne prend pas en charge les espaces d'adresses IP qui se chevauchent.
- Le relais DHCP et le service DHCP ne peuvent pas s'exécuter sur la même vNIC (carte réseau virtuelle) en même temps. Si un agent de relais est configuré sur une vNIC, il n'est pas possible de configurer un pool DHCP sur les sous-réseaux de cette vNIC. Pour plus d'informations, consultez le *Guide d'administration NSX*.

Spécifier une configuration de relais DHCP pour une passerelle Edge NSX Data Center for vSphere

Le logiciel NSX dans votre environnement vCloud Director offre la possibilité, pour la passerelle Edge, de relayer les messages DHCP vers des serveurs DHCP externes au centre de données virtuel de votre organisation vCloud Director. Vous pouvez configurer la fonctionnalité de relais DHCP de la passerelle Edge.

Comme cela est décrit dans la documentation sur l'*administration de NSX*, les serveurs DHCP peuvent être spécifiés à l'aide d'un ensemble d'adresses IP existant, d'un bloc d'adresses IP, d'un domaine ou d'une combinaison de ces éléments. Les messages DHCP sont relayés vers chaque serveur DHCP spécifié.

Vous devez également configurer au moins un agent de relais DHCP. Un agent de relais DHCP est une interface sur la passerelle Edge à partir de laquelle les demandes DHCP sont relayées aux serveurs DHCP externes.

Conditions préalables

Si vous souhaitez utiliser un ensemble d'adresses IP pour spécifier un serveur DHCP, vérifiez qu'un ensemble d'adresses IP existe en tant qu'objet de regroupement accessible à la passerelle Edge. Reportez-vous à Créer un ensemble d'adresses IP à utiliser dans les règles de pare-feu et la configuration du relais DHCP.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **DHCP > Relais**.

3 Utilisez les champs à l'écran pour spécifier les serveurs DHCP par adresses IP, noms de domaine ou ensembles d'adresses IP.

   Utilisez le bouton **Ajouter** ( ) pour parcourir les ensembles d'adresses IP existants et sélectionner ceux qui vous intéressent.

4 Configurez un agent de relais DHCP et ajoutez sa configuration au tableau à l'écran en cliquant sur le bouton **Ajouter** ( ), en sélectionnant une vNIC et l'adresse IP de sa passerelle, puis en cliquant sur **Conserver**.

   Par défaut, l'adresse IP de la passerelle correspond à l'adresse principale de la vNIC sélectionnée. Vous pouvez conserver la valeur par défaut ou sélectionner une autre adresse, si elle est disponible sur cette vNIC.

5 Cliquez sur **Enregistrer les modifications**.

Ajouter une règle SNAT ou DNAT

Vous pouvez créer une règle NAT source (SNAT) pour rendre privée l'adresse IP source publique et inversement. Vous pouvez créer une règle NAT de destination (DNAT) pour rendre privée l'adresse IP de destination publique et inversement.

Lorsque vous créez des règles NAT, vous pouvez spécifier les adresses IP d'origine et converties en utilisant les formats suivants :

- Adresse IP ; par exemple, 192.0.2.0
- Plage d'adresses IP ; par exemple, 192.0.2.0-192.0.2.24
- Adresse IP/masque de sous-réseau ; par exemple, 192.0.2.0/24
- any

Lorsque vous configurez une règle SNAT ou DNAT sur une passerelle Edge dans l'environnement vCloud Director, vous configurez toujours la règle du point de vue de votre centre de données virtuel d'organisation. Une règle SNAT traduit l'adresse IP source des paquets envoyés à partir du réseau d'un centre de données virtuel d'organisation vers un réseau externe ou un

autre réseau de centre de données virtuel d'organisation. Une règle DNAT traduit l'adresse IP, et éventuellement le port, des paquets reçus par un réseau de centre de données virtuel d'organisation en provenance d'un réseau externe ou d'un autre réseau de centre de données virtuel d'organisation.

Conditions préalables

Les adresses IP publiques doivent avoir été ajoutées à l'interface de la passerelle Edge NSX Data Center for vSphere sur laquelle vous voulez ajouter la règle. Pour des règles DNAT, l'adresse IP (publique) initiale doit avoir été ajoutée à l'interface de la passerelle Edge et pour les règles SNAT, l'adresse IP convertie (publique) doit avoir été ajoutée à l'interface.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur **NAT** pour afficher l'écran des règles NAT.

3 Selon le type de règle NAT que vous créez, cliquez sur **Règle DNAT** ou **Règle SNAT**.

4 Configurez une règle NAT de destination (de l'extérieur vers l'intérieur).

Option	Description
Appliqué sur	Sélectionnez l'interface sur laquelle appliquer la règle.
IP/plage d'origine	Entrez l'adresse IP requise. Cette adresse doit être l'adresse IP publique de la passerelle Edge pour laquelle vous configurez la règle DNAT. Dans le paquet en cours d'inspection, cette adresse IP ou cette plage est celle qui apparaît comme adresse IP de destination du paquet. Ces adresses de destination du paquet sont celles traduites par cette règle DNAT.
Protocole	Sélectionnez le protocole auquel la règle s'applique. Pour appliquer cette règle à tous les protocoles, sélectionnez **Tous**.
Port d'origine	(Facultatif) Sélectionnez le port ou la plage de ports que le trafic entrant utilise sur la passerelle Edge pour se connecter au réseau interne sur lequel les machines virtuelles sont connectées. Cette sélection n'est pas disponible lorsque le **Protocole** est défini sur **ICMP** ou sur **Tous**.
Type ICMP	Lorsque vous sélectionnez **ICMP** (un utilitaire de signalement d'erreur et de diagnostic utilisé entre les périphériques pour communiquer des informations d'erreur) pour **Protocole**, sélectionnez le **Type ICMP** dans le menu déroulant. Les messages ICMP sont identifiés par le champ type. Par défaut, le type ICMP est défini sur tous.

Option	Description
Adresse IP/plage traduite	Tapez l'adresse IP ou la plage d'adresses IP vers laquelle les adresses de destination des paquets entrants seront traduites. Ces adresses sont les adresses IP d'une ou plusieurs machines virtuelles pour lesquelles vous configurez DNAT afin qu'elles puissent recevoir le trafic depuis le réseau externe.
Port traduit	(Facultatif) Sélectionnez le port ou la plage de ports avec lesquels le trafic entrant se connecte sur les machines virtuelles du réseau interne. Ces ports sont ceux vers lesquels la règle DNAT effectue la traduction pour les paquets entrants destinés aux machines virtuelles.
Description	(Facultatif) Saisissez une description qui permet d'identifier ce que fait cette règle.
Activé	Activez cette option pour activer cette règle.
Activer la journalisation	Activez cette option pour que la traduction d'adresses effectuée par cette règle soit consignée.

5 Configurez une règle NAT source (de l'intérieur vers l'extérieur).

Option	Description
Appliqué sur	Sélectionnez l'interface sur laquelle appliquer la règle.
IP/plage source d'origine	Tapez l'adresse IP ou la plage d'adresses IP d'origine à appliquer à cette règle. Ces adresses sont les adresses IP d'une ou plusieurs machines virtuelles pour lesquelles vous configurez la règle SNAT, afin qu'elles puissent envoyer du trafic vers le réseau externe.
IP/plage source traduite	Entrez l'adresse IP requise. Cette adresse est toujours l'adresse IP publique de la passerelle pour laquelle vous configurez la règle SNAT. Spécifie l'adresse IP vers laquelle les adresses source (les machines virtuelles) des paquets sortants sont traduites lorsqu'elles envoient du trafic vers le réseau externe.
Description	(Facultatif) Saisissez une description qui permet d'identifier ce que fait cette règle.
Activé	Activez cette option pour activer cette règle.
Activer la journalisation	Activez cette option pour que la traduction d'adresses effectuée par cette règle soit consignée.

6 Cliquez sur **Conserver** pour ajouter la règle à la table affichée à l'écran.

7 Répétez les étapes pour configurer des règles supplémentaires.

8 Cliquez sur **Enregistrer les modifications** pour enregistrer les règles dans le système.

Étape suivante

Ajoutez les règles de pare-feu de passerelle Edge correspondant aux règles SNAT ou DNAT que vous venez de configurer. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Configuration de routage avancée

Vous pouvez configurer les fonctionnalités de routage statique et dynamique fournies par le logiciel NSX pour vos passerelles Edge NSX Data Center for vSphere.

Pour activer le routage dynamique, vous devez configurer une passerelle Edge avancée à l'aide des protocoles BGP (Border Gateway Protocol) ou OSPF (Open Shortest Path First).

Pour obtenir des informations détaillées sur les capacités de routage fournies par NSX, consultez la section *Routage* dans la documentation d'*administration de NSX*.

Vous pouvez spécifier un routage statique et dynamique pour chaque passerelle Edge avancée. La fonctionnalité de routage dynamique fournit les informations de transfert nécessaires entre des domaines de diffusion de la couche 2, ce qui vous permet de diminuer les domaines de diffusion de la couche 2 et d'améliorer l'efficacité et l'échelle du réseau. NSX étend ces informations aux emplacements des charges de travail pour un routage horizontal. Cette fonctionnalité permet une communication plus directe entre les machines virtuelles sans devoir procéder à une extension de sauts longue et coûteuse.

Spécifier les configurations de routage par défaut pour la passerelle Edge NSX Data Center for vSphere

Vous pouvez spécifier les paramètres par défaut pour le routage statique et le routage dynamique pour une passerelle Edge.

Note Pour supprimer tous les paramètres de routage configurés, utilisez le bouton **EFFACER LA CONFIGURATION GLOBALE** situé en bas de l'écran de **Configuration de routage**. Cette action supprime tous les paramètres de routage actuellement spécifiés dans les sous-écrans : paramètres de routage par défaut, routes statiques, OSPF, BGP et redistribution de route.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Routage > Configuration de routage**.

3 Pour activer le routage ECMP (Equal Cost Multipath) pour cette passerelle Edge, activez le commutateur **ECMP**.

   Comme décrit dans la documentation *Administration NSX*, ECMP est une stratégie de routage qui permet que la transmission du paquet de saut suivant vers une destination unique se produise sur plusieurs meilleurs chemins. NSX détermine ces meilleurs chemins soit de

manière statique, à l'aide de routes statiques configurées, ou suite à des calculs métriques effectués par des protocoles de routage dynamique tels que OSPF ou BGP. Vous pouvez spécifier les chemins multiples des routes statiques en spécifiant plusieurs sauts suivants sur l'écran Routes statiques.

Pour plus de détails sur ECMP et NSX, consultez les rubriques traitant du routage dans le *Guide de dépannage de NSX*.

4 Spécifiez les paramètres de la passerelle de routage par défaut.

a Utilisez la liste déroulante **Appliqué sur** pour sélectionner une interface à partir de laquelle le saut suivant vers le réseau de destination peut être atteint.

Pour afficher des détails sur l'interface sélectionnée, cliquez sur l'icône d'information bleue.

b Entrez l'adresse IP de la passerelle.

c Saisissez la MTU.

d (Facultatif) Entrez une description facultative.

e Cliquez sur **Enregistrer les modifications**.

5 Spécifiez les paramètres de routage dynamique par défaut.

Note Si VPN IPsec est configuré dans votre environnement, vous ne devez pas utiliser le routage dynamique.

a Sélectionnez un ID de routeur.

Vous pouvez sélectionner un ID de routeur dans la liste ou utiliser l'icône **+** pour en choisir un nouveau. Cet ID de routeur est la première adresse IP ascendante de la passerelle Edge qui envoie des routes au noyau pour le routage dynamique.

b Configurez la journalisation en activant le commutateur **Activer la journalisation** et en sélectionnant le niveau de journalisation.

c Cliquez sur **OK**.

6 Cliquez sur **Enregistrer les modifications**.

Étape suivante

Ajouter des routes statiques. Reportez-vous à Ajouter une route statique.

Configurer la redistribution de route Reportez-vous à Configurer les redistributions de route.

Configurer le routage dynamique. Consultez les rubriques suivantes :

- Configurer BGP
- Configurer OSPF

Ajouter une route statique

Vous pouvez ajouter un itinéraire statique pour un sous-réseau ou un hôte de destination.

Si ECMP est activé dans la configuration de routage par défaut, vous pouvez spécifier plusieurs sauts suivants dans les routes statiques. Reportez-vous à la section Spécifier les configurations de routage par défaut pour la passerelle Edge NSX Data Center for vSphere pour voir les étapes concernant l'activation d'ECMP.

Conditions préalables

Comme décrit dans la documentation de NSX, l'adresse IP du saut suivant de la route statique doit exister dans un sous-réseau associé à l'une des interfaces de la passerelle Edge NSX Data Center for vSphere. Dans le cas contraire, la configuration de cette route statique échoue.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Routage > Routes statiques**.

3 Cliquez sur le bouton **Créer** ( ).

4 Configurez les options suivantes pour la route statique :

Option	Description
Réseau	Saisissez le réseau en notation CIDR.
Prochain saut	Saisissez l'adresse IP du saut suivant. L'adresse IP du saut suivant doit exister dans un sous-réseau associé à l'une des interfaces de la passerelle Edge. Si ECMP est activé, vous pouvez saisir plusieurs sauts suivants.
MTU	Modifiez la valeur de transmission maximale pour les paquets de données. La valeur MTU ne peut pas être supérieure à celle définie sur l'interface de passerelle Edge sélectionnée. Vous pouvez voir le MTU défini sur l'interface de passerelle Edge par défaut sur l'écran Configuration de routage.
Interface	Le cas échéant, sélectionnez l'interface de la passerelle Edge sur laquelle vous voulez ajouter une route statique. Par défaut, l'interface qui correspond à l'adresse du saut suivant est sélectionnée.
Description	Saisissez éventuellement la description de la route statique.

5 Cliquez sur **Enregistrer les modifications**.

Étape suivante

Configurez une règle NAT pour la route statique. Reportez-vous à Ajouter une règle SNAT ou DNAT.

Ajoutez une règle de pare-feu pour autoriser le trafic à traverser la route statique. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Configurer OSPF

Vous pouvez configurer le protocole de routage OSPF (Open Shortest Path First) pour les capacités de routage dynamique d'une passerelle Edge NSX Data Center for vSphere. Une application courante du protocole OSPF sur une passerelle Edge dans un environnement vCloud Director consiste à échanger des informations de routage entre les passerelles Edge de vCloud Director.

La passerelle NSX Edge prend en charge OSPF, un protocole de passerelle interne qui achemine les paquets IP uniquement au sein d'un seul domaine de routage. Comme décrit dans la documentation d'*administration de NSX*, la configuration d'OSPF sur une passerelle NSX Edge permet à cette dernière d'apprendre et d'annoncer des routes. La passerelle Edge se sert d'OSPF pour recueillir des informations sur l'état des liens auprès des passerelles Edge disponibles et construire une carte de topologie du réseau. La topologie détermine la table de routage présentée à la couche Internet, laquelle prend des décisions de routage en fonction de l'adresse IP de destination trouvée dans les paquets IP.

Ainsi, les stratégies de routage OSPF fournissent un processus dynamique d'équilibrage de charge du trafic entre des routes à coût égal. Un réseau OSPF est divisé en zones de routage afin d'optimiser le flux de trafic et de limiter la taille des tables de routage. Une zone est une collection logique de réseaux, routeurs et liens OSPF ayant la même identification de zone. Les zones sont identifiées par un ID de zone.

Conditions préalables

Vous devez configurer un ID de routeur. Pour plus d'informations, reportez-vous à Spécifier les configurations de routage par défaut pour la passerelle Edge NSX Data Center for vSphere.

Procédure

1. Ouvrez les services de passerelle Edge.
   a. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
   b. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
   c. Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.
2. Accédez à **Routage > OSPF**.
3. Si OSPF n'est pas activé, utilisez le bouton bascule **OSPF activé**.

4 Configurez les paramètres OSPF selon les besoins de votre organisation.

Option	Description
Activer le redémarrage normal	Indique que le transfert des paquets doit demeurer sans interruption lors du redémarrage des services OSPF.
Activer la provenance par défaut	Permet à la passerelle Edge à s'annoncer en tant que passerelle par défaut à ses homologues OSPF.

5 (Facultatif) Vous pouvez cliquer sur **Enregistrer les modifications** ou continuer avec la configuration des définitions de zone et des mappages d'interface.

6 Ajoutez une définition de zone OSPF en cliquant sur le bouton **Ajouter** ( ), en spécifiant les détails du mappage dans la boîte de dialogue, puis en cliquant sur **Conserver**.

Note Par défaut, le système configure une zone NSSA (not-so-stubby area) avec l'ID de zone de 51. Cette zone ne s'affiche pas automatiquement dans la table de définitions de zone sur l'écran OSPF. Vous pouvez modifier ou supprimer la zone NSSA.

Option	Description
ID de zone	Tapez un ID de zone sous la forme d'une adresse IP ou d'un nombre décimal.
Type de zone	Sélectionnez **Normal** ou **NSSA**. Les NSSA empêchent la saturation des annonces d'état des liens (LSA) externes aux AS dans les NSSA. Comme elles reposent sur le routage par défaut vers des destinations externes, elles doivent être placées en périphérie d'un domaine de routage OSPF. Une NSSA peut importer des routes externes dans le domaine de routage OSPF, offrant ainsi un service de transit vers les petits domaines de routage ne faisant pas partie du domaine de routage OSPF.
Authentification de zone	Sélectionnez le type d'authentification qu'OSPF doit effectuer au niveau de la zone. Toutes les passerelles Edge au sein de la zone doivent avoir la même authentification et le même mot de passe correspondant configuré. Pour que l'authentification MD5 fonctionne, le récepteur et l'émetteur doivent posséder la même clé MD5. Les options possibles sont les suivantes : ■ **Aucun** Aucune authentification n'est requise. ■ **Mot de passe** Avec cette option, le mot de passe que vous spécifiez dans le champ **Valeur d'authentification de zone** est inclus dans le paquet transmis. ■ **MD5** Avec cette option, l'authentification utilise le chiffrement MD5 (Message Digest type 5). Un total de contrôle MD5 est inclus dans le paquet transmis. Dans le champ **Valeur d'authentification de zone**, tapez la clé MD5.

7 Cliquez sur **Enregistrer les modifications** pour que les définitions de zone récemment configurées soient disponibles en sélection lorsque vous ajoutez des mappages d'interface.

8 Ajoutez un mappage d'interfaces en cliquant sur le bouton **Ajouter** ( ), en spécifiant les détails du mappage dans la boîte de dialogue, puis en cliquant sur **Conserver**.

Ces mappages associent les interfaces de la passerelle Edge aux zones.

a Dans la boîte de dialogue, sélectionnez l'interface que vous souhaitez mapper à une définition de zone.

L'interface spécifie le réseau externe auquel les deux passerelles Edge sont connectées.

b Sélectionnez l'ID de zone de la zone à mapper à l'interface sélectionnée.

c (Facultatif) Modifiez les paramètres OSPF à partir des valeurs par défaut afin de les personnaliser pour ce mappage d'interface.

Lorsque vous configurez un nouveau mappage, les valeurs par défaut de ces paramètres sont affichées. Dans la plupart des cas, il est recommandé de conserver les paramètres par défaut. Si vous ne modifiez pas les paramètres, assurez-vous que les homologues OSPF utilisent les mêmes.

Option	Description
Intervalle de salutation	Intervalle (en secondes) entre les paquets de salutation qui sont envoyés sur l'interface.
Intervalle d'inactivité	Intervalle (en secondes) pendant lequel au moins un paquet de salutation doit être reçu d'un voisin avant que ce dernier ne soit déclaré inactif.
Priorité	Priorité de l'interface. L'interface avec la priorité la plus élevée est le routeur de la passerelle Edge désignée.
Coût	Capacité supplémentaire requise pour envoyer des paquets sur cette interface. Le coût d'une interface est inversement proportionnel à la bande passante de cette interface. Plus la bande passante est grande et plus les coûts diminuent.

d Cliquez sur **Conserver**.

9 Cliquez sur **Enregistrer les modifications** sur l'écran OSPF.

Étape suivante

Configurez OSPF sur les autres passerelles Edge avec lesquelles vous souhaitez échanger des informations de routage.

Ajoutez une règle de pare-feu qui autorise le trafic entre les passerelles Edge activées pour OSPF. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Assurez-vous que la redistribution des routes et la configuration du pare-feu permettent l'annonce des routes correctes. Reportez-vous à Configurer les redistributions de route.

Configurer BGP

Vous pouvez configurer le protocole BGP (Border Gateway Protocol) pour les capacités de routage dynamique d'une passerelle Edge NSX Data Center for vSphere.

Comme décrit dans le *Guide d'administration de NSX*, BGP prend des décisions de routage de base en se servant d'une table de réseaux ou de préfixes IP qui désignent l'accessibilité des réseaux entre plusieurs systèmes autonomes. Dans le domaine de la mise en réseau, le terme routeur BGP désigne un périphérique de mise en réseau exécutant BGP. Deux routeurs BGP établissent une connexion avant tout échange d'informations de routage. Le terme voisin BGP désigne un routeur BGP qui a établi une connexion de ce type. Après avoir établi la connexion, les périphériques échangent des routes et synchronisent leurs tables. Chaque périphérique envoie des messages de survie pour maintenir la relation active.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Routage > BGP**.

3 Si BGP n'est pas activé, utilisez le bouton bascule **Activer BGP**.

4 Configurez les paramètres BGP selon les besoins de votre organisation.

Option	Description
Activer le redémarrage normal	Indique que le transfert des paquets doit demeurer sans interruption lors du redémarrage des services BGP.
Activer la provenance par défaut	Permet à la passerelle Edge de s'annoncer en tant que passerelle par défaut à ses voisins BGP.
AS local	Requis. Indiquez le numéro d'identification du système autonome (AS) à utiliser pour la fonctionnalité AS local du protocole. La valeur que vous indiquez doit être un numéro global unique compris entre 1 et 65 534. L'AS local est une fonctionnalité de BGP. Le système attribue le numéro de l'AS local à la passerelle Edge que vous configurez. La passerelle Edge annonce cet ID lorsque la passerelle Edge établit une homologation avec ses voisins BGP dans d'autres systèmes autonomes. Le chemin d'accès des systèmes autonomes traversant une route est utilisé comme mesure dans l'algorithme de routage dynamique lors de la sélection du meilleur itinéraire vers une destination.

5 Vous pouvez choisir de cliquer sur **Enregistrer les modifications** ou de continuer avec la configuration des paramètres des voisins de routage BGP.

6 Ajoutez une configuration de voisin BGP en cliquant sur le bouton **Ajouter** ( ), en spécifiant les détails du voisin dans la boîte de dialogue, puis en cliquant sur **Conserver**.

Option	Description
Adresse IP	Tapez l'adresse IP d'un voisin BGP pour cette passerelle Edge.
AS distant	Tapez un numéro global unique compris entre 1 et 65 534 pour le système autonome auquel appartient ce voisin BGP. Ce numéro de l'AS distant est utilisé dans l'entrée du voisin BGP dans la table des voisins BGP du système.
Poids	Poids par défaut de la connexion du voisin. Le cas échéant, modifiez ce paramètre pour répondre aux besoins de votre organisation.
Durée de survie	Fréquence à laquelle le logiciel envoie des messages de survie à son homologue. La fréquence par défaut est de 60 secondes. Ajustez cette valeur selon les besoins de votre organisation.
Durée de retenue	Intervalle pendant lequel le logiciel déclare l'inactivité d'un homologue après la non-réception d'un message de survie. Cet intervalle doit être trois fois celui de l'intervalle de survie. L'intervalle par défaut est de 180 secondes. Ajustez cette valeur selon les besoins de votre organisation. Une fois l'homologation entre les deux voisins BGP terminée, la passerelle Edge démarre un temporisateur de retenue. Chaque message de survie qu'elle reçoit du voisin réinitialise le temporisateur de retenue à 0. Si la passerelle Edge ne parvient pas à recevoir trois messages de survie consécutifs, de sorte que le temporisateur de retenue atteigne trois fois l'intervalle de survie, elle considère que le voisin est inactif et supprime les routes venant de lui.
Mot de passe	Si ce voisin BGP requiert une authentification, tapez le mot de passe d'authentification. Chaque segment envoyé sur la connexion entre les voisins est vérifié. L'authentification MD5 doit être configurée avec le même mot de passe sur les deux voisins BGP, sinon la connexion entre eux ne sera pas établie.
Filtres BGP	Utilisez cette table pour définir le filtrage des routes à l'aide d'une liste des préfixes provenant de ce voisin BGP. **Attention** Une règle `Bloquer tout` est appliquée à la fin des filtres. Ajoutez un filtre à la table en cliquant sur l'icône **+** et en configurant les options. Cliquez sur **Conserver** pour enregistrer chaque filtre. ■ Sélectionnez la direction pour indiquer si vous filtrez le trafic vers ou depuis le voisin. ■ Sélectionnez l'action pour indiquer si vous autorisez ou refusez le trafic. ■ Tapez le réseau que vous souhaitez filtrer vers ou depuis le voisin. Tapez `ANY` ou un réseau au format CIDR. ■ Tapez le **GE de préfixe IP** et le **LE de préfixe IP** pour utiliser les mots clés `le` et `ge` dans la liste des préfixes IP.

7 Cliquez sur **Enregistrer les modifications** pour enregistrer les configurations dans le système.

Étape suivante

Configurez BGP sur les autres passerelles Edge avec lesquelles vous souhaitez échanger des informations de routage.

Ajoutez une règle de pare-feu qui autorise le trafic vers et depuis les passerelles Edge configurées pour BGP. Consultez Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere pour plus d'informations.

Configurer les redistributions de route

Par défaut, le routeur ne partage les routes qu'avec d'autres routeurs exécutant le même protocole. Lorsque vous avez configuré un environnement multi-protocole, vous devez configurer la redistribution des routes pour disposer du partage de route entre protocoles. Vous pouvez configurer la redistribution des routes pour une passerelle Edge NSX Data Center for vSphere.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Routage > Redistribution des routes**.

3 Utilisez les boutons bascule de protocole pour activer les protocoles dont vous souhaitez activer la redistribution des routes.

4 Ajoutez les préfixes IP à la table à l'écran.

   a Cliquez sur le bouton **Ajouter** (+).

   b Tapez un nom et l'adresse IP du réseau au format CIDR.

   c Cliquez sur **Conserver**.

5 Spécifier les critères de redistribution pour chaque préfixe IP en cliquant sur le bouton **Ajouter** ( ), en spécifiant les critères dans la boîte de dialogue, puis en cliquant sur **Conserver**.

Les entrées de la table sont traitées dans l'ordre. Utilisez les flèches vers le haut et vers le bas pour modifier l'ordre.

Option	Description
Nom du préfixe	Sélectionnez un préfixe d'adresse IP spécifique pour appliquer ces critères ou sélectionnez **Tout** pour appliquer les critères à tous les itinéraires réseau.
Protocole d'apprenant	Sélectionnez le protocole devant apprendre des routes à partir d'autres protocoles sous ces critères de redistribution.
Autoriser l'apprentissage à partir de	Sélectionnez les types de réseaux à partir desquels des routes peuvent être apprises pour le protocole sélectionné dans la liste **Protocole d'apprenant**.
Action	Indiquez si vous voulez autoriser ou interdire la redistribution à partir des types de réseaux sélectionnés.

6 Cliquez sur **Enregistrer les modifications**.

Équilibrage de charge

L'équilibrage de charge répartit les demandes de services entrantes entre plusieurs serveurs de façon à ce que la répartition de charge soit transparente pour les utilisateurs. L'équilibrage de charge favorise une utilisation optimale des ressources, une optimisation du débit, une réduction des temps de réponse, et permet d'éviter la surcharge.

L'équilibrage de charge NSX prend en charge deux moteurs d'équilibrage de charge. L'équilibrage de charge de couche 4 est basé sur des paquets et fournit un traitement de chemin d'accès rapide. L'équilibrage de charge de couche 7 est basé sur des sockets et prend en charge des stratégies de gestion de trafic avancées et l'atténuation DDOS pour les services principaux.

L'équilibrage de charge pour une passerelle Edge NSX Data Center for vSphere est configuré sur l'interface externe, car la charge de la passerelle Edge équilibre le trafic entrant en provenance du réseau externe. Lorsque vous configurez des serveurs virtuels pour l'équilibrage de charge, spécifiez l'une des adresses IP disponibles dont vous disposez dans votre VDC d'organisation.

Stratégies et concepts relatifs à l'équilibrage de charge

Une stratégie d'équilibrage de charge basée sur les paquets est implémentée sur la couche TCP et UDP. L'équilibrage de charge basé sur les paquets n'arrête pas la connexion et ne conserve pas la demande en mémoire tampon. Au lieu de cela, il envoie directement le paquet au serveur sélectionné après l'avoir traité. Les sessions TCP et UDP sont conservées dans l'équilibrage de charge afin que les paquets pour une seule session soient dirigés vers le même serveur. Vous pouvez sélectionner Accélération activée dans la configuration globale et la configuration du serveur virtuel pertinente pour activer l'équilibrage de charge basé sur les paquets.

Une stratégie d'équilibrage de charge basée sur des sockets est implémentée au-dessus de l'interface de socket. Deux connexions sont établies pour une demande unique, une connexion exposée au client et une connexion exposée au serveur. La connexion exposée au serveur est établie après la sélection du serveur. Pour l'implémentation basée sur des sockets HTTP, toute la demande est reçue avant l'envoi au serveur sélectionné avec la manipulation L7 facultative. Pour l'implémentation basée sur des sockets HTTPS, les informations d'authentification sont échangées sur la connexion exposée au client ou la connexion exposée au serveur. L'équilibrage de charge basé sur des sockets est le mode par défaut pour les serveurs virtuels TCP, HTTP et HTTPS.

Les concepts clés de l'équilibrage de charge NSX sont serveur virtuel, pool de serveurs, membre de pool de serveurs et moniteur de services.

Serveur virtuel

Résumé d'un service d'application, représenté par une combinaison unique d'adresse IP, de port, de protocole et de profil d'application tel que TCP ou UDP.

Pool de serveurs

Groupe de serveurs principaux.

Membre de pool de serveurs

Représente le serveur principal en tant que membre d'un pool.

Moniteur de services

Définit comment interroger l'état de santé d'un serveur principal.

Profil d'application

Représente la configuration TCP, UDP, de persistance et de certificat pour une application donnée.

Présentation de la configuration

Vous commencez par définir des options globales pour l'équilibrage de charge. Vous créez un pool de serveurs composé de serveurs membres principaux et associez un moniteur de services au pool pour gérer et partager les serveurs principaux de manière efficace.

Vous créez ensuite un profil d'application pour définir le comportement d'application commun dans un équilibrage de charge, tel que SSL client, SSL serveur, x-transféré-pour ou persistance. La persistance envoie les demandes suivantes avec des caractéristiques semblables de telle sorte qu'une adresse IP source ou un cookie doit être distribué au même membre de pool, sans exécuter l'algorithme d'équilibrage de charge. Le profil d'application peut être réutilisé entre serveurs virtuels.

Vous créez ensuite une règle d'application facultative pour configurer les paramètres spécifiques d'une application pour la manipulation du trafic, tels que la correspondance à une URL ou un nom d'hôte afin que différentes demandes puissent être gérées par différents pools. Ensuite, vous créez un moniteur de services propre à votre application ou vous pouvez utiliser un moniteur de services existant s'il répond à vos besoins.

Vous pouvez éventuellement créer une règle d'application pour prendre en charge les fonctionnalités avancées de serveurs virtuels de niveau 7. Certains cas d'utilisation de règles d'application incluent le changement de contenu, la manipulation d'en-tête, les règles de sécurité et la protection DOS.

Enfin, vous créez un serveur virtuel qui connecte votre pool de serveurs, le profil d'application et les règles d'application potentielles.

Lorsque le serveur virtuel reçoit une demande, l'algorithme d'équilibrage de charge tient compte de la configuration du membre du pool et de l'état d'exécution. L'algorithme calcule ensuite le pool approprié pour distribuer le trafic comprenant un ou plusieurs membres. La configuration d'un membre de pool inclut des paramètres tels que le poids, le nombre maximal de connexions et l'état de condition. L'état d'exécution inclut les connexions actuelles, le temps de réponse et des informations sur l'état du contrôle de santé. Les méthodes de calcul peuvent être round-robin, round-robin pondéré, least connection, hachage IP source, least connections pondérées, URL, URI ou en-tête HTTP.

Chaque pool est surveillé par le moniteur de services associé. Lorsque l'équilibrage de charge détecte un problème sur un membre du pool, ce membre est marqué comme étant hors service. Seul un serveur actif est sélectionné lors du choix d'un membre de pool à partir du pool de serveurs. Si le pool de serveurs n'est pas configuré avec un moniteur de services, tous les membres du pool sont considérés comme étant actifs.

Configuration du service d'équilibrage de charge

Les paramètres de configuration globale de l'équilibrage de charge comprennent l'activation générale, la sélection du moteur de niveau 4 ou 7 et la spécification des types d'événements à consigner.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Configuration globale**.

3 Sélectionnez les options que vous souhaitez activer :

Option	Action
État	Activez l'équilibrage de charge en cliquant sur l'icône Activer/Désactiver. Activez l'option **Accélération activée** pour configurer le service d'équilibrage de charge de sorte qu'il utilise le moteur L4, plus rapide, de préférence au moteur L7. L'adresse IP virtuelle TCP L4 est traitée avant le pare-feu de passerelle Edge. Par conséquent, aucune règle de pare-feu Autoriser n'est requise. **Note** Les adresses IP virtuelles L7 pour HTTP et HTTPS sont traitées après le pare-feu. Ainsi, l'accélération n'est pas activée, une règle de pare-feu de passerelle Edge doit exister afin d'autoriser l'accès à l'adresse IP virtuelle L7 pour ces protocoles. Lorsque l'accélération n'est pas activée et que le pool de serveurs est en mode non transparent, une règle SNAT est ajoutée. Vous devez donc vous assurer que le pare-feu est activé sur la passerelle Edge.
Activer la journalisation	Activez la journalisation afin que l'équilibrage de charge de la passerelle Edge collecte des journaux de trafic.
Niveau de consignation	Choisissez le niveau de gravité des événements à collecter dans les journaux.

4 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

Étape suivante

Configurez les profils d'application pour l'équilibrage de charge. Reportez-vous à Créer un profil d'application.

Créer un profil d'application

Un profil d'application définit le comportement de l'équilibrage de charge pour un type particulier de trafic réseau. Après avoir configuré un profil, vous devez l'associer à un serveur virtuel. Le serveur virtuel traite ensuite le trafic conformément aux valeurs spécifiées dans le profil. L'utilisation des profils améliore votre contrôle sur la gestion du trafic réseau et rend les tâches de gestion du trafic plus simples et plus efficaces.

Lorsque vous créez un profil pour le trafic HTTPS, les modèles de trafic HTTPS suivants sont autorisés :

- Client -> HTTPS -> Équilibrage de charge (désactive SSL) -> HTTP -> Serveurs
- Client -> HTTPS -> Équilibrage de charge (désactive SSL) -> HTTPS -> Serveurs
- Client -> HTTPS -> Équilibrage de charge (relais SSL) -> HTTPS -> Serveurs
- Client -> HTTP -> Équilibrage de charge -> HTTP -> Serveurs

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Profils d'application**.

3 Cliquez sur le bouton **Créer** ( ).

4 Entrez un nom pour le profil.

5 Configurez le profil d'application.

Option	Description
Type	Sélectionnez le type de protocole utilisé pour envoyer des demandes au serveur. La liste des paramètres requis dépend du protocole que vous sélectionnez. Il est impossible d'entrer des paramètres qui ne s'appliquent pas au protocole sélectionné. Tous les autres paramètres sont requis.
Activer le relais SSL	Cliquez ici pour que l'authentification SSL soit transmise au serveur virtuel. Dans le cas contraire, l'authentification SSL a lieu à l'adresse de destination.
URL de redirection HTTP	(HTTP et HTTPS) Entrez l'URL à laquelle le trafic qui arrive sur l'adresse de destination doit être redirigé.

Option	Description
Persistance	Spécifiez un mécanisme de persistance pour le profil. La persistance suit et enregistre les données de session, telles que le membre de pool spécifique qui a pris en charge une demande du client. Cela garantit que les demandes du client sont dirigées vers le même membre du pool tout au long de la durée de vie d'une session ou au cours des sessions ultérieures. Les options sont : ■ **IP source** La persistance IP source suit les sessions en fonction de l'adresse IP source. Lorsqu'un client demande la connexion à un serveur virtuel qui prend en charge la persistance d'affinité des adresses sources, l'équilibrage de charge vérifie si ce client s'est précédemment connecté et, si c'est le cas, renvoie le client vers le même membre de pool. ■ **MSRDP** (TCP uniquement) La persistance du protocole MSRDP (Microsoft Remote Desktop Protocol) maintient des sessions persistantes entre les clients et les serveurs Windows qui exécutent le service Microsoft RDP (Remote Desktop Protocol). Le scénario recommandé pour activer la persistance MSRDP consiste à créer un pool d'équilibrage de charge composé de membres exécutant un système d'exploitation Windows Server invité, dans lequel tous les membres appartiennent à un cluster Windows et participent à un annuaire de sessions Windows. ■ **ID de session SSL** La persistance de l'ID de session SSL est disponible lorsque vous activez le relais SSL. La persistance d'ID de session SSL garantit que les connexions de répétition à partir du même client sont envoyées au même serveur. La persistance de l'ID de session permet l'utilisation de la reprise de session SSL, ce qui permet d'économiser du temps de traitement pour le client et le serveur.
Nom du cookie	(HTTP et HTTPS) Si vous avez spécifié **Cookie** en tant que mécanisme de persistance, entrez le nom du cookie. La persistance des cookies permet d'utiliser un cookie pour identifier de façon unique la session lorsqu'un client accède au site pour la première fois. L'équilibrage de charge fait référence à ce cookie lorsqu'il connecte les demandes ultérieures pour cette session, de sorte qu'elles soient dirigées vers le même serveur virtuel.

Option	Description
Mode	Sélectionnez le mode suivant lequel le cookie doit être inséré. Les modes suivants sont pris en charge : ■ **Insérer** La passerelle Edge envoie un cookie. Lorsque le serveur envoie un ou plusieurs cookies, le client reçoit un cookie supplémentaire (les cookies du serveur et le cookie de la passerelle Edge). Lorsque le serveur n'envoie pas de cookie, le client reçoit uniquement le cookie de la passerelle Edge. ■ **Préfixe** Sélectionnez cette option lorsque votre client ne prend pas en charge plusieurs cookies. **Note** Tous les navigateurs acceptent plusieurs cookies. Mais vous pouvez avoir une application propriétaire utilisant un client propriétaire qui ne prend en charge qu'un seul cookie. Le serveur Web envoie ses cookies comme d'habitude. La passerelle Edge injecte (en tant que préfixe) ses informations de cookie dans la valeur de cookie du serveur. Ces informations de cookie supplémentaires sont supprimées lorsque la passerelle Edge les envoie au serveur. ■ **Session d'application** Pour cette option, le serveur n'envoie pas de cookie. Il envoie plutôt les informations de session d'utilisateur sous forme d'URL. Par exemple, `http://example.com/admin/UpdateUserServlet;jsessionid=OI24B9ASD7BSSD`, où `jsessionid` correspond aux informations de session utilisateur qui sont utilisées pour la persistance. Il n'est pas possible d'afficher le tableau de persistance de la session d'application pour le dépannage.
Expire dans (secondes)	Entrez une durée (en secondes) pendant laquelle la persistance reste en vigueur. Doit être un nombre entier positif compris entre 1 et 86 400. **Note** Pour l'équilibrage de charge de couche 7 utilisant la persistance d'IP source TCP, l'entrée de persistance expire si aucune nouvelle connexion TCP n'est établie pendant une période de temps, même si les connexions existantes sont toujours actives.
Insérer l'en-tête HTTP X-transféré-pour	(HTTP et HTTPS) Sélectionnez l'en-tête **Insérer l'en-tête HTTP X-transféré-pour** pour vous permettre d'identifier l'adresse IP initiale d'un client se connectant à un serveur Web via l'équilibrage de charge. **Note** L'utilisation de cet en-tête n'est pas prise en charge si vous avez activé le relais SSL.
Activer SSL du côté du pool	(HTTPS uniquement) Sélectionnez **Activer SSL du côté du pool** pour définir le certificat, les autorités de certification ou les listes de révocation de certificats (CRL) utilisés pour authentifier l'équilibrage de charge côté serveur dans l'onglet Certificats du pool.

6 (HTTPS uniquement) Configurez les certificats à utiliser avec le profil d'application. Si les certificats dont vous avez besoin n'existent pas, vous pouvez les créer à partir de l'onglet **Certificats**.

Option	Description
Certificats du serveur virtuel	Sélectionnez le certificat, les autorités de certification ou les listes de révocation de certificats (CRL) utilisés pour déchiffrer le trafic HTTPS.
Certificats du pool	Définissez le certificat, les autorités de certification ou les listes de révocation de certificats (CRL) utilisés pour authentifier l'équilibrage de charge côté serveur. **Note** Sélectionnez **Activer SSL du côté du pool** pour activer cet onglet.
Chiffrement	Sélectionnez les algorithmes de chiffrement (ou la suite de chiffrement) négociés pendant l'établissement de la liaison SSL/TLS.
Authentification client	Spécifiez si l'authentification client doit être ignorée ou requise. **Note** Lorsqu'elle est définie sur **Requise**, le client doit fournir un certificat après la demande ou l'établissement de la liaison est annulé.

7 Cliquez sur **Conserver** pour conserver vos modifications.

L'exécution de l'opération peut prendre quelques instants.

Étape suivante

Ajoutez un moniteur de services pour l'équilibrage de charge afin de définir les contrôles de santé pour différents types de trafic réseau. Reportez-vous à Créer un moniteur de services.

Créer un moniteur de services

Vous pouvez créer un moniteur de services pour définir les paramètres de contrôle de santé pour un type particulier de trafic réseau. Lorsque vous associez un moniteur de services à un pool, les membres du pool sont surveillés en fonction des paramètres du moniteur de services.

Procédure

1 Ouvrez les services de passerelle Edge.

a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Surveillance des services**.

3 Cliquez sur le bouton **Créer** (+).

4 Entrez un nom pour le moniteur de services.

5 (Facultatif) Configurez les options suivantes pour le moniteur de services :

Option	Description
Intervalle	Entrez l'intervalle auquel le serveur doit être surveillé à l'aide de la **Méthode** spécifiée.
Expiration	Entrez le délai maximal (en secondes) au terme duquel une réponse du serveur doit être reçue.
Nombre maximal de tentatives	Entrez le nombre de fois que la **Méthode** de surveillance spécifiée doit échouer de manière séquentielle avant que le serveur ne soit déclaré inactif.
Type	Sélectionnez la manière dont vous souhaitez envoyer la demande de contrôle d'intégrité au serveur : HTTP, HTTPS, TCP, ICMP ou UDP. En fonction du type sélectionné, les autres options de la boîte de dialogue **Nouveau moniteur de services** sont actives ou inactives.
Attendu	(HTTP et HTTPS) Entrez la chaîne attendue par le moniteur de sorte qu'elle corresponde à la ligne d'état de la réponse HTTP ou HTTPS (par exemple, HTTP/1.1).
Méthode	(HTTP et HTTPS) Sélectionnez la méthode à utiliser pour détecter l'état du serveur.
URL	(HTTP et HTTPS) Entrez l'URL à utiliser pour la demande d'état du serveur. **Note** Lorsque vous sélectionnez la méthode POST, vous devez spécifier une valeur pour le champ **Envoyer**.
Envoyer	(HTTP, HTTPS, UDP) Entrez les données à envoyer.
Recevoir	(HTTP, HTTPS et UDP) Entrez la chaîne qui doit correspondre au contenu de la réponse. **Note** Lorsque **Attendu** ne correspond pas, le moniteur ne tente pas de faire correspondre le contenu de **Recevoir** .

Extension	(TOUS) Entrez les paramètres avancés du moniteur en tant que paires clé=valeurs. Par exemple, avertissement=10 indique que si un serveur ne répond pas dans les 10 secondes, son état est défini comme un avertissement. Tous les éléments de l'extension doivent être séparés par un retour chariot. Par exemple :
	`<extension>delay=2`
	`critical=3`
	`escape</extension>`

6 Cliquez sur **Conserver** pour conserver vos modifications.

L'exécution de l'opération peut prendre quelques instants.

Exemple : Extensions prises en charge pour chaque protocole

Tableau 7-1. Extensions pour les protocoles HTTP/HTTPS

Extension du moniteur	Description
no-body	N'attend pas le corps du document et arrête la lecture après l'en-tête HTTP/HTTPS. **Note** Une méthode HTTP GET ou POST est toujours envoyée, pas une méthode HEAD.
max-age=*SECONDS*	Vous avertit lorsqu'un document est plus ancien que la valeur SECONDS. Le nombre peut être défini sous la forme 10m pour les minutes, 10h pour les heures ou 10d pour les jours.
content-type=*STRING*	Spécifie un type d'en-tête Content-Type dans les appels POST.
linespan	Permet à regex de couvrir de nouvelles lignes (doit précéder - r ou -R).
regex=*STRING* ou ereg=*STRING*	Recherche la chaîne STRING regex dans la page.
eregi=*STRING*	Recherche la chaîne STRING regex non sensible à la casse dans la page.
invert-regex	Renvoie CRITICAL lorsqu'un résultat est trouvé et OK lorsqu'il est introuvable.
proxy-authorization=*AUTH_PAIR*	Spécifie le couple identifiant:motdepasse sur les serveurs proxy avec authentification de base.
useragent=*STRING*	Envoie la chaîne dans l'en-tête HTTP en tant que `User Agent`.
header=*STRING*	Envoie toutes les autres balises dans l'en-tête HTTP. Utilisez cette extension plusieurs fois pour les en-têtes supplémentaires.
onredirect=ok|warning|critical|follow|sticky|stickyport	Indique comment gérer les pages redirigées. `sticky` fonctionne comme `follow` mais garde l'adresse IP spécifiée. `stickyport` garantit que le port reste le même.
pagesize=*INTEGER:INTEGER*	Spécifie les tailles de page minimales et maximales (en octets).
warning=DOUBLE	Spécifie le temps de réponse (en secondes) qui doit entraîner un état d'avertissement.
critical=DOUBLE	Spécifie le temps de réponse (en secondes) qui doit entraîner un état critique.

Tableau 7-2. Extensions du protocole HTTPS uniquement

Extension du moniteur	Description
sni	Active la prise en charge de l'extension de nom d'hôte SSL/TLS (SNI).
certificate=**INTEGER**	Spécifie le nombre minimal de jours pendant lesquels un certificat doit être valide. La valeur par défaut du port est 443. Lorsque cette option est utilisée, l'URL n'est pas vérifiée.
authorization=AUTH_PAIR	Spécifie le couple identifiant:motdepasse sur les sites avec authentification de base.

Tableau 7-3. Extensions du protocole TCP

Extension du moniteur	Description
escape	Autorise l'utilisation de `\n`, `\r`, `\t` ou `\` dans une chaîne send ou quit. Doit précéder une option send ou quit. Par défaut, rien n'est ajouté à send et `\r\n` est ajouté à la fin de quit.
all	Spécifie que toutes les chaînes attendues doivent se produire dans la réponse du serveur. Par défaut, `any` est utilisée.
quit=*STRING*	Envoie une chaîne vers le serveur afin de fermer proprement la connexion.
refuse=ok|warn|crit	Accepte les refus TCP avec des états `ok`, `warn` ou `criti`. Utilise l'état `crit` par défaut.
mismatch=ok|warn|crit	Accepte les non-concordances de chaînes attendues avec des états `ok`, `warn` ou `crit`. Utilise l'état `warn` par défaut.
jail	Masque la sortie à partir du socket TCP.
maxbytes=*INTEGER*	Ferme la connexion lorsqu'un nombre d'octets supérieur au nombre spécifié est reçu.
delay=*INTEGER*	Attend le nombre de secondes spécifié entre l'envoi de la chaîne et l'interrogation d'une réponse.
certificate=*INTEGER*[,*INTEGER*]	Spécifie le nombre minimal de jours pendant lesquels un certificat doit être valide. La première valeur est `#days` pour l'avertissement et la seconde valeur est critique (0 si non spécifiée).
ssl	Utilise le protocole SSL pour la connexion.
warning=DOUBLE	Spécifie le temps de réponse (en secondes) qui doit entraîner un état d'avertissement.
critical=DOUBLE	Spécifie le temps de réponse (en secondes) qui doit entraîner un état critique.

Étape suivante

Ajouter des pools de serveurs à votre équilibrage de charge. Reportez-vous à Ajouter un pool de serveurs pour l'équilibrage de charge.

Ajouter un pool de serveurs pour l'équilibrage de charge

Vous pouvez ajouter un pool de serveurs pour gérer et partager des serveurs principaux de façon flexible et efficace. Un pool gère les méthodes de distribution d'équilibrage de charge et dispose d'un moniteur de services qui lui est connecté pour les paramètres de contrôle de santé.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Pools**.

3 Cliquez sur le bouton **Créer** (+).

4 Saisissez le nom et la description (facultative) du pool d'équilibrage de charge.

5 Sélectionnez une méthode d'équilibrage du service dans le menu déroulant **Algorithme** :

Option	Description
ROUND-ROBIN	Chaque serveur est utilisé l'un après l'autre en fonction du poids qui lui est attribué. Il s'agit de l'algorithme le plus régulier et le plus juste lorsque le temps de traitement du serveur reste distribué équitablement.
IP-HASH	Sélectionne un serveur basé sur un hachage des adresses IP source et de destination de chaque paquet.
LEASTCONN	Distribue les demandes de client à plusieurs serveurs en fonction du nombre de connexions déjà ouvertes sur le serveur. Les nouvelles connexions sont envoyées au serveur ayant le moins de connexions ouvertes.
URI	La partie gauche de l'URI (avant le point d'interrogation) est hachée et divisée par le poids total des serveurs en cours d'exécution. Le résultat indique le serveur qui recevra la demande. Cela permet de toujours diriger un URI vers le même serveur tant que celui-ci n'est pas arrêté.

Option	Description
HTTPHEADER	Le nom de l'en-tête HTTP est recherché dans chaque demande HTTP. Le nom d'en-tête entre parenthèses n'est pas sensible à la casse, ce qui est semblable à la fonction ACL « hdr() ». Si l'en-tête est absent ou ne contient aucune valeur, l'algorithme round robin s'applique. Le paramètre d'algorithme HTTP HEADER dispose d'une option `headerName=<name>`. Par exemple, vous pouvez utiliser **`host`** comme paramètre d'algorithme HTTP HEADER.
URL	Le paramètre URL spécifié dans l'argument est recherché dans la chaîne de requête de chaque demande HTTP GET. Si le paramètre est suivi du signe égal (=) et d'une valeur, la valeur est hachée et divisée par le poids total des serveurs en cours d'exécution. Le résultat indique le serveur qui reçoit la demande. Ce processus est utilisé pour suivre les identifiants d'utilisateurs dans les demandes et s'assurer qu'un même ID d'utilisateur est toujours envoyé au même serveur tant qu'aucun serveur n'est activé ou arrêté. Si aucune valeur ou aucun paramètre n'est trouvé, un algorithme de répétition alternée s'applique. Le paramètre d'algorithme d'URL dispose d'une option `urlParam=<url>`.

6 Ajoutez des membres au pool.

a Cliquez sur le bouton **Ajouter** ( ).

b Entrez le nom du membre du pool.

c Entrez l'adresse IP du membre du pool.

d Entrez le port sur lequel le membre doit recevoir le trafic de l'équilibrage de charge.

e Entrez le port du moniteur sur lequel le membre doit recevoir des demandes du moniteur de santé.

f Dans la zone de texte **Poids**, tapez la proportion du trafic que ce membre doit gérer. Doit être un entier dans la plage 1-256.

g (Facultatif) Dans la zone de texte **Nombre maximal de connexions**, saisissez le nombre maximal de connexions simultanées que le membre peut gérer.

Lorsque le nombre de demandes entrantes dépasse le maximum, les demandes sont mises en file d'attente et l'équilibrage de charge attend qu'une connexion soit libérée.

h (Facultatif) Dans la zone de texte **Nombre minimal de connexions**, saisissez le nombre minimal de connexions simultanées qu'un membre doit toujours accepter.

i Cliquez sur **Conserver** pour ajouter le nouveau membre au pool.

L'exécution de l'opération peut prendre quelques instants.

7 (Facultatif) Pour rendre les adresses IP des clients visibles aux serveurs principaux, sélectionnez **Transparent**.

Si **Transparent** n'est pas sélectionné (valeur par défaut), les serveurs principaux voient l'adresse IP de la source du trafic comme adresse IP interne de l'équilibrage de charge.

Lorsque **Transparent** est sélectionné, l'adresse IP source est l'adresse IP réelle du client et la passerelle Edge doit être définie comme passerelle par défaut pour s'assurer que les paquets de retour passent par elle.

8 Cliquez sur **Conserver** pour conserver vos modifications.

L'exécution de l'opération peut prendre quelques instants.

Étape suivante

Ajoutez des serveurs virtuels à votre équilibrage de charge. Un serveur virtuel a une adresse IP publique et traite toutes les demandes entrantes des clients. Reportez-vous à Ajouter un serveur virtuel.

Ajouter une règle d'application

Vous pouvez écrire une règle d'application pour manipuler et gérer directement le trafic IP des applications.

Procédure

1 Ouvrez les services de passerelle Edge.

a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Règles d'application**.

3 Cliquez sur le bouton **Ajouter** (+).

4 Entrez le nom de la règle d'application.

5 Entrez le script de la règle d'application.

Pour plus d'informations sur la syntaxe des règles d'application, reportez-vous à la section http://cbonte.github.io/haproxy-dconv/configuration-1.5.html.

6 Cliquez sur **Conserver** pour conserver vos modifications.

L'exécution de l'opération peut prendre quelques instants.

Étape suivante

Associez la nouvelle règle d'application à un serveur virtuel ajouté pour l'équilibrage de charge. Reportez-vous à Ajouter un serveur virtuel.

Ajouter un serveur virtuel

Ajoutez une interface interne ou de liaison montante de passerelle Edge NSX Data Center for vSphere en tant que serveur virtuel. Un serveur virtuel a une adresse IP publique et traite toutes les demandes entrantes des clients.

Par défaut, l'équilibrage de charge ferme la connexion TCP du serveur après chaque demande de client.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **Équilibrage de charge** > **Serveurs virtuels**.

3 Cliquez sur le bouton **Ajouter** ( ).

4 Dans l'onglet **Général**, configurez les options suivantes pour le serveur virtuel :

Option	Description
Activer le serveur virtuel	Cliquez pour activer le serveur virtuel.
Activer l'accélération	Cliquez pour activer l'accélération.
Profil d'application	Sélectionnez le profil d'application à associer au serveur virtuel.
Nom	Saisissez un nom pour le serveur virtuel.
Description	Saisissez une description (facultative) pour le serveur virtuel.
Adresse IP	Saisissez ou recherchez et sélectionnez l'adresse IP sur laquelle l'équilibrage de charge écoute.
Protocole	Sélectionnez le protocole que le serveur virtuel accepte. Vous devez sélectionner le même protocole que celui utilisé par le **Profil d'application** sélectionné.
Port	Tapez le numéro du port sur lequel l'équilibrage de charge écoute.
Pool par défaut	Choisissez le pool de serveurs que l'équilibrage de charge utilise.
Limite de connexion	(Facultatif) Saisissez le nombre maximal de connexions simultanées que le serveur virtuel peut traiter.
Limite de vitesse de connexion (CPS)	(Facultatif) Saisissez le nombre maximal de demandes de nouvelles connexions entrantes par seconde.

5 (Facultatif) Pour associer des règles d'application avec le serveur virtuel, cliquez sur l'onglet **Avancé** et effectuez les étapes suivantes :

   a Cliquez sur le bouton **Ajouter** ( ).

   Les règles d'application créées pour l'équilibrage de charge s'affichent. Si nécessaire, ajoutez des règles d'application pour l'équilibrage de charge. Reportez-vous à Ajouter une règle d'application.

6 Cliquez sur **Conserver** pour conserver vos modifications.

   L'exécution de l'opération peut prendre quelques instants.

Étape suivante

Créez une règle de pare-feu de passerelle Edge pour autoriser le trafic vers le nouveau serveur virtuel (adresse IP de destination). Consultez Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere

Sécuriser l'accès à l'aide de réseaux privés virtuels

Vous pouvez configurer les fonctionnalités de VPN fournies par le logiciel NSX pour vos passerelles Edge NSX Data Center for vSphere. Vous pouvez configurer des connexions VPN au centre de données virtuel de votre organisation à l'aide d'un tunnel SSL VPN-Plus, d'un tunnel VPN IPsec ou d'un tunnel VPN L2.

Comme décrit dans le *Guide d'Administration NSX*, la passerelle NSX Edge prend en charge ces services VPN :

- SSL VPN-Plus, qui permet aux utilisateurs distants d'accéder aux applications d'entreprise privées.
- VPN IPsec, qui offre une connectivité de site à site entre une passerelle NSX Edge et des sites distants ayant également NSX, des routeurs matériels tiers ou des passerelles VPN.
- VPN L2, qui permet l'extension du centre de données virtuel de votre organisation en autorisant les machines virtuelles à conserver la connectivité réseau tout en conservant la même adresse IP entre les limites géographiques.

Dans un environnement vCloud Director, vous pouvez créer des tunnels VPN entre :

- Des réseaux de centre de données virtuel d'organisation sur la même organisation
- Des réseaux de centre de données virtuel d'organisation sur différentes organisations
- Un réseau de centre de données virtuel d'organisation et un réseau externe

Note vCloud Director ne prend pas en charge plusieurs tunnels VPN entre deux mêmes passerelles Edge. Si un tunnel existe entre deux passerelles Edge et que vous souhaitez ajouter un autre sous-réseau au tunnel, supprimez le tunnel VPN existant et créez-en un nouveau qui inclut le nouveau sous-réseau.

Après avoir configuré des tunnels VPN pour une passerelle Edge, vous pouvez utiliser un client VPN à partir d'un emplacement distant pour vous connecter au centre de données virtuel d'organisation soutenu par cette passerelle Edge.

Configurer VPN-Plus SSL

Les services VPN-Plus SSL d'une passerelle Edge NSX Data Center for vSphere dans un environnement vCloud Director permettent aux utilisateurs distants de se connecter en toute sécurité aux réseaux privés et aux applications des centres de données virtuels d'organisation reposant sur cette passerelle Edge. Vous pouvez configurer divers services VPN-Plus SSL sur la passerelle Edge.

Dans votre environnement vCloud Director, la fonctionnalité SSL VPN-Plus de la passerelle Edge prend en charge le mode d'accès réseau. Les utilisateurs distants doivent installer un client SSL pour établir des connexions sécurisées et accéder aux réseaux et applications situés derrière la passerelle Edge. Dans le cadre de la configuration de SSL VPN-Plus de la passerelle Edge, vous devez ajouter les modules d'installation du système d'exploitation et configurer certains paramètres. Consultez Ajouter un module d'installation de client SSL VPN-Plus pour plus d'informations.

La configuration de SSL VPN-Plus sur une passerelle Edge est un processus à plusieurs étapes.

Conditions préalables

Vérifiez que tous les certificats SSL nécessaires pour VPN-Plus SSL ont été ajoutés à l'écran **Certificats**. Reportez-vous à Gestion des certificats SSL.

Note Sur une passerelle Edge, le port 443 est le port par défaut pour HTTPS. Pour la fonctionnalité SSL VPN, le port HTTPS de la passerelle Edge doit être accessible depuis les réseaux externes. Le client SSL VPN impose que l'adresse IP et le port de la passerelle Edge qui sont configurés dans l'écran Paramètres du serveur dans l'onglet **VPN-Plus SSL** soient accessibles depuis le système client. Reportez-vous à Configurer les paramètres du serveur SSL VPN.

Procédure

1 Accès à l'écran SSL-VPN Plus

   Vous pouvez accéder à l'écran SSL-VPN Plus afin de commencer à configurer le service SSL-VPN Plus pour une passerelle Edge NSX Data Center for vSphere.

2 Configurer les paramètres du serveur SSL VPN

   Ces paramètres de serveur configurent le serveur SSL VPN, comme l'adresse IP et le port sur lequel le service écoute, la liste de chiffrements du service et son certificat de service. Lorsque vous vous connectez à la passerelle Edge NSX Data Center for vSphere, les utilisateurs distants spécifient la même adresse IP et le même port que vous définissez dans ces paramètres de serveur.

3 Créer un pool d'adresses IP utilisable avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

   Les utilisateurs distants obtiennent des adresses IP virtuelles à partir des pools d'adresses IP statiques que vous configurez à l'aide de l'écran **Pools d'adresses IP** dans l'onglet **VPN-Plus SSL**.

4 Ajouter un réseau privé pour une utilisation avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

   Utilisez l'écran Réseaux privés dans l'onglet **VPN-Plus SSL** pour configurer les réseaux privés. Les réseaux privés sont ceux auxquels vous souhaitez donner accès aux clients VPN lorsque les utilisateurs distants se connectent à l'aide de leurs clients VPN et du tunnel SSL VPN. Les réseaux privés activés seront installés dans la table de routage du client VPN.

5 Configurer un service d'authentification pour VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

   Utilisez l'écran **Authentification** dans l'onglet **VPN-Plus SSL** pour configurer un serveur d'authentification local pour le service VPN SSL de la passerelle Edge et éventuellement activer l'authentification du certificat client. Ce serveur d'authentification est utilisé pour authentifier les utilisateurs lors de leur connexion. Tous les utilisateurs configurés dans le serveur d'authentification local seront authentifiés.

6 Ajouter des utilisateurs SSL VPN-Plus au serveur d'authentification SSL VPN-Plus local

   Utilisez l'écran **Utilisateurs** dans l'onglet **VPN-Plus SSL** pour ajouter des comptes pour vos utilisateurs distants au serveur d'authentification local du service VPN SSL de la passerelle Edge NSX Data Center for vSphere.

7 Ajouter un module d'installation de client SSL VPN-Plus

   Utilisez l'écran Modules d'installation dans l'onglet **VPN-Plus SSL** pour créer des modules d'installation nommés de client VPN-Plus SSL pour les utilisateurs distants.

8 Modifier la configuration du client SSL VPN-Plus

   Utilisez l'écran **Configuration du client** dans l'onglet **VPN-Plus SSL** pour personnaliser la manière dont le tunnel du client VPN SSL répond lorsque l'utilisateur distant se connecte au VPN SSL.

9 Personnaliser les paramètres VPN-Plus SSL généraux pour une passerelle Edge NSX Data Center for vSphere

   Par défaut, le système définit des paramètres SSL VPN-Plus sur une passerelle Edge dans votre environnement vCloud Director. Vous pouvez utiliser l'écran **Paramètres généraux** de l'onglet **VPN-Plus SSL** du portail de locataires de vCloud Director pour personnaliser ces paramètres.

Accès à l'écran SSL-VPN Plus

Vous pouvez accéder à l'écran SSL-VPN Plus afin de commencer à configurer le service SSL-VPN Plus pour une passerelle Edge NSX Data Center for vSphere.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **VPN-Plus SSL**.

Étape suivante

Configurez les paramètres SSL VPN-Plus par défaut dans l'écran **Général**. Reportez-vous à Personnaliser les paramètres VPN-Plus SSL généraux pour une passerelle Edge NSX Data Center for vSphere.

Configurer les paramètres du serveur SSL VPN

Ces paramètres de serveur configurent le serveur SSL VPN, comme l'adresse IP et le port sur lequel le service écoute, la liste de chiffrements du service et son certificat de service. Lorsque vous vous connectez à la passerelle Edge NSX Data Center for vSphere, les utilisateurs distants spécifient la même adresse IP et le même port que vous définissez dans ces paramètres de serveur.

Si votre passerelle Edge est configurée avec plusieurs réseaux d'adresses IP en superposition sur son interface externe, l'adresse IP que vous sélectionnez pour le serveur SSL VPN peut être différente de celle de l'interface externe par défaut de la passerelle Edge.

Lors de la configuration des paramètres du serveur SSL VPN, vous devez choisir quels algorithmes de chiffrement utiliser pour le tunnel SSL VPN. Vous pouvez choisir un ou plusieurs chiffrements. Choisissez soigneusement les chiffrements selon les points forts et les faiblesses de vos sélections.

Par défaut, le système utilise le certificat autosigné généré par défaut par le système pour chaque passerelle Edge en tant que certificat d'identité de serveur par défaut pour le tunnel SSL VPN. Au lieu de cette valeur par défaut, vous pouvez choisir d'utiliser un certificat numérique que vous avez ajouté au système sur l'écran **Certificats**.

Conditions préalables

- Vérifiez que vous disposez de la configuration requise décrite dans la section Configurer VPN-Plus SSL.
- Si vous choisissez d'utiliser un certificat de service différent du certificat par défaut, importez le certificat requis dans le système. Reportez-vous à Ajouter un certificat de service à la passerelle Edge.
- Accès à l'écran SSL-VPN Plus.

Procédure

1 Dans l'écran **VPN-Plus SSL**, cliquez sur **Paramètres du serveur**.

2 Cliquez sur **Activé**.

3 Sélectionnez une adresse IP dans le menu déroulant.

4 (Facultatif) Entrez un numéro de port TCP.

Le numéro de port TCP est utilisé par le module d'installation du client SSL. Par défaut, le système utilise le port 443, qui est le port par défaut pour le trafic HTTPS/SSL. Même si le numéro de port est requis, vous pouvez définir n'importe quel port TCP pour les communications.

Note Le client SSL VPN impose que l'adresse IP et le port configurés ici soient accessibles depuis les systèmes clients des utilisateurs distants. Si vous modifiez le numéro de port par défaut, assurez-vous que la combinaison d'adresse IP et de port soit accessible à partir des systèmes des utilisateurs concernés.

5 Sélectionnez une méthode de chiffrement dans la liste de chiffrements.

6 Configurez la stratégie de journalisation Syslog du service.

La journalisation est activée par défaut. Vous pouvez modifier le niveau des messages à consigner ou désactiver la journalisation.

7 (Facultatif) Si vous souhaitez utiliser un certificat de service plutôt que le certificat autosigné généré par le système par défaut, cliquez sur **Modifier le certificat du serveur**, sélectionnez un certificat, puis cliquez sur **OK**.

8 Cliquez sur **Enregistrer les modifications**.

Étape suivante

Note Les utilisateurs distants doivent pouvoir accéder à l'adresse IP de la passerelle Edge et au numéro de port TCP que vous définissez. Ajoutez une règle de pare-feu de passerelle Edge qui autorise l'accès à l'adresse IP et au port SSL VPN-Plus configurés dans cette procédure. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Ajoutez un pool d'adresses IP afin que les utilisateurs distants obtiennent des adresses IP lorsqu'ils se connectent à l'aide de SSL VPN-Plus. Reportez-vous à Créer un pool d'adresses IP utilisable avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.

Créer un pool d'adresses IP utilisable avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

Les utilisateurs distants obtiennent des adresses IP virtuelles à partir des pools d'adresses IP statiques que vous configurez à l'aide de l'écran **Pools d'adresses IP** dans l'onglet **VPN-Plus SSL**.

Chaque pool d'adresses IP ajouté dans cet écran entraîne la configuration d'un sous-réseau d'adresses IP sur la passerelle Edge. Les plages d'adresses IP utilisées dans ces pools d'adresses IP doivent être différentes de tous les autres réseaux configurés sur la passerelle Edge.

Note Le SSL VPN attribue des adresses IP aux utilisateurs distants à partir des pools d'adresses IP selon l'ordre dans lequel les pools d'adresses IP apparaissent dans le tableau à l'écran. Une fois les pools d'adresses IP ajoutés au tableau à l'écran, vous pouvez ajuster leurs positions dans le tableau à l'aide des flèches vers le haut et vers le bas.

Conditions préalables

- Accès à l'écran SSL-VPN Plus.
- Configurer les paramètres du serveur SSL VPN.

Procédure

1 Dans l'onglet **VPN-Plus SSL**, cliquez sur **Pools d'adresses IP**.

2 Cliquez sur le bouton **Créer** ( ).

3 Configurez les paramètres du pool d'adresses IP.

Option	Action
Plage d'adresses IP	Entrez une plage d'adresses IP pour ce pool d'adresses IP, par exemple `127.0.0.1–127.0.0.9`. Ces adresses IP seront attribuées à des clients VPN lorsqu'ils s'authentifient et se connectent au tunnel SSL VPN.
Masque réseau	Entrez le masque de réseau du pool d'adresses IP, par exemple `255.255.255.0`.
Passerelle	Entrez l'adresse IP que vous souhaitez que la passerelle Edge crée et attribue en tant qu'adresse de passerelle pour ce pool d'adresses IP. Lorsque le pool d'adresses IP est créé, un adaptateur virtuel est créé sur la machine virtuelle de la passerelle Edge et cette adresse IP est configurée sur cette interface virtuelle. Cette adresse IP peut être n'importe quelle adresse IP dans le sous-réseau qui ne figure pas également dans la plage indiquée dans le champ **Plage IP**.
Description	(Facultatif) Entrez une description pour ce pool d'adresses IP.
État	Choisissez d'activer ou de désactiver le pool d'adresses IP.
DNS primaire	(Facultatif) Entrez le nom du serveur DNS principal qui sera utilisé pour la résolution de noms pour ces adresses IP virtuelles.
DNS secondaire	(Facultatif) Entrez le nom du serveur DNS secondaire à utiliser.
Suffixe DNS	(Facultatif) Entrez le suffixe DNS du domaine sur lequel les systèmes clients sont hébergés, pour la résolution de noms d'hôtes basée sur un domaine.
Serveur WINS	(Facultatif) Entrez l'adresse du serveur WINS en fonction des besoins de votre organisation.

4 Cliquez sur **Conserver**.

Résultats

La configuration du pool d'adresses IP est ajoutée au tableau à l'écran.

Étape suivante

Ajoutez les réseaux privés que vous souhaitez rendre accessibles à vos utilisateurs distants se connectant avec SSL VPN-Plus. Reportez-vous à Ajouter un réseau privé pour une utilisation avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.

Ajouter un réseau privé pour une utilisation avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

Utilisez l'écran Réseaux privés dans l'onglet **VPN-Plus SSL** pour configurer les réseaux privés. Les réseaux privés sont ceux auxquels vous souhaitez donner accès aux clients VPN lorsque les utilisateurs distants se connectent à l'aide de leurs clients VPN et du tunnel SSL VPN. Les réseaux privés activés seront installés dans la table de routage du client VPN.

Les réseaux privés correspondent à la liste de tous les réseaux IP accessibles derrière la passerelle Edge dont vous souhaitez chiffrer le trafic pour un client VPN ou que vous souhaitez exclure du chiffrage. Chaque réseau privé qui nécessite un accès via un tunnel SSL VPN doit être ajouté en tant qu'entrée distincte. Vous pouvez utiliser des techniques de synthèse de route pour limiter le nombre d'entrées.

- SSL VPN-Plus permet aux utilisateurs distants d'accéder aux réseaux privés selon l'ordre de haut en bas dans lequel les pools d'adresses IP figurent dans le tableau à l'écran. Une fois les réseaux privés ajoutés au tableau à l'écran, vous pouvez ajuster leurs positions dans le tableau en utilisant les flèches vers le haut et vers le bas.
- Si vous choisissez d'activer l'optimisation TCP pour un réseau privé, certaines applications telles que le FTP en mode actif risquent de ne pas fonctionner dans ce sous-réseau. Pour ajouter un serveur FTP configuré en mode actif, vous devez ajouter un autre réseau privé pour ce serveur FTP et désactiver l'optimisation TCP pour ce réseau privé. En outre, le réseau privé pour ce serveur FTP doit être activé et figurer dans le tableau à l'écran au-dessus du réseau privé optimisé pour TCP.

Conditions préalables

- Accès à l'écran SSL-VPN Plus.
- Créer un pool d'adresses IP utilisable avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.

Procédure

1 Dans l'onglet **VPN-Plus SSL**, cliquez sur **Réseaux privés**.

2 Cliquez sur le bouton **Ajouter** ( ).

3 Configurez les paramètres du réseau privé.

Option	Action
Réseau	Tapez l'adresse IP du réseau privé au format CIDR, par exemple **192.169.1.0/24**.
Description	(Facultatif) Tapez une description du réseau.
Envoyer le trafic	Spécifiez comment le client VPN doit envoyer le trafic sur le réseau privé et sur Internet. ■ **Par tunnel** Le client VPN envoie le trafic sur le réseau privé et sur Internet par le biais de la passerelle Edge compatible avec le SSL VPN-Plus. ■ **Contourner le tunnel** Le client VPN contourne la passerelle Edge et envoie le trafic directement au serveur privé.
Activer l'optimisation TCP	(Facultatif) Pour optimiser encore plus la vitesse sur Internet, lorsque vous sélectionnez l'option **Par tunnel** pour envoyer le trafic, vous devez également sélectionner **Activer l'optimisation TCP**. La sélection de cette option améliore les performances des paquets TCP dans le tunnel VPN, mais n'améliore pas les performances du trafic UDP. Le tunnel des SSL VPN à accès complet traditionnels envoie les données TCP/IP dans une seconde pile TCP/IP pour le chiffrement sur Internet. Cette méthode conventionnelle encapsule les données de la couche d'application dans deux flux TCP distincts. Lors d'une perte de paquets, laquelle peut survenir même dans des conditions optimales de connexion à Internet, un effet de dégradation des performances appelé effondrement TCP sur TCP se produit. Lors d'un effondrement TCP sur TCP, deux instruments TCP corrigent le même paquet de données IP, altérant le débit du réseau et entraînant des expirations de délai de connexion. La sélection de l'option **Activer l'optimisation TCP** élimine le risque de ce problème TCP sur TCP. **Note** Lorsque vous activez l'optimisation TCP : ■ Vous devez entrer les numéros de ports pour lesquels vous souhaitez optimiser le trafic Internet. ■ Le serveur SSL VPN ouvre la connexion TCP pour le compte du client VPN. Lorsque la connexion TCP est ouverte par le serveur SSL VPN, la première règle de pare-feu Edge automatiquement générée est appliquée, ce qui permet le passage de toutes les connexions ouvertes à partir de la passerelle Edge. Le trafic qui n'est pas optimisé est évalué par les règles de pare-feu Edge régulières. La règle TCP générée par défaut est d'autoriser toutes les connexions.
Ports	Lorsque vous sélectionnez l'option **Par tunnel**, saisissez une plage de numéros de ports que vous souhaitez ouvrir pour permettre à l'utilisateur distant d'accéder aux serveurs internes, par exemple **20–21** pour le trafic FTP et **80–81** pour le trafic HTTP. Pour fournir un accès non restreint aux utilisateurs, laissez ce champ vide.
État	Activez ou désactivez le réseau privé.

4 Cliquez sur **Conserver**.

5 Cliquez sur **Enregistrer les modifications** pour enregistrer la configuration dans le système.

Étape suivante

Ajoutez un serveur d'authentification. Reportez-vous à Configurer un service d'authentification pour VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.

Important Ajoutez les règles de pare-feu correspondantes pour autoriser le trafic réseau vers les réseaux privés que vous avez ajoutés dans cet écran. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX Data Center for vSphere.

Configurer un service d'authentification pour VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere

Utilisez l'écran **Authentification** dans l'onglet **VPN-Plus SSL** pour configurer un serveur d'authentification local pour le service VPN SSL de la passerelle Edge et éventuellement activer l'authentification du certificat client. Ce serveur d'authentification est utilisé pour authentifier les utilisateurs lors de leur connexion. Tous les utilisateurs configurés dans le serveur d'authentification local seront authentifiés.

Un seul serveur d'authentification VPN-Plus SSL local peut être configuré sur la passerelle Edge. Si vous cliquez sur **+ LOCAL** et spécifiez des serveurs d'authentification supplémentaires, un message d'erreur s'affiche lorsque vous tentez d'enregistrer la configuration.

Le délai maximal pour s'authentifier via SSL VPN est de 3 minutes. Cette valeur maximale est déterminée par le délai d'expiration de non-authentification, qui est de 3 minutes par défaut et n'est pas configurable. Par conséquent, si vous avez plusieurs serveurs d'authentification dans l'autorisation en chaîne et que l'authentification de l'utilisateur met plus de 3 minutes, l'utilisateur n'est pas authentifié.

Conditions préalables

- Accès à l'écran SSL-VPN Plus.
- Ajouter un réseau privé pour une utilisation avec VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.
- Si vous prévoyez d'activer l'authentification du certificat client, vérifiez qu'un certificat d'autorité de certification a été ajouté à la passerelle Edge. Reportez-vous à Ajouter un certificat d'autorité de certification à la passerelle Edge pour la vérification de l'approbation des certificats SSL.

Procédure

1 Cliquez sur l'onglet **SSL VPN-Plus**, puis sur **Authentification**.

2 Cliquez sur **Local**.

3 Configurez les paramètres du serveur d'authentification.

a (Facultatif) Activez et configurez la stratégie de mot de passe.

Option	Description
Activer la stratégie de mot de passe	Activez l'application des paramètres de stratégie de mot de passe que vous configurez ici.
Longueur du mot de passe	Entrez la valeur minimale et la valeur maximale autorisées pour le nombre de caractères de la longueur du mot de passe.
Nb minimal de caractères alphabétiques	(Facultatif) Entrez le nombre minimal de caractères alphabétiques requis dans le mot de passe.
Nb minimal de chiffres	(Facultatif) Entrez le nombre minimal de caractères numériques requis dans le mot de passe.
Nb minimal de caractères spéciaux	(Facultatif) Entrez le nombre minimal de caractères spéciaux, tels que l'esperluette (&), le mot-dièse (#), le symbole de pourcentage (%), et ainsi de suite, qui sont requis dans le mot de passe.
Le mot de passe ne doit pas contenir l'identifiant utilisateur	(Facultatif) Activez l'option imposant que le mot de passe ne puisse pas contenir l'ID d'utilisateur.
Le mot de passe expire dans	(Facultatif) Tapez le nombre maximal de jours d'existence d'un mot de passe au terme duquel l'utilisateur doit le changer.
Notification d'expiration dans	(Facultatif) Tapez le nombre de jours précédant l'échéance **Le mot de passe expire dans** où l'utilisateur est informé que le mot de passe est sur le point d'expirer.

b (Facultatif) Activez et configurez la stratégie de verrouillage de compte.

Option	Description
Activer la stratégie de verrouillage du compte	Activez l'application des paramètres de stratégie de verrouillage de compte que vous configurez ici.
Nombre de tentatives	Entrez le nombre de tentatives d'accès au compte autorisé pour l'utilisateur.
Durée de la tentative	Entrez la période, en minutes, au terme de laquelle le compte de l'utilisateur est verrouillé lors de tentatives de connexion infructueuses. Par exemple, si vous spécifiez la valeur 5 pour **Nombre de tentatives** et 1 minute pour **Durée de nouvelle tentative**, le compte de l'utilisateur distant est verrouillé après 5 tentatives infructueuses de connexion en 1 minute.
Durée de verrouillage	Entrez la période pendant laquelle le compte de l'utilisateur reste verrouillé. Passé ce délai, le compte est automatiquement déverrouillé.

c Dans la section État, activez ce serveur d'authentification.

d (Facultatif) Configurez l'authentification secondaire.

Options	Description
Utiliser ce serveur pour l'authentification secondaire	(Facultatif) Spécifiez si vous voulez utiliser le serveur comme second niveau d'authentification.
Mettre fin à la session en cas d'échec de l'authentification	(Facultatif) Spécifiez si vous voulez mettre fin à la session VPN lorsque l'authentification échoue.

e Cliquez sur **Conserver**.

4 (Facultatif) Pour activer l'authentification par certification de client, cliquez sur **Modifier le certificat**, puis activez le bouton bascule d'activation, sélectionnez le certificat d'autorité de certification à utiliser et cliquez sur **OK**.

Étape suivante

Ajoutez des utilisateurs locaux au serveur d'authentification local afin qu'ils puissent se connecter avec SSL VPN-Plus. Reportez-vous à Ajouter des utilisateurs SSL VPN-Plus au serveur d'authentification SSL VPN-Plus local.

Créez un module d'installation contenant le client SSL afin que les utilisateurs distants puissent l'installer sur leurs systèmes locaux. Reportez-vous à Ajouter un module d'installation de client SSL VPN-Plus.

Ajouter des utilisateurs SSL VPN-Plus au serveur d'authentification SSL VPN-Plus local

Utilisez l'écran **Utilisateurs** dans l'onglet **VPN-Plus SSL** pour ajouter des comptes pour vos utilisateurs distants au serveur d'authentification local du service VPN SSL de la passerelle Edge NSX Data Center for vSphere.

Note Si un serveur d'authentification local n'est pas déjà configuré, l'ajout d'un utilisateur sur l'écran **Utilisateurs** ajoute automatiquement un serveur d'authentification local avec les valeurs par défaut. Vous pouvez ensuite utiliser le bouton Modifier dans l'écran **Authentification** pour afficher et modifier les valeurs par défaut. Pour plus d'informations sur l'utilisation de l'écran **Authentification**, reportez-vous à la section Configurer un service d'authentification pour VPN-Plus SSL sur une passerelle Edge NSX Data Center for vSphere.

Conditions préalables

Accès à l'écran SSL-VPN Plus.

Procédure

1 Dans l'onglet **VPN-Plus SSL**, cliquez sur **Utilisateurs**.

2 Cliquez sur le bouton **Créer** (+).

3 Configurez les options suivantes pour l'utilisateur.

Option	Description
ID utilisateur	Entrez l'ID d'utilisateur.
Mot de passe	Entrez un mot de passe pour l'utilisateur.
Confirmer le mot de passe	Entrez à nouveau le mot de passe.
Prénom	(Facultatif) Entrez le prénom de l'utilisateur.
Nom	(Facultatif) Entrez le nom de l'utilisateur.
Description	(Facultatif) Entrez une description pour l'utilisateur.
Activé	Spécifiez si l'utilisateur est activé ou désactivé.
Le mot de passe n'expire jamais	(Facultatif) Spécifiez si vous voulez conserver indéfiniment le même mot de passe pour cet utilisateur.
Autoriser la modification du mot de passe	(Facultatif) Spécifiez si vous souhaitez laisser l'utilisateur modifier le mot de passe.
Modifier le mot de passe à la prochaine connexion	(Facultatif) Indiquez si vous voulez que cet utilisateur modifie le mot de passe la prochaine fois qu'il ouvre une session.

4 Cliquez sur **Conserver**.

5 Répétez les étapes pour ajouter d'autres utilisateurs.

Étape suivante

Ajoutez des utilisateurs locaux au serveur d'authentification local afin qu'ils puissent se connecter avec SSL VPN-Plus. Reportez-vous à Ajouter des utilisateurs SSL VPN-Plus au serveur d'authentification SSL VPN-Plus local.

Créez un module d'installation contenant le client SSL afin que les utilisateurs distants puissent l'installer sur leurs systèmes locaux. Reportez-vous à Ajouter un module d'installation de client SSL VPN-Plus.

Ajouter un module d'installation de client SSL VPN-Plus

Utilisez l'écran Modules d'installation dans l'onglet **VPN-Plus SSL** pour créer des modules d'installation nommés de client VPN-Plus SSL pour les utilisateurs distants.

Vous pouvez ajouter un module d'installation de client VPN-Plus SSL à la passerelle Edge NSX Data Center for vSphere. Les nouveaux utilisateurs sont invités à télécharger et installer ce module lorsqu'ils se connectent pour utiliser la connexion VPN pour la première fois. Une fois ajoutés, ces modules d'installation client sont ensuite téléchargeables à partir du nom de domaine complet de l'interface publique de la passerelle Edge.

Vous pouvez créer des modules d'installation qui s'exécutent sur les systèmes d'exploitation Windows, Linux et Mac. Si vous avez besoin de paramètres d'installation différents selon le client SSL VPN, créez un module d'installation pour chaque configuration.

Conditions préalables

Accès à l'écran SSL-VPN Plus

Procédure

1 Dans l'onglet **SSL VPN-Plus** du portail de locataires, cliquez sur **Modules d'installation**.

2 Cliquez sur le bouton **Ajouter** ( ).

3 Configurez les paramètres du module d'installation.

Option	Description
Nom de profil	Entrez un nom de profil pour ce module d'installation. Ce nom permet à l'utilisateur distant d'identifier cette connexion SSL VPN dans la passerelle Edge.
Passerelle	Entrez l'adresse IP ou le nom de domaine complet de l'interface publique de la passerelle Edge. L'adresse IP ou le nom de domaine complet que vous entrez est lié(e) au client SSL VPN. Lorsque le client est installé sur le système local de l'utilisateur distant, cette adresse IP ou ce nom de domaine complet s'affiche sur ce client SSL VPN. Pour lier des interfaces de liaison montante de passerelle Edge supplémentaires à ce client SSL VPN, cliquez sur le bouton **Ajouter** ( ) pour ajouter des lignes et entrez les adresses IP ou les noms de domaine complets, ainsi que les ports dans leur interface.
Port	(Facultatif) Pour modifier la valeur de port affichée par défaut, double-cliquez sur celle-ci, puis entrez une nouvelle valeur.
Windows **Linux** **Mac**	Sélectionnez les systèmes d'exploitation pour lesquels vous souhaitez créer les modules d'installation.
Description	(Facultatif) Tapez une description pour l'utilisateur.
Activé	Spécifiez si ce module est activé ou désactivé.

4 Sélectionnez les paramètres d'installation pour Windows.

Option	Description
Démarrer le client lors de la connexion	Démarre le client SSL VPN lorsque l'utilisateur distant se connecte à son système local.
Autoriser la mémorisation du mot de passe	Permet au client de mémoriser le mot de passe de l'utilisateur.
Activer l'installation en mode silencieux	Masque les commandes d'installation aux utilisateurs distants.
Masquer l'adaptateur réseau du client SSL	Masque l'adaptateur SSL VPN-Plus VMware installé sur l'ordinateur de l'utilisateur distant, ainsi que le module d'installation du client SSL VPN.

Option	Description
Masquer l'icône de la barre d'état système du client	Masque l'icône de la barre d'état du SSL VPN qui indique si la connexion VPN est active ou non.
Créer une icône de bureau	Crée une icône sur le bureau de l'utilisateur pour appeler le client SSL.
Activer l'opération en mode silencieux	Masque la fenêtre qui indique que l'installation est terminée.
Validation du certificat de sécurité du serveur	Le client SSL VPN valide le certificat du serveur SSL VPN avant d'établir la connexion sécurisée.

5 Cliquez sur **Conserver**.

Étape suivante

Modifiez la configuration du client. Reportez-vous à Modifier la configuration du client SSL VPN-Plus.

Modifier la configuration du client SSL VPN-Plus

Utilisez l'écran **Configuration du client** dans l'onglet **VPN-Plus SSL** pour personnaliser la manière dont le tunnel du client VPN SSL répond lorsque l'utilisateur distant se connecte au VPN SSL.

Conditions préalables

Accès à l'écran SSL-VPN Plus

Procédure

1 Dans l'onglet **VPN-Plus SSL**, cliquez sur **Configuration du client**.

2 Sélectionnez le **Mode Tunnel**.

- En mode Tunnel fractionné, seul le trafic VPN passe à travers la passerelle Edge.
- En mode Tunnel complet, la passerelle Edge devient la passerelle par défaut de l'utilisateur distant et l'ensemble du trafic (VPN, local et Internet) passe par cette passerelle.

3 Si vous sélectionnez le mode Tunnel complet, entrez l'adresse IP pour la passerelle par défaut utilisée par les clients des utilisateurs distants et, éventuellement, sélectionnez s'il faut empêcher le trafic du sous-réseau local de passer par le tunnel VPN.

4 (Facultatif) Désactivez la reconnexion automatique.

Activer la reconnexion automatique est activée par défaut. Si la reconnexion automatique est activée, le client VPN SSL reconnecte automatiquement les utilisateurs lorsqu'ils sont déconnectés.

5 (Facultatif) Activez éventuellement la possibilité pour le client d'avertir les utilisateurs distants lorsqu'une mise à niveau du client est disponible.

Cette option est désactivée par défaut. Si vous activez cette option, les utilisateurs distants peuvent choisir d'installer la mise à niveau.

6 Cliquez sur **Enregistrer les modifications**.

Personnaliser les paramètres VPN-Plus SSL généraux pour une passerelle Edge NSX Data Center for vSphere

Par défaut, le système définit des paramètres SSL VPN-Plus sur une passerelle Edge dans votre environnement vCloud Director. Vous pouvez utiliser l'écran **Paramètres généraux** de l'onglet **VPN-Plus SSL** du portail de locataires de vCloud Director pour personnaliser ces paramètres.

Conditions préalables

Accès à l'écran SSL-VPN Plus.

Procédure

1 Dans l'onglet **VPN-Plus SSL**, cliquez sur **Paramètres généraux**.

2 Modifiez les paramètres généraux selon les besoins de votre organisation.

Option	Description
Empêcher les connexions multiples avec le même nom d'utilisateur	Activez cette option pour qu'un utilisateur distant ne puisse avoir qu'une seule session active sous un même nom d'utilisateur.
Compression	Activez cette option pour permettre une compression intelligente des données basée sur TCP et améliorer la vitesse de transmission des données.
Activer la journalisation	Activez cette option pour conserver un journal du trafic qui emprunte la passerelle SSL VPN. La journalisation est activée par défaut.
Forcer le clavier virtuel	Activez cette option pour obliger les utilisateurs distants à utiliser uniquement un clavier virtuel (à l'écran) pour entrer les informations de connexion.
Randomiser les touches du clavier virtuel	Activez cette option pour que le clavier virtuel utilise une disposition de touches aléatoire.
Délai d'inactivité de la session	Entrez le délai d'inactivité de la session en minutes. En l'absence d'activité dans une session d'utilisateur pendant la période spécifiée, le système déconnecte la session de l'utilisateur. La valeur système par défaut est de 10 minutes.
Notification utilisateur	Entrez le message à afficher après la connexion des utilisateurs distants.
Activer l'accès aux URL publiques	Activez cette option pour permettre aux utilisateurs distants d'accéder aux sites qui ne sont pas explicitement configurés par vous pour l'accès des utilisateurs distants.
Activer le délai d'expiration forcé	Activez cette option pour que le système déconnecte les utilisateurs distants après la période spécifiée dans le champ **Délai d'expiration forcé**.
Délai d'expiration forcé	Tapez le délai d'expiration en minutes. Ce champ s'affiche lorsque le bouton bascule **Activer le délai d'expiration forcé** est activé.

3 Cliquez sur **Enregistrer les modifications**.

Configurer la fonction VPN IPSec

Les passerelles Edge NSX Data Center for vSphere d'un environnement vCloud Director prennent en charge le protocole IPsec (Internet Protocol Security) site-à-site pour sécuriser les tunnels VPN entre des réseaux de centre de données virtuel d'organisation, ou entre un réseau de centre de données virtuel d'organisation et une adresse IP externe. Vous pouvez configurer le service VPN IPsec sur une passerelle Edge.

La configuration d'une connexion VPN IPsec depuis un réseau distant vers votre centre de données virtuel d'organisation est le scénario le plus courant. Le logiciel NSX fournit les capacités de VPN IPsec pour une passerelle Edge, notamment la prise en charge de l'authentification de certificat, le mode de clé prépartagée et le trafic IP monodiffusion entre lui-même et des routeurs VPN distants. Vous pouvez également configurer plusieurs sous-réseaux pour se connecter via des tunnels IPSec au réseau interne situé derrière une passerelle Edge. Lorsque vous configurez plusieurs sous-réseaux pour se connecter via des tunnels IPSec au réseau interne, les plages d'adresses de ces sous-réseaux et du réseau interne situé derrière la passerelle Edge ne doivent pas se chevaucher.

Note Si les adresses IP des homologues locaux et distants sur un tunnel IPSec se chevauchent, l'acheminement du trafic dans le tunnel peut ne pas être cohérent selon qu'il existe ou non des routes locales connectées et des routes raccordées automatiquement.

Les algorithmes VPN IPSec suivants sont pris en charge :

- AES (AES128-CBC)
- AES256 (AES256-CBC)
- Triple DES (3DES192-CBC)
- AES-GCM (AES128-GCM)
- DH-2 (groupe Diffie-Hellman 2)
- DH-5 (groupe Diffie-Hellman 5)
- DH-14 (groupe Diffie-Hellman 14)

Note Les protocoles de routage dynamique ne sont pas pris en charge avec VPN IPSec. Si vous configurez un tunnel VPN IPsec entre une passerelle Edge du centre de données virtuel d'organisation et une passerelle VPN physique sur un site distant, vous ne pouvez pas configurer le routage dynamique pour cette connexion. L'adresse IP du site distant ne peut pas être apprise par routage dynamique sur la liaison montante de passerelle Edge.

Comme décrit dans la section *Présentation de VPN IPSec* du *Guide d'administration de NSX*, le nombre maximal de tunnels pris en charge sur une passerelle Edge est déterminé par sa taille configurée : Compacte, Grande, Très grande, Quadruple.

Pour afficher la taille de votre configuration de passerelle Edge, accédez à la passerelle Edge et cliquez sur son nom.

La configuration de VPN IPSec sur une passerelle Edge est un processus à plusieurs étapes.

Note Si un pare-feu se trouve entre les points de terminaison du tunnel, après avoir configuré le service VPN IPSec, mettez à jour les règles du pare-feu pour autoriser les protocoles IP et les ports UDP suivants :

- Protocole IP, ID 50 (ESP)
- Protocole IP, ID 51 (AH)
- Port 500 UDP (IKE)
- Port 4500 UDP

Procédure

1 Accéder à l'écran VPN IPsec

Dans l'écran **VPN IPsec**, vous pouvez commencer à configurer le service VPN IPsec pour une passerelle Edge NSX Data Center for vSphere.

2 Configurer les connexions de site VPN IPSec pour la passerelle Edge NSX Data Center for vSphere

Utilisez l'écran **Sites VPN IPsec** dans le portail de locataires de vCloud Director pour configurer les paramètres nécessaires à la création d'une connexion VPN IPsec entre votre centre de données virtuel d'organisation et un autre site utilisant les capacités VPN IPsec de la passerelle Edge.

3 Activer le service VPN IPsec sur une passerelle Edge NSX Data Center for vSphere

Lorsqu'au moins une connexion VPN IPsec est configurée, vous pouvez activer le service VPN IPsec sur la passerelle Edge.

4 Spécifiez les paramètres VPN IPsec globaux

Utilisez l'écran **Configuration globale** pour configurer les paramètres d'authentification VPN IPsec au niveau d'une passerelle Edge. Sur cet écran, vous pouvez définir une clé prépartagée globale et activer l'authentification par certificat.

Accéder à l'écran VPN IPsec

Dans l'écran **VPN IPsec**, vous pouvez commencer à configurer le service VPN IPsec pour une passerelle Edge NSX Data Center for vSphere.

Procédure

1 Ouvrez les services de passerelle Edge.

a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **VPN > VPN IPsec**.

Étape suivante

Utilisez l'écran **Sites de VPN IPsec** pour configurer une connexion VPN IPsec. Une connexion au moins doit être configurée pour qu'il soit possible d'activer le service VPN IPsec sur la passerelle Edge. Reportez-vous à Configurer les connexions de site VPN IPSec pour la passerelle Edge NSX Data Center for vSphere.

Configurer les connexions de site VPN IPSec pour la passerelle Edge NSX Data Center for vSphere

Utilisez l'écran **Sites VPN IPsec** dans le portail de locataires de vCloud Director pour configurer les paramètres nécessaires à la création d'une connexion VPN IPsec entre votre centre de données virtuel d'organisation et un autre site utilisant les capacités VPN IPsec de la passerelle Edge.

Lorsque vous configurez une connexion VPN IPSec entre des sites, vous configurez la connexion du point de vue de votre emplacement actuel. La configuration de la connexion nécessite que vous compreniez les concepts dans le contexte de l'environnement vCloud Director afin de pouvoir configurer la connexion VPN correctement.

- Les sous-réseaux locaux et homologues spécifient les réseaux auxquels le VPN se connecte. Lorsque vous spécifiez ces sous-réseaux dans les configurations des sites VPN IPSec, entrez une plage réseau et non une adresse IP spécifique. Utilisez le format CIDR, par exemple `192.168.99.0/24`.
- L'ID de l'homologue est un identifiant unique du périphérique distant qui termine la connexion VPN, généralement son adresse IP publique. Pour les homologues qui utilisent l'authentification de certificat, cet ID doit être le nom unique défini dans le certificat homologue. Pour les homologues PSK, cet ID peut être une chaîne quelconque. Une meilleure pratique NSX consiste à utiliser l'adresse IP publique du périphérique distant ou le nom de domaine complet (FQDN) comme ID de l'homologue. Si l'adresse IP de l'homologue provient d'un autre réseau de centre de données virtuel d'organisation, saisissez l'adresse IP native de l'homologue. Si NAT est configuré pour l'homologue, vous devez entrer l'adresse IP privée de l'homologue.
- Le point de terminaison de l'homologue spécifie l'adresse IP publique du périphérique distant auquel vous vous connectez. Ce point de terminaison peut être une adresse différente de l'ID de l'homologue si la passerelle de l'homologue n'est pas directement accessible depuis Internet mais qu'elle se connecte par le biais d'un autre périphérique. Si NAT est configuré pour l'homologue, vous devez entrer l'adresse IP publique que les périphériques utilisent pour NAT.
- L'ID local spécifie l'adresse IP publique de la passerelle Edge du centre de données virtuel d'organisation. Vous pouvez entrer une adresse IP ou un nom d'hôte conjointement avec le pare-feu de la passerelle Edge.

- Le point de terminaison local spécifie le réseau de votre centre de données virtuel d'organisation sur lequel transmet la passerelle Edge. En général, le réseau externe de la passerelle Edge est le point de terminaison local.

Conditions préalables

- Accéder à l'écran VPN IPsec.
- Configurer la fonction VPN IPSec.
- Si vous prévoyez d'utiliser un certificat global comme méthode d'authentification, vérifiez que l'authentification de certificat est activée sur l'écran **Configuration globale**. Reportez-vous à Spécifiez les paramètres VPN IPsec globaux.

Procédure

1 Sous l'onglet **VPN IPsec**, cliquez sur **Sites VPN IPsec**.

2 Cliquez sur le bouton **Ajouter** ( ).

3 Configurez les paramètres de connexion VPN IPsec.

Option	Action
Activé	Activez cette connexion entre les deux points de terminaison VPN.
Activer PFS (Confidentialité de transmission parfaite)	Sélectionnez cette option pour que le système génère des clés publiques uniques pour toutes les sessions VPN IPSec initiées par vos utilisateurs. L'activation de PFS garantit que le système ne crée pas un lien entre la clé privée de la passerelle Edge et la clé de chaque session. La compromission d'une clé de session n'affecte pas les données autres que celles échangées lors de la session spécifique protégée par cette clé particulière. La compromission de la clé privée du serveur ne peut pas être utilisée pour déchiffrer les sessions archivées ou les futures sessions. Lorsque PFS est activé, les connexions VPN IPSec établies avec cette passerelle Edge rencontrent un léger surdébit de processeur. **Important** Les clés de session uniques ne doivent pas être utilisées pour dériver des clés supplémentaires. En outre, les deux côtés du tunnel VPN IPSec doivent prendre en charge PFS pour qu'il puisse fonctionner.
Nom	(Facultatif) Entrez un nom pour la connexion.
ID local	Entrez l'adresse IP externe de l'instance de passerelle Edge, qui correspond à l'adresse IP publique de la passerelle Edge. Cette adresse IP sera celle utilisée pour l'ID de l'homologue dans la configuration de VPN IPSec sur le site distant.
Point de terminaison local	Entrez le réseau qui est le point de terminaison local de la connexion. Le point de terminaison local spécifie le réseau de votre centre de données virtuel d'organisation sur lequel transmet la passerelle Edge. En général, le réseau externe est le point de terminaison local. Si vous ajoutez un tunnel IP vers IP à l'aide d'une clé prépartagée, l'ID local et l'adresse IP du point de terminaison local peuvent être identiques.

Option	Action
Sous-réseaux locaux	Entrez les réseaux à partager entre les sites et utilisez une virgule comme séparateur pour entrer plusieurs sous-réseaux. Entrez une plage réseau (pas une adresse IP spécifique) en saisissant l'adresse IP au format CIDR. Par exemple, **192.168.99.0/24**.
ID de l'homologue	Entrez un ID d'homologue pour identifier de manière unique le site homologue. L'ID de l'homologue est un identifiant unique du périphérique distant qui termine la connexion VPN, généralement son adresse IP publique. Pour les homologues qui utilisent l'authentification de certificat, l'ID doit correspondre au nom unique du certificat de l'homologue. Pour les homologues PSK, cet ID peut être une chaîne quelconque. Une meilleure pratique NSX consiste à utiliser l'adresse IP publique du périphérique distant ou le nom de domaine complet (FQDN) comme ID de l'homologue. Si l'adresse IP de l'homologue provient d'un autre réseau de centre de données virtuel d'organisation, saisissez l'adresse IP native de l'homologue. Si NAT est configuré pour l'homologue, vous devez entrer l'adresse IP privée de l'homologue.
Point final homologue	Entrez l'adresse IP ou le nom de domaine complet (FQDN) du site homologue, qui correspond à l'adresse publique du périphérique distant auquel vous vous connectez. **Note** Lorsque NAT est configuré pour l'homologue, entrez l'adresse IP publique que le périphérique utilise pour NAT.
Sous-réseaux homologues	Entrez le réseau distant auquel le VPN se connecte et utilisez une virgule comme séparateur pour entrer plusieurs sous-réseaux. Entrez une plage réseau (pas une adresse IP spécifique) en saisissant l'adresse IP au format CIDR. Par exemple, **192.168.99.0/24**.
Algorithme de chiffrement	Sélectionnez le type d'algorithme de chiffrement dans le menu déroulant. **Note** Le type de chiffrement que vous sélectionnez doit correspondre au type de chiffrement qui est configuré sur le périphérique VPN du site distant.
Authentification	Sélectionnez une authentification. Les options sont : ■ **PSK** L'option PSK (clé prépartagée) indique que la clé secrète partagée entre la passerelle Edge et le site homologue doit être utilisée pour l'authentification. ■ **Certificat** L'option Certificat indique que le certificat défini au niveau global doit être utilisé pour l'authentification. Cette option n'est pas disponible, sauf si vous avez configuré le certificat global sur l'écran **Configuration globale** de l'onglet **VPN IPSec**.
Modifier la clé partagée	(Facultatif) Lorsque vous mettez à jour les paramètres d'une connexion existante, vous pouvez activer cette option pour rendre le champ **Clé prépartagée** disponible et pouvoir ainsi mettre à jour la clé partagée.

Option	Action
Clé prépartagée	Si vous avez sélectionné le type d'authentification **PSK**, entrez une chaîne alphanumérique secrète qui peut être une chaîne d'une longueur maximale de 128 octets. **Note** La clé partagée doit correspondre à la clé qui est configurée sur le périphérique VPN du site distant. Une meilleure pratique consiste à configurer une clé partagée lorsque des sites anonymes se connectent au service VPN.
Afficher la clé partagée	(Facultatif) Sélectionnez cette option pour rendre la clé partagée visible à l'écran.
Groupe Diffie-Hellman	Sélectionnez le schéma cryptographique qui permettra au site homologue et à la passerelle Edge d'établir un secret partagé sur un canal de communication non sécurisé. **Note** Le Groupe Diffie-Hellman doit correspondre à ce qui est configuré sur le périphérique VPN du site distant.
Extension	(Facultatif) Tapez l'une des options suivantes : ■ `securelocaltrafficbyip=`*IPAddress* pour rediriger le trafic local de la passerelle Edge vers le tunnel VPN IPsec. Il s'agit de la valeur par défaut. ■ `passthroughSubnets=`*PeerSubnetIPAddress* pour prendre en charge les sous-réseaux se chevauchant.

4 Cliquez sur **Conserver**.

5 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

Étape suivante

Configurez la connexion du site distant. Vous devez configurer la connexion VPN IPsec sur les deux côtés de la connexion : votre centre de données virtuel d'organisation et le site homologue.

Activez le service VPN IPSec sur cette passerelle Edge. Lorsqu'au moins une connexion VPN IPSec est configurée, vous pouvez activer le service. Reportez-vous à Activer le service VPN IPsec sur une passerelle Edge NSX Data Center for vSphere.

Activer le service VPN IPsec sur une passerelle Edge NSX Data Center for vSphere

Lorsqu'au moins une connexion VPN IPsec est configurée, vous pouvez activer le service VPN IPsec sur la passerelle Edge.

Conditions préalables

- Accéder à l'écran VPN IPsec.
- Assurez-vous qu'au moins une connexion VPN IPsec est configurée pour cette passerelle Edge. Reportez-vous à la procédure décrite dans la section Configurer les connexions de site VPN IPSec pour la passerelle Edge NSX Data Center for vSphere.

Procédure

1 Dans l'onglet **VPN IPsec**, cliquez sur **État d'activation**.

2 Cliquez sur **État du service VPN IPsec** pour activer le service VPN IPsec.

3 Cliquez sur **Enregistrer les modifications**.

Résultats

Le service VPN IPsec de la passerelle Edge est activé.

Spécifiez les paramètres VPN IPsec globaux

Utilisez l'écran **Configuration globale** pour configurer les paramètres d'authentification VPN IPsec au niveau d'une passerelle Edge. Sur cet écran, vous pouvez définir une clé prépartagée globale et activer l'authentification par certificat.

Une clé prépartagée globale est utilisée pour les sites dont le point de terminaison homologue est défini sur **Tous**.

Conditions préalables

- Si vous prévoyez d'activer l'authentification de certificat, vérifiez que vous disposez d'au moins un certificat de service et des certificats signés par l'autorité de certification correspondants dans l'écran **Certificats**. Les certificats auto-signés ne peuvent pas être utilisés pour les VPN IPsec. Reportez-vous à Ajouter un certificat de service à la passerelle Edge.
- Accéder à l'écran VPN IPsec.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Dans l'onglet **VPN IPsec**, cliquez sur **Configuration globale**.

3 (Facultatif) Définir une clé prépartagée globale :

   a Activez l'option **Modifier la clé partagée**.

   b Entrez une clé prépartagée.

   La clé pré-partagée (PSK) globale est partagée par tous les sites dont le point de terminaison homologue est défini sur any. Si une clé pré-partagée globale est déjà définie, la modification de celle-ci pour lui donner une valeur vide avant de l'enregistrer n'a aucun effet sur la configuration existante.

c (Facultatif) Activez éventuellement **Afficher la clé partagée** pour rendre visible la clé pré-partagée.

d Cliquez sur **Enregistrer les modifications**.

4 Configurez l'authentification par certificat :

a Activez l'option **Activer l'authentification de certificat**.

b Sélectionnez les certificats de service, les certificats d'autorité de certification et les listes de révocation de certificats appropriés.

c Cliquez sur **Enregistrer les modifications**.

Étape suivante

Vous pouvez éventuellement activer la journalisation pour le service VPN IPsec de la passerelle Edge. Reportez-vous à Statistiques et journaux pour une passerelle Edge.

Configurer le VPN L2

Les passerelles Edge NSX Data Center for vSphere dans un environnement vCloud Director prennent en charge VPN L2. Un VPN L2 vous permet d'étendre le centre de données virtuel de votre organisation en autorisant les machines virtuelles à maintenir la connectivité réseau tout en conservant la même adresse IP entre les limites géographiques. Vous pouvez configurer le service VPN L2 sur une passerelle Edge.

NSX Data Center for vSphere fournit les fonctionnalités de VPN L2 d'une passerelle Edge. Le service VPN L2 vous permet de configurer un tunnel entre deux sites. Les machines virtuelles restent sur le même sous-réseau bien qu'elles soient déplacées entre ces sites, ce qui vous permet d'étendre votre centre de données virtuel d'organisation en étirant son réseau par le biais de VPN L2. Une passerelle Edge configurée sur un site peut fournir tous les services aux machines virtuelles de l'autre site.

Pour créer le tunnel VPN L2, vous devez configurer un serveur VPN L2 et un client VPN L2. Comme décrit dans le *Guide d'administration de NSX*, le serveur VPN L2 est la passerelle Edge de destination tandis que le client VPN L2 est la passerelle Edge source. Après avoir configuré les paramètres de VPN L2 sur chaque passerelle Edge, vous devez ensuite activer le service VPN L2 sur le serveur et le client.

Note Un réseau de centre de données virtuel d'organisation acheminé doit avoir été préalablement créé en tant que sous-interface sur les passerelles Edge.

Procédure

1 Accéder à l'écran VPN L2

Pour commencer à configurer le service VPN L2 pour une passerelle Edge NSX Data Center for vSphere, vous devez accéder à l'écran **VPN L2**.

2 Configurer la passerelle Edge NSX Data Center for vSphere en tant que serveur VPN L2

Le serveur VPN L2 est la passerelle NSX Edge de destination à laquelle le client VPN L2 va se connecter.

3 Configurer la passerelle Edge NSX Data Center for vSphere en tant que client VPN L2

Le client VPN L2 est le dispositif NSX Edge source qui établit la communication avec le dispositif NSX Edge de destination, c'est-à-dire le serveur VPN L2.

4 Activer le service VPN L2 sur une passerelle Edge NSX Data Center for vSphere

Lorsque les paramètres VPN L2 requis sont configurés, vous pouvez activer le service VPN L2 sur la passerelle Edge.

Accéder à l'écran VPN L2

Pour commencer à configurer le service VPN L2 pour une passerelle Edge NSX Data Center for vSphere, vous devez accéder à l'écran **VPN L2**.

Procédure

1 Ouvrez les services de passerelle Edge.

a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Accédez à **VPN > VPN L2**.

Étape suivante

Configurez le serveur VPN L2. Reportez-vous à Configurer la passerelle Edge NSX Data Center for vSphere en tant que serveur VPN L2.

Configurer la passerelle Edge NSX Data Center for vSphere en tant que serveur VPN L2

Le serveur VPN L2 est la passerelle NSX Edge de destination à laquelle le client VPN L2 va se connecter.

Comme décrit dans le *Guide d'administration de NSX*, vous pouvez connecter plusieurs sites homologues à ce serveur VPN L2.

Note La modification des paramètres de configuration de site entraîne la déconnexion de la passerelle Edge et la reconnexion de toutes les connexions existantes.

Conditions préalables

- Vérifiez que la passerelle Edge dispose d'un réseau de centre de données virtuel d'organisation acheminé qui est configuré en tant que sous-interface sur la passerelle Edge.
- Accéder à l'écran VPN L2.

- Si vous souhaitez lier un certificat du service à la connexion VPN L2, vérifiez que le certificat du serveur a déjà été téléchargé vers la passerelle Edge. Reportez-vous à Ajouter un certificat de service à la passerelle Edge.
- Vous devez disposer de l'adresse IP de l'écouteur, du port de l'écouteur, de l'algorithme de chiffrement du serveur et d'au moins un site homologue configuré avant de pouvoir activer le service VPN L2.

Procédure

1 Sous l'onglet **VPN L2**, sélectionnez **Serveur** pour le mode VPN L2.

2 Sous l'onglet **Serveur global**, configurez les détails de la configuration globale du serveur VPN L2.

Option	Action
Adresse IP de l'écouteur	Sélectionnez l'adresse IP principale ou secondaire d'une interface externe de la passerelle Edge.
Port de l'écouteur	Modifiez la valeur affichée selon les besoins de votre organisation. Le port par défaut du service VPN L2 est 443.
Algorithme de chiffrement	Sélectionnez l'algorithme de chiffrement utilisé pour les communications entre le serveur et le client.
Détails du certificat du service	Cliquez sur **Modifier le certificat du serveur** pour sélectionner le certificat à lier au serveur VPN L2. Dans la fenêtre **Modifier le certificat du serveur**, activez l'option **Valider le certificat du serveur**, sélectionnez un certificat de serveur dans la liste, puis cliquez sur **OK**.

3 Pour configurer les sites homologues, cliquez sur l'onglet **Sites de serveurs**.

4 Cliquez sur le bouton **Ajouter** ( ).

5 Configurez les paramètres pour un site homologue VPN L2.

Option	Action
Activé	Activez ce site homologue.
Nom	Entrez un nom unique pour le site homologue.
Description	(Facultatif) Tapez une description.
ID utilisateur **Mot de passe** **Confirmer le mot de passe**	Entrez le nom d'utilisateur et le mot de passe avec lesquels le site homologue doit être authentifié. Les informations d'identification de l'utilisateur sur le site homologue doivent être les mêmes que celles du côté client.

Option	Action
Interfaces étirées	Sélectionnez au moins une sous-interface à étirer avec le client. Les sous-interfaces disponibles pour sélection sont les réseaux de centre de données virtuel d'organisation qui sont configurés en tant que sous-interfaces sur la passerelle Edge.
Adresse de la passerelle d'optimisation de sortie	(Facultatif) Si la passerelle par défaut des machines virtuelles est identique sur les deux sites, entrez les adresses IP de passerelle des sous-interfaces pour lesquelles vous souhaitez que le trafic soit acheminé ou bloqué localement sur le tunnel VPN L2.

6 Cliquez sur **Conserver**.

7 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

Étape suivante

Activez le service VPN L2 sur cette passerelle Edge. Reportez-vous à Activer le service VPN L2 sur une passerelle Edge NSX Data Center for vSphere.

Configurer la passerelle Edge NSX Data Center for vSphere en tant que client VPN L2

Le client VPN L2 est le dispositif NSX Edge source qui établit la communication avec le dispositif NSX Edge de destination, c'est-à-dire le serveur VPN L2.

Conditions préalables

- Accéder à l'écran VPN L2.
- Si ce client VPN L2 se connecte à un serveur VPN L2 qui utilise un certificat de serveur, vérifiez que le certificat d'autorité de certification correspondant est téléchargé sur la passerelle Edge pour activer la validation du certificat de serveur pour ce client VPN L2. Reportez-vous à Ajouter un certificat d'autorité de certification à la passerelle Edge pour la vérification de l'approbation des certificats SSL.

Procédure

1 Sous l'onglet **VPN L2**, sélectionnez **Client** pour le mode VPN L2.

2 Sous l'onglet **Client global**, définissez les détails de configuration globale du client VPN L2.

Option	Description
Adresse du serveur	Entrez l'adresse IP du serveur VPN L2 auquel ce client doit être connecté.
Port du serveur	Entrez le port du serveur VPN L2 auquel le client doit se connecter. Le port par défaut est 443.
Algorithme de chiffrement	Sélectionnez l'algorithme de chiffrement pour la communication avec le serveur.

Option	Description
Interfaces étirées	Sélectionnez les sous-interfaces à étirer sur le serveur. Les sous-interfaces disponibles pour sélection sont les réseaux de centre de données virtuel d'organisation qui sont configurés en tant que sous-interfaces sur la passerelle Edge.
Adresse de la passerelle d'optimisation de sortie	(Facultatif) Si la passerelle par défaut pour les machines virtuelles est identique sur les deux sites, tapez les adresses IP de passerelle des sous-interfaces ou les adresses IP pour lesquelles le trafic ne doit pas circuler par le tunnel.
Détails de l'utilisateur	Entrez l'ID d'utilisateur et le mot de passe pour l'authentification auprès du serveur.

3 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

4 (Facultatif) Pour configurer les options avancées, cliquez sur l'onglet **Client avancé**.

5 Si ce dispositif Edge client VPN L2 ne dispose pas d'un accès direct à Internet et doit contacter le dispositif Edge serveur VPN L2 à l'aide d'un serveur proxy, spécifiez les paramètres du proxy.

Option	Description
Activer le proxy sécurisé	Choisissez d'activer le proxy sécurisé.
Adresse	Entrez l'adresse IP du serveur proxy.
Port	Entrez le numéro de port du serveur proxy.
Nom d'utilisateur **Mot de passe**	Entrez les informations d'authentification du serveur proxy.

6 Pour activer la validation de la certification du serveur, cliquez sur **Changer le certificat d'autorité de certification (CA)** et sélectionnez le certificat d'autorité de certification approprié.

7 Cliquez sur **Enregistrer les modifications**.

L'exécution de l'opération d'enregistrement peut prendre quelques minutes.

Étape suivante

Activez le service VPN L2 sur cette passerelle Edge. Reportez-vous à Activer le service VPN L2 sur une passerelle Edge NSX Data Center for vSphere.

Activer le service VPN L2 sur une passerelle Edge NSX Data Center for vSphere

Lorsque les paramètres VPN L2 requis sont configurés, vous pouvez activer le service VPN L2 sur la passerelle Edge.

Note Si la fonctionnalité HA est déjà configurée sur la passerelle Edge, assurez-vous que celle-ci comprend plusieurs interfaces internes configurées. Si une seule interface existe et qu'elle a déjà été utilisée par la fonctionnalité HA, la configuration de VPN L2 sur la même interface interne échoue.

Conditions préalables

- Si la passerelle Edge est un serveur VPN L2, sur le dispositif NSX Edge de destination, vérifiez que les paramètres du serveur VPN L2 requis et au moins un site homologue de VPN L2 sont configurés. Reportez-vous à la procédure décrite dans la section Configurer la passerelle Edge NSX Data Center for vSphere en tant que serveur VPN L2.
- Si la passerelle Edge est un client VPN L2, sur le dispositif NSX Edge source, vérifiez que les paramètres du client VPN L2 sont configurés. Reportez-vous à la procédure décrite dans la section Configurer la passerelle Edge NSX Data Center for vSphere en tant que client VPN L2.
- Accéder à l'écran VPN L2.

Procédure

1. Dans l'onglet **VPN L2**, cliquez sur le bouton **Activer**.
2. Cliquez sur **Enregistrer les modifications**.

Résultats

Le service VPN L2 de la passerelle Edge est désormais activé.

Étape suivante

Créez des règles NAT ou de pare-feu sur le côté du pare-feu exposé à Internet pour permettre au serveur VPN L2 de se connecter au client VPN L2.

Supprimer la configuration du service VPN L2 depuis une passerelle Edge NSX Data Center for vSphere

Vous pouvez supprimer la configuration de service VPN L2 existante de la passerelle Edge. Cette action désactive également le service VPN L2 sur la passerelle Edge.

Conditions préalables

Accéder à l'écran VPN L2

Procédure

1. Faites défiler l'écran VPN L2 vers le bas et cliquez sur **Supprimer la configuration**.
2. Pour confirmer la suppression, cliquez sur **OK**.

Résultats

Le service VPN L2 est désactivé et les détails de la configuration sont supprimés de la passerelle Edge.

Gestion des certificats SSL

Le logiciel NSX dans l'environnement vCloud Director permet d'utiliser des certificats SSL (Secure Sockets Layer) avec les tunnels VPN-Plus SSL et VPN IPsec que vous configurez pour vos passerelles Edge.

Les passerelles Edge de votre environnement vCloud Director prennent en charge les certificats auto-signés, les certificats signés par une autorité de certification et les certificats générés et signés par une autorité de certification. Vous pouvez générer des demandes de signature de certificat (CSR, Certificate Signing Request), importer les certificats, gérer les certificats importés et créer des listes de révocation de certificats (CRL, Certificate Revocation List).

À propos de l'utilisation de certificats avec le centre de données virtuel de votre organisation

Vous pouvez gérer les certificats pour les domaines de réseau suivants dans le centre de données virtuel de votre organisation vCloud Director.

- Tunnels VPN IPsec entre le réseau du centre de données virtuel d'une organisation et un réseau distant.
- Connexions SSL VPN-Plus entre les utilisateurs distants à des réseaux privés et ressources Web dans le centre de données virtuel de votre organisation.
- Tunnel VPN L2 entre deux passerelles Edge NSX.
- Serveurs virtuels et serveurs de pools configurés pour l'équilibrage de charge dans le centre de données virtuel de votre organisation

Utilisation des certificats clients

Vous pouvez créer un certificat client via une commande CAI ou un appel REST. Vous pouvez ensuite distribuer ce certificat à vos utilisateurs distants, qui peuvent installer le certificat sur leur navigateur Web.

L'avantage principal de l'implémentation de certificats clients réside dans le fait qu'un certificat client de référence pour chaque utilisateur distant peut être stocké et comparé au certificat client présenté par l'utilisateur distant. Afin d'empêcher un utilisateur particulier de se connecter à l'avenir, vous pouvez supprimer le certificat de référence de la liste des certificats clients du serveur de sécurité. La suppression du certificat prive cet utilisateur de toute connexion.

Générer une demande de signature de certificat pour une passerelle Edge

Pour pouvoir commander un certificat signé à une autorité de certification ou créer un certificat autosigné, vous devez générer une demande de signature de certificat (CSR) pour votre passerelle Edge.

Une demande de signature de certificat (CSR) est un fichier codé que vous devez générer sur une passerelle Edge NSX qui requiert un certificat SSL. L'utilisation d'une demande de signature de certificat (CSR) uniformise la façon dont les sociétés envoient leurs clés publiques, ainsi que les informations qui identifient leurs noms de sociétés et les noms de domaine.

Vous générez une demande de signature de certificat (CSR) avec un fichier de clé privée correspondant qui doit rester sur la passerelle Edge. La demande de signature de certificat (CSR) contient la clé publique correspondante et d'autres informations telles que le nom, l'emplacement et le nom du domaine de votre organisation.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **Certificats**.

3 Sous l'onglet **Certificats**, cliquez sur **Demande de signature de certificat (CSR)**.

4 Configurez les options suivantes pour la demande de signature de certificat :

Option	Description
Nom commun	Entrez le nom de domaine complet (FQDN) de l'organisation pour laquelle vous utiliserez le certificat. Par exemple, `www.example.com`. N'incluez pas le préfixe `http://` ni le préfixe `https://` dans votre nom commun.
Unité d'organisation	Utilisez ce champ pour différencier les divisions au sein de votre organisation vCloud Director auxquelles ce certificat est associé. Par exemple, Ingénierie ou Ventes.
Nom de l'organisation	Entrez le nom sous lequel votre entreprise est juridiquement enregistrée. L'organisation répertoriée doit être le détenteur légal du nom de domaine dans la demande de certificat.
Ville	Entrez la ville ou la localité où votre entreprise est juridiquement enregistrée.
Nom de l'état ou de la province	Entrez le nom complet (ne pas abréger) de l'état, de la province, de la région ou du territoire où votre entreprise est juridiquement enregistrée.
Code pays	Entrez le nom du pays dans lequel votre entreprise est juridiquement enregistrée.
Algorithme de clé privée	Tapez le type de clé, RSA ou DSA, pour le certificat. RSA est généralement utilisé. Le type de clé définit l'algorithme de chiffrement pour la communication entre les hôtes. **Note** SSL VPN-Plus prend uniquement en charge les certificats RSA.

Option	Description
Taille de la clé	Entrez la taille de clé en bits. La valeur minimale est de 2 048 bits.
Description	(Facultatif) Entrez une description pour le certificat.

5 Cliquez sur **Conserver**.

Le système génère la demande de signature de certificat et ajoute une nouvelle entrée de type CSR à la liste à l'écran.

Résultats

Dans la liste à l'écran, lorsque vous sélectionnez une entrée de type CSR, ses détails sont affichés à l'écran. Vous pouvez copier les données au format PEM affichées de la demande de signature de certificat (CSR) et les soumettre à une autorité de certification (CA) pour obtenir un certificat d'autorité de certification.

Étape suivante

Utilisez la demande de signature de certificat pour créer un certificat de service en utilisant l'une de ces deux options :

- Transmettez la demande CSR à une autorité de certification pour obtenir un certificat signé par une autorité de certification. Lorsque l'autorité de certification vous envoie le certificat signé, importez-le dans le système. Reportez-vous à Importer le certificat signé par une autorité de certification correspondant à la demande de signature de certificat générée pour une passerelle Edge.
- Utilisez la demande de signature de certificat pour créer un certificat autosigné. Reportez-vous à Configuration d'un certificat de service autosigné.

Importer le certificat signé par une autorité de certification correspondant à la demande de signature de certificat générée pour une passerelle Edge

Après avoir généré une demande de signature de certificat (CSR) et obtenu le certificat signé par une autorité de certification sur la base de cette demande, vous pouvez importer le certificat obtenu afin que la passerelle Edge l'utilise.

Conditions préalables

Vérifiez que vous avez obtenu le certificat signé par une autorité de certification qui correspond à la demande de signature de certificat. Si la clé privée dans le certificat signé par une autorité de certification ne correspond pas à celle de la demande de signature de certificat sélectionnée, le processus d'importation échoue.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **Certificats**.

3 Sélectionnez la demande de signature de certificat dans le tableau à l'écran pour lequel vous importez le certificat signé par une autorité de certification.

4 Importez le certificat signé.

   a Cliquez sur **Certificat signé généré pour la demande de signature de certificat (CSR)**.

   b Fournissez les données PEM du certificat signé par une autorité de certification.

   - Si les données se trouvent dans un fichier PEM sur un système auquel vous pouvez accéder, cliquez sur le bouton **Télécharger** pour accéder au fichier et sélectionnez-le.
   - Si vous pouvez copier et coller les données du fichier PEM, collez-les dans le champ **Certificat signé (format PEM)**.

     Incluez les lignes `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`.

   c (Facultatif) Saisir une description.

   d Cliquez sur **Conserver**.

   Note Si la clé privée du certificat signé par une autorité de certification ne correspond pas à celle de la demande de signature de certificat que vous avez sélectionnée sur l'écran Certificats, le processus d'importation échoue.

Résultats

Le certificat signé par une autorité de certification avec le type Certificat de service s'affiche dans la liste à l'écran.

Étape suivante

Attachez le certificat signé par une autorité de certification aux tunnels SSL VPN-Plus ou VPN IPsec selon les besoins. Reportez-vous à Configurer les paramètres du serveur SSL VPN et Spécifiez les paramètres VPN IPsec globaux.

Configuration d'un certificat de service autosigné

Vous pouvez configurer des certificats de service autosignés avec vos passerelles Edge, à utiliser dans leurs fonctionnalités liées aux VPN. Vous pouvez créer, installer et gérer des certificats autosignés.

Si le certificat de service est disponible sur l'écran Certificats, vous pouvez le spécifier lorsque vous configurez les paramètres liés au VPN de la passerelle Edge. Le VPN présente le certificat de service spécifié aux clients qui accèdent à ce réseau.

Conditions préalables

Vérifiez qu'au moins une CSR est disponible sur l'écran **Certificats** pour la passerelle Edge. Reportez-vous à Générer une demande de signature de certificat pour une passerelle Edge.

Procédure

1. Ouvrez les services de passerelle Edge.
   a. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
   b. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
   c. Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.
2. Cliquez sur l'onglet **Certificats**.
3. Sélectionnez la demande de signature de certificat (CSR) dans la liste que vous souhaitez utiliser pour ce certificat autosigné et cliquez sur **Demande de signature de certificat (CSR) autosignée**.
4. Tapez le nombre de jours correspondant à la validité du certificat autosigné.
5. Cliquez sur **Conserver**.

   Le système génère le certificat autosigné et ajoute une nouvelle entrée de type Certificat de service à la liste à l'écran.

Résultats

Le certificat autosigné est disponible sur la passerelle Edge. Dans la liste à l'écran, lorsque vous sélectionnez une entrée de type Certificat de service, ses détails s'affichent.

Ajouter un certificat d'autorité de certification à la passerelle Edge pour la vérification de l'approbation des certificats SSL

L'ajout d'un certificat d'autorité de certification à une passerelle Edge permet la vérification de l'approbation des certificats SSL qui sont présentés à la passerelle Edge pour authentification, généralement les certificats client utilisés dans les connexions VPN à la passerelle Edge.

Il vous est recommandé d'ajouter le certificat racine de votre entreprise ou organisation en tant que certificat d'autorité de certification. Il est généralement utilisé pour un réseau SSL VPN, lorsque vous souhaitez authentifier des clients VPN à l'aide de certificats. Les certificats client peuvent être distribués aux clients VPN et, lorsque ces derniers se connectent, leurs certificats client sont validés par rapport au certificat de l'autorité de certification.

Note Lorsque vous ajoutez un certificat d'autorité de certification, vous configurez généralement une liste de révocation des certificats (CRL) pertinente. La liste de révocation des certificats protège contre les clients qui présentent des certificats révoqués. Reportez-vous à Ajouter une liste de révocation des certificats à une passerelle Edge.

Conditions préalables

Vérifiez que les données de certificat d'autorité de certification sont au format PEM. Dans l'interface utilisateur, vous pouvez coller les données du fichier PEM du certificat d'autorité de certification ou accéder à un fichier qui contient les données et est disponible sur votre réseau depuis votre système local.

Procédure

1. Ouvrez les services de passerelle Edge.
   a. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
   b. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
   c. Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.
2. Cliquez sur l'onglet **Certificats**.
3. Cliquez sur **Certificat d'autorité de certification**.
4. Fournissez les données du certificat d'autorité de certification.
   - Si les données se trouvent dans un fichier PEM sur un système auquel vous pouvez accéder, cliquez sur le bouton **Télécharger** pour accéder au fichier et sélectionnez-le.
   - Si vous pouvez copier et coller les données du fichier PEM, collez-les dans le champ **Certificat d'autorité de certification (format PEM)**.

     Incluez les lignes `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`.
5. (Facultatif) Saisir une description.
6. Cliquez sur **Conserver**.

Résultats

Le certificat d'autorité de certification avec le type Certificat d'autorité de certification figure dans la liste à l'écran. Il est désormais possible de spécifier ce certificat d'autorité de certification lorsque vous configurez les paramètres liés au VPN de la passerelle Edge.

Ajouter une liste de révocation des certificats à une passerelle Edge

Une liste de révocation des certificats (CRL) est une liste de certificats numériques que l'autorité de certification (CA) émettrice déclare avoir révoqués, afin que les systèmes puissent être mis à jour pour ne pas approuver les utilisateurs qui présentent ces certificats révoqués. Vous pouvez ajouter des listes de révocation des certificats à la passerelle Edge.

Comme cela est décrit dans le *Guide d'administration de NSX*, la liste de révocation des certificats contient les éléments suivants :

- Les certificats révoqués et les motifs de la révocation
- Les dates d'émission des certificats
- Les entités ayant émis les certificats
- Une date proposée pour la prochaine version

Lorsqu'un utilisateur potentiel tente d'accéder à un serveur, le serveur autorise ou refuse l'accès en fonction de l'entrée de cet utilisateur dans la liste de révocation des certificats.

Procédure

1. Ouvrez les services de passerelle Edge.
   a. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
   b. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
   c. Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.
2. Cliquez sur l'onglet **Certificats**.
3. Cliquez sur **CRL**.
4. Fournissez les données de la liste de révocation des certificats.
   - Si les données se trouvent dans un fichier PEM sur un système auquel vous pouvez accéder, cliquez sur le bouton **Télécharger** pour accéder au fichier et sélectionnez-le.
   - Si vous pouvez copier et coller les données du fichier PEM, collez-les dans le champ **Liste de révocation de certificats (format PEM)**.

     Incluez les lignes **`-----BEGIN X509 CRL-----`** et **`-----END X509 CRL-----`**.
5. (Facultatif) Saisir une description.
6. Cliquez sur **Conserver**.

Résultats

La liste de révocation des certificats s'affiche dans la liste à l'écran.

Ajouter un certificat de service à la passerelle Edge

L'ajout de certificats de service à une passerelle Edge permet l'utilisation de ces certificats dans les paramètres liés au VPN de la passerelle Edge. Vous pouvez ajouter un certificat de service à l'écran **Certificats**.

Conditions préalables

Vérifiez que vous disposez du certificat de service et de sa clé privée au format PEM. Dans l'interface utilisateur, vous pouvez coller les données du fichier PEM ou accéder à un fichier qui contient les données et est disponible sur votre réseau depuis votre système local.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **Certificats**.

3 Cliquez sur **Certificat de service**.

4 Entrez les données au format PEM du certificat du service.

   - Si les données se trouvent dans un fichier PEM sur un système auquel vous pouvez accéder, cliquez sur le bouton **Télécharger** pour accéder au fichier et sélectionnez-le.
   - Si vous pouvez copier et coller les données du fichier PEM, collez-les dans le champ **Certificat de service (format PEM)**.

     Incluez les lignes `-----BEGIN CERTIFICATE-----` et `-----END CERTIFICATE-----`.

5 Entrez les données au format PEM de la clé privée du certificat.

   - Si les données se trouvent dans un fichier PEM sur un système auquel vous pouvez accéder, cliquez sur le bouton **Télécharger** pour accéder au fichier et sélectionnez-le.
   - Si vous pouvez copier et coller les données du fichier PEM, collez-les dans le champ **Clé privée (format PEM)**.

     Incluez les lignes `---BEGIN RSA PRIVATE KEY---` et `---END RSA PRIVATE KEY---`.

6 Entrez une phrase secrète de clé privée et confirmez-la.

7 (Facultatif) Saisir une description.

8 Cliquez sur **Conserver**.

Résultats

Le certificat de type Certificat de service figure dans la liste à l'écran. Il est désormais possible de sélectionner ce certificat de service lorsque vous configurez les paramètres liés au VPN de la passerelle Edge.

Personnaliser le regroupement d'objets

Le logiciel NSX de votre environnement vCloud Director vous offre la possibilité de définir des ensembles et des groupes de certaines entités, que vous pouvez ensuite utiliser pour spécifier d'autres configurations relatives au réseau, comme pour les règles de pare-feu.

Créer un ensemble d'adresses IP à utiliser dans les règles de pare-feu et la configuration du relais DHCP

Un ensemble d'adresses IP est un groupe d'adresses IP que vous pouvez créer au niveau d'un centre de données virtuel d'organisation. Vous pouvez utiliser un ensemble d'adresses IP comme source ou destination dans une règle de pare-feu ou dans une configuration de relais DHCP.

Créez un ensemble d'adresses IP à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres des services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Ensembles d'adresses IP**.

Les ensembles d'adresses IP qui sont déjà définis sont affichés dans cet écran.

3 Pour ajouter un ensemble d'adresses IP, cliquez sur le bouton **Créer** (+).

4 Entrez un nom et, éventuellement, une description de l'ensemble d'adresses IP, ainsi que les adresses IP à inclure dans l'ensemble.

5 Pour enregistrer cet ensemble d'adresses IP, cliquez sur **Conserver**.

Résultats

Le nouvel ensemble d'adresses IP peut être sélectionné en tant que source ou destination dans les règles de pare-feu ou dans les configurations du relais DHCP.

Créer un ensemble d'adresses MAC à utiliser dans les règles de pare-feu

Un ensemble d'adresses MAC est un groupe d'adresses MAC que vous pouvez créer au niveau d'un centre de données virtuel d'organisation. Vous pouvez utiliser un ensemble d'adresses MAC comme source ou destination dans une règle de pare-feu.

Vous créez un ensemble d'adresses MAC à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Ensembles d'adresses MAC**.

Les ensembles d'adresses MAC qui sont déjà définis sont affichés dans cet écran.

3 Pour ajouter un ensemble d'adresses MAC, cliquez sur le bouton **Créer** (+).

4 Entrez un nom pour l'ensemble, une description facultative et les adresses MAC à inclure dans l'ensemble.

5 Pour enregistrer l'ensemble d'adresses MAC, cliquez sur **Conserver**.

Résultats

Le nouvel ensemble d'adresses MAC peut être sélectionné en tant que source ou destination dans les règles de pare-feu.

Afficher les services disponibles pour les règles de pare-feu

Vous pouvez afficher la liste des groupes de services utilisables dans les règles de pare-feu. Dans ce contexte, un service est une combinaison port-protocole.

Vous pouvez afficher les services disponibles à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez sur l'onglet **Services**.

Résultats

Les services disponibles sont affichés sur l'écran.

Afficher les groupes de services disponibles pour les règles de pare-feu

Vous pouvez afficher la liste des groupes de services pouvant être utilisés dans les règles de pare-feu. Dans ce contexte, un service est une combinaison port-protocole et un groupe de services est un groupe de services ou d'autres groupes de services.

Vous pouvez afficher les groupes de services disponibles à l'aide de la page **Regroupement d'objets**. Pour ouvrir cette page, vous devez accéder aux paramètres de pare-feu distribué du VDC d'organisation ou aux paramètres de services d'une passerelle Edge qui appartient au VDC d'organisation.

Procédure

1 Ouvrez la page **Regroupement d'objets**.

Option	Action
À partir des paramètres du pare-feu distribué du VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **VDC d'organisation**. c Sélectionnez le bouton radio situé en regard du nom du centre de données virtuel d'organisation cible, puis cliquez sur **Gérer le pare-feu**. d Cliquez sur l'onglet **Regroupement d'objets**.
À partir des paramètres de services d'une passerelle Edge sur le VDC d'organisation	a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**. b Dans le panneau de gauche, cliquez sur **Passerelles Edge**. c Sélectionnez le bouton radio situé en regard du nom d'une passerelle Edge appartenant au centre de données virtuel d'organisation cible, puis cliquez sur **Services**. d Cliquez sur l'onglet **Regroupement d'objets**.

2 Cliquez dans l'onglet **Groupes de services**.

Résultats

Les groupes de services disponibles s'affichent sur l'écran. La colonne Description affiche les services qui sont regroupés dans chaque groupe de services.

Afficher l'utilisation des réseaux et les allocations IP sur une passerelle Edge

Vous pouvez afficher les réseaux sur une passerelle Edge avec des informations sur l'utilisation de leur pool d'adresses IP et sur leurs sous-réseaux. Vous pouvez également afficher l'adresse IP allouée à chaque réseau.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.

3 Pour afficher les réseaux externes avec des informations sur l'utilisation de leur pool d'adresses IP et sur leurs sous-réseaux, cliquez sur l'onglet **Réseaux externes > Réseaux et sous-réseaux**.

4 Pour afficher les réseaux externes avec des informations sur leurs adresses IP et leurs catégories, cliquez sur l'onglet **Réseaux externes > Allocations IP**.

Modification des propriétés de la passerelle Edge

Activer ou désactiver le routage distribué sur une passerelle Edge

Après avoir activé le routage distribué vCloud Director sur une passerelle Edge, l'administrateur d'organisation peut créer de nombreux réseaux de centre de données virtuel d'organisation acheminés avec des interfaces distribuées connectées à cette passerelle Edge. Le trafic sur ces réseaux est optimisé pour la communication entre machines virtuelles.

Conditions préalables

L'instance de NSX Manager de sauvegarde est configurée avec un cluster NSX Controller. Reportez-vous au *Guide d'administration de NSX*.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
3. Sélectionnez le bouton radio situé en regard du nom de la passerelle Edge cible, puis cliquez sur **Activer le routage distribué** ou **Désactiver le routage distribué**.
4. Pour confirmer, cliquez sur **OK**.

Modifier les réseaux externes et les paramètres de passerelle Edge

Pour modifier les réseaux externes et les paramètres de passerelle Edge, vous pouvez utiliser l'Assistant **Modifier la passerelle Edge**, qui contient les mêmes pages que l'assistant que vous avez utilisé pour créer la passerelle Edge.

Vous pouvez modifier les paramètres configurés lors de l'ajout de la passerelle Edge. Reportez-vous à Ajouter une passerelle Edge NSX Data Center for vSphere .

Pour modifier le paramètre de routage distribué, reportez-vous à Activer ou désactiver le routage distribué sur une passerelle Edge.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
3. Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge à modifier, puis cliquez sur **Modifier**.
4. Pour modifier les paramètres de la passerelle Edge, accédez aux pages de l'Assistant **Modifier la passerelle Edge** en cliquant sur **Suivant** et, sur la page **Prêt à terminer**, cliquez sur **Terminer**.

Modifier les paramètres généraux d'une passerelle Edge

Vous pouvez modifier le nom et la description d'une passerelle Edge, activer ou désactiver le mode FIPS et l'état de haute disponibilité, et changer la configuration de la taille de la passerelle Edge.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.
3. Sous l'onglet **Général**, dans le coin supérieur droit, cliquez sur **Modifier**.
4. (Facultatif) Modifiez le nom et la description de la passerelle Edge.
5. (Facultatif) Activez ou désactivez chaque paramètre de passerelle Edge général.

Paramètre général	Description
Mode FIPS	Configure la passerelle Edge pour utiliser le mode FIPS NSX.
Haute disponibilité	Active le basculement automatique vers une passerelle Edge de sauvegarde.

6. (Facultatif) Changez la configuration de la passerelle Edge pour vos ressources système.

Configuration	Description
Compacte	Requiert moins de ressources de mémoire et de calcul.
Grande	Fournit une plus grande capacité et des performances plus importantes que la configuration Compacte. Les configurations Grande et Extra grande offrent des fonctions de sécurité identiques.
Extra grande	À utiliser pour les environnements bénéficiant d'un équilibrage de charge avec un grand nombre de sessions simultanées.
Quadruple	À utiliser pour les environnements à débit élevé. Nécessite un débit de connexion élevé.

7. Pour confirmer les modifications, cliquez sur **Enregistrer**.

Modifier la passerelle par défaut sur une passerelle Edge

Vous pouvez changer le réseau qu'une passerelle Edge utilise comme passerelle par défaut.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.

3 Dans l'onglet **Réseaux externes > Passerelle par défaut**, dans le coin supérieur droit, cliquez sur **Modifier**.

4 (Facultatif) Configurez un réseau en tant que passerelle par défaut.

   a Activez le bouton bascule **Configurer la passerelle par défaut**.

   b Sélectionnez le bouton radio en regard du nom du réseau externe cible, puis celui en regard de l'adresse IP cible.

   c (Facultatif) Activez le bouton bascule **Utiliser la passerelle par défaut pour le relais DNS**.

5 Pour confirmer les modifications, cliquez sur **Enregistrer**.

Modifier les paramètres IP d'une passerelle Edge

Vous pouvez modifier les paramètres IP des réseaux externes sur une passerelle Edge.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.

3 Dans l'onglet **Réseaux externes > Paramètres IP**, cliquez sur **Modifier**.

4 Pour chaque réseau de la passerelle Edge, dans la cellule **Adresses IP**, entrez une adresse IP ou laissez la cellule vide.

   Si vous n'entrez pas d'adresse IP pour un réseau, le système attribue une adresse IP arbitraire à ce réseau.

5 Pour confirmer les modifications, cliquez sur **Enregistrer**.

Modifier les pools d'adresses IP sous-alloués d'une passerelle Edge

Vous pouvez sous-allouer plusieurs pools d'adresses IP statiques à partir des pools d'adresses IP disponibles d'un réseau externe sur une passerelle Edge.

Note L'allocation d'adresses IP à une passerelle Edge via la sous-allocation est un processus par lequel le fournisseur attribue la propriété des adresses IP à la passerelle. vCloud Director configure automatiquement l'interface de passerelle appropriée avec les adresses secondaires lors du processus de sous-allocation, ce qui peut provoquer des conflits d'adresses IP si l'une des adresses IP est utilisée en dehors de vCloud Director.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.

3 Cliquez sur l'onglet **Réseaux externes > Pools d'adresses IP sous-alloués**.

   Vous pouvez voir les pools d'adresses IP sous-alloués actuels pour chaque réseau externe sur cette passerelle Edge.

4 Cliquez sur le bouton radio en regard du nom d'un réseau externe, puis cliquez sur **Modifier**.

   Vous pouvez voir les pools d'adresses IP disponibles pour ce réseau externe et les pools d'adresses IP sous-alloués actuels, s'ils ont été configurés.

5 Modifiez les pools d'adresses IP sous-alloués pour ce réseau externe et cliquez sur **Enregistrer**.

   Vous pouvez ajouter, modifier et supprimer des adresses IP et des plages à partir des plages de pools d'adresses IP disponibles.

Résultats

Le système associe des plages d'adresses IP qui se chevauchent.

Modifier les limites de débit sur une passerelle Edge

Vous pouvez configurer les limites de débit entrant et sortant pour chaque réseau externe sur la passerelle Edge.

Des limites de débit ne s'appliquent qu'à des réseaux externes qui dépendent de groupes de ports distribués avec une liaison statique.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**, puis sur le nom de la passerelle Edge cible.

3 Dans l'onglet **Réseaux externes > Limites de débit**, dans le coin supérieur droit, cliquez sur **Modifier**.

   Vous pouvez voir les limites de débit actuelles pour chaque réseau externe sur cette passerelle Edge.

4 Modifiez les limites de débit, puis cliquez sur **Enregistrer**.

   Pour chaque réseau externe sur la passerelle Edge, vous pouvez activer ou désactiver les limites de débit, et vous pouvez modifier les débits entrant et sortant.

Redéployer une passerelle Edge

Vous pouvez supprimer et déployer un nouveau dispositif de passerelle Edge avec les dernières configurations.

Si les services Edge ne fonctionnent pas comme prévu, vous pouvez redéployer le dispositif de passerelle Edge.

Lorsque vous redéployez une passerelle Edge, vCloud Director la supprime et la recrée avec les dernières configurations.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

3 Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Redéployer**.

4 Pour confirmer, cliquez sur **OK**.

Résultats

La machine virtuelle de la passerelle Edge est remplacée par une nouvelle machine virtuelle et tous les services sont restaurés.

Supprimer une passerelle Edge

Vous pouvez supprimer une passerelle Edge du centre de données virtuel d'organisation.

Conditions préalables

Supprimez tous les réseaux de centre de données virtuel d'organisation qui utilisent la passerelle Edge cible.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

3 Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Supprimer**.

4 Pour confirmer, cliquez sur **Supprimer**.

Statistiques et journaux pour une passerelle Edge

Vous pouvez afficher les statistiques et les journaux d'une passerelle Edge.

Afficher les statistiques

Vous pouvez afficher des statistiques sur l'écran **Services de passerelle Edge**.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez dans l'onglet **Statistiques**.

3 Naviguez dans les onglets en fonction du type de statistiques que vous souhaitez afficher.

Option	Description
Connexions	L'écran Connexions offre une visibilité opérationnelle. L'écran affiche les graphiques correspondant au trafic circulant à travers les interfaces de la passerelle Edge sélectionnée et les statistiques de connexion des services de pare-feu et d'équilibrage de charge. Sélectionnez la période pour laquelle vous voulez afficher les statistiques.
VPN IPsec	L'écran VPN IPsec affiche l'état et les statistiques VPN IPsec, ainsi que l'état et les statistiques de chaque tunnel.
VPN L2	L'écran VPN L2 affiche l'état et les statistiques VPN L2.

Activer la journalisation

Vous pouvez activer la journalisation pour une passerelle Edge. Outre l'activation de la journalisation pour les fonctionnalités pour lesquelles vous souhaitez collecter des données de journal, vous devez disposer d'un serveur Syslog pour recevoir les données de journaux collectés pour terminer la configuration. Lorsque vous configurez un serveur Syslog sur l'écran Paramètres Edge, vous pouvez accéder aux données consignées depuis ce serveur Syslog.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Sous l'onglet **Paramètres Edge**, cliquez sur le bouton **Modifier le serveur Syslog**.

Vous pouvez personnaliser le serveur Syslog des journaux liés à la mise en réseau de votre passerelle Edge pour les services pour lesquels la journalisation est activée.

Si l'administrateur système de vCloud Director a déjà configuré un serveur Syslog pour l'environnement vCloud Director, le système utilise ce serveur Syslog par défaut et son adresse IP s'affiche sur l'écran **Paramètres Edge**.

3 Activez la journalisation par fonctionnalité.

- Sous l'onglet **NAT**, cliquez sur le bouton **Règle DNAT** et activez le bouton bascule **Activer la journalisation**.

  Consigne la traduction d'adresses.

- Sous l'onglet **NAT**, cliquez sur le bouton **Règle SNAT** et activez le bouton bascule **Activer la journalisation**.

  Consigne la traduction d'adresses.

- Sous l'onglet **Routage**, cliquez sur **Configuration du routage** et sous Configuration de routage dynamique, activez le bouton bascule **Activer la journalisation**.

  Enregistre les activités de routage dynamique. Dans le menu déroulant **Niveau de journal**, vous pouvez sélectionner la limite inférieure du niveau d'état du message à enregistrer.

- Sous l'onglet **Équilibrage de charge**, cliquez sur **Configuration globale** et activez le bouton bascule **Activer la journalisation**.

  Consigne le flux de trafic pour l'équilibrage de charge. Dans le menu déroulant **Niveau de journal**, vous pouvez sélectionner la limite inférieure du niveau d'état du message à enregistrer.

- Sous l'onglet **VPN**, accédez à **VPN IPSec > Paramètres de journalisation**, puis activez le bouton bascule **Activer la journalisation**.

  Enregistre le flux de trafic entre le sous-réseau local et le sous-réseau homologue. Dans le menu déroulant **Niveau de journal**, vous pouvez sélectionner la limite inférieure du niveau d'état du message à enregistrer.

- Sous l'onglet **VPN-Plus SSL**, cliquez sur **Paramètres généraux** et activez le bouton bascule **Activer la journalisation**.

  Conserve un journal du trafic traversant la passerelle du SSL VPN.

- Sous l'onglet **VPN-Plus SSL**, cliquez sur **Paramètres du serveur** et activez le bouton bascule **Activer la journalisation**.

  Enregistre les activités qui se produisent sur le serveur VPN SSL pour Syslog. Dans le menu déroulant **Niveau de journal**, vous pouvez sélectionner la limite inférieure du niveau d'état du message à enregistrer.

Activer l'accès de ligne de commande SSH à une passerelle Edge

Vous pouvez activer l'accès de ligne de commande SSH à une passerelle Edge

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur l'onglet **Paramètres Edge**.

3 Configurez les paramètres SSH.

Option	Description
Nom d'utilisateur **Mot de passe** **Confirmer le mot de passe**	Entrez les informations d'identification pour l'accès SSH à la passerelle Edge. Par défaut, le nom d'utilisateur SSH est **admin**.
Expiration du mot de passe	Entrez la période d'expiration du mot de passe en jours.
Bannière de connexion	Entrez le texte qui s'affiche lorsque les utilisateurs établissent une connexion SSH à la passerelle Edge.

4 Activez le bouton bascule **Activé**.

Étape suivante

Configurez les règles NAT ou de pare-feu appropriées pour autoriser l'accès SSH à la passerelle Edge.

Gestion de passerelles Edge NSX-T Data Center

8

Une passerelle Edge NSX-T Data Center fournit un réseau VDC d'organisation routé avec connectivité aux réseaux externes et aux propriétés de gestion IP. Elle peut également fournir des services tels qu'un pare-feu, la traduction d'adresses réseau (NAT), le transfert DNS et DHCP, ce qui est activé par défaut.

Ce chapitre contient les rubriques suivantes :

- Ajouter une passerelle Edge NSX-T Data Center
- Ajouter un groupe de pare-feu à une passerelle Edge NSX-T
- Ajouter une règle de pare-feu de passerelle Edge NSX-T
- Ajouter une règle SNAT ou DNAT à une passerelle Edge NSX-T
- Configurer un service de redirecteur DNS sur une passerelle Edge NSX-T
- Modifier les allocations IP d'une passerelle Edge NSX-T
- Allocation d'adresses IP rapide
- Créer des profils de port d'application personnalisés

Ajouter une passerelle Edge NSX-T Data Center

Une passerelle Edge NSX-T Data Center fournit à un réseau VDC d'organisation routé la connectivité aux réseaux externes et peut fournir des services, tels que l'équilibrage de charge, la traduction d'adresses réseau et un pare-feu.

Conditions préalables

Pour plus d'informations sur la configuration système requise pour le déploiement d'une passerelle Edge NSX-T Data Center, reportez-vous au *Guide d'administration de NSX-T*.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le panneau de gauche, cliquez sur **Passerelles Edge**.
3. Cliquez sur **Nouveau**.

4 Sélectionnez le VDC d'organisation reposant sur NSX-T sur lequel vous souhaitez créer la passerelle Edge, puis cliquez sur **Suivant**.

5 Entrez un nom et une éventuelle description pour la nouvelle passerelle Edge, puis cliquez sur **Suivant**.

6 Sélectionnez le réseau externe auquel la nouvelle passerelle Edge se connecte, puis cliquez sur **Suivant**.

7 (Facultatif) Modifiez les adresses IP ou les plages d'adresses IP allouées à la passerelle Edge, puis cliquez sur **Suivant**.

8 Vérifiez la page **Prêt à terminer** et cliquez sur **Terminer**.

Ajouter un groupe de pare-feu à une passerelle Edge NSX-T

Pour créer des règles de pare-feu et les ajouter à une passerelle Edge NSX-T, vous devez d'abord créer les groupes de pare-feu. Les groupes de pare-feu sont des groupes d'objets auxquels les règles de pare-feu s'appliquent. La combinaison de plusieurs objets en groupes de pare-feu contribue à réduire le nombre total de règles de pare-feu à créer.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge NSX-T, puis sur **Sécurité**.

3 Cliquez sur l'onglet **Groupes**, puis sur **Nouveau**.

4 Entrez le nom du groupe de pare-feu et, éventuellement, une description.

5 Entrez une adresse IP ou une plage d'adresses IP pour les machines virtuelles que le groupe comprend, puis cliquez sur **Ajouter**.

6 Pour enregistrer le groupe de pare-feu, cliquez sur **Enregistrer**.

Résultats

Vous avez créé un groupe de pare-feu et vous l'avez ajouté à la passerelle Edge NSX-T.

Étape suivante

Ajouter une règle de pare-feu de passerelle Edge NSX-T

Ajouter une règle de pare-feu de passerelle Edge NSX-T

Pour contrôler le trafic réseau entrant et sortant vers et depuis une passerelle Edge NSX-T, vous créez des règles de pare-feu.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis sur **Services**.

3 Si l'écran **Pare-feu** n'est pas visible, cliquez sur l'onglet **Pare-feu**.

4 Cliquez sur **Modifier les règles**.

5 Sélectionnez une règle de pare-feu, puis cliquez sur le bouton **Ajouter au-dessus**.

   Une ligne pour la nouvelle règle est ajoutée au-dessus de la règle sélectionnée.

6 Configurez la règle de pare-feu.

Option	Description
Nom	Entrez un nom pour la règle.
État	Pour activer la règle lors de la création, activez l'option **État**.
Applications	(Facultatif) Pour sélectionner un profil de port spécifique auquel la règle s'applique, activez l'option **Applications** et cliquez sur **Enregistrer**.
Source	Sélectionnez une option et cliquez sur **Conserver**. ■ Pour autoriser ou refuser le trafic depuis n'importe quelle adresse source, activez l'option **N'importe quelle source**. ■ Pour autoriser ou refuser le trafic de groupes de pare-feu spécifiques, sélectionnez les groupes de pare-feu dans la liste.
Destination	Sélectionnez une option et cliquez sur **Conserver**. ■ Pour autoriser ou refuser le trafic vers n'importe quelle adresse de destination, activez l'option **N'importe quelle destination**. ■ Pour autoriser ou refuser le trafic de groupes de pare-feu spécifiques, sélectionnez les groupes de pare-feu dans la liste.
Action	Dans le menu déroulant **Action**, sélectionnez une option. ■ Pour autoriser le trafic depuis ou vers les sources, les destinations et les services spécifiés, sélectionnez **Accepter**. ■ Pour bloquer le trafic depuis ou vers les sources, les destinations et les services spécifiés, sélectionnez **Refuser**.
Protocole IP	Indiquez si vous souhaitez appliquer la règle au trafic IPv4 ou IPv6.

Option	Description
Direction	Sélectionnez le sens du trafic auquel appliquer la règle.
Activez la journalisation.	Pour que la traduction d'adresses effectuée par cette règle soit journalisée, activez l'option **Activer la journalisation** .

7 Cliquez sur **Enregistrer**.

8 Pour configurer des règles supplémentaires, répétez ces étapes.

Résultats

Une fois les règles de pare-feu créées, elles figurent dans la liste des règles de pare-feu de la passerelle Edge. Vous pouvez déplacer les règles vers le haut, vers le bas, les modifier ou les supprimer si nécessaire.

Ajouter une règle SNAT ou DNAT à une passerelle Edge NSX-T

Pour modifier l'adresse IP source d'une adresse IP privée en une adresse IP publique, vous créez une règle NAT source (SNAT). Pour modifier l'adresse IP de destination d'une adresse IP publique en une adresse IP privée, vous créez une règle NAT de destination (DNAT).

Lorsque vous configurez une règle SNAT ou DNAT sur une passerelle Edge dans l'environnement vCloud Director, vous configurez toujours la règle du point de vue de votre VDC d'organisation. Une règle SNAT traduit l'adresse IP source des paquets envoyés à partir d'un réseau VDC d'organisation vers un réseau externe ou un autre réseau VDC d'organisation. Une règle DNAT traduit l'adresse IP, et éventuellement le port, des paquets reçus par un réseau VDC d'organisation en provenance d'un réseau externe ou d'un autre réseau VDC d'organisation.

Conditions préalables

Les adresses IP publiques doivent avoir été ajoutées à l'interface de la passerelle Edge sur laquelle vous voulez ajouter la règle.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis sur **NAT**.

3 Pour ajouter une règle, cliquez sur **Ajouter**.

4 Configurez une règle NAT source (de l'intérieur vers l'extérieur).

Option	Description
Nom	Entrez un nom pour la règle.
État	Pour activer la règle lors de la création, activez l'option **État**.
Type d'interface	Sélectionnez l'interface sur laquelle appliquer la règle.
IP externe	Entrez l'adresse IP publique de la passerelle Edge pour laquelle vous configurez la règle SNAT.
IP interne	Entrez l'adresse IP ou une plage d'adresses IP des machines virtuelles pour lesquelles vous configurez la règle SNAT afin qu'elles puissent envoyer du trafic vers le réseau externe.
Activez la journalisation.	Pour que la traduction d'adresses effectuée par cette règle soit journalisée, activez l'option **Activer la journalisation** .

5 Configurez une règle NAT de destination (de l'extérieur vers l'intérieur).

Option	Description
Nom	Entrez un nom pour la règle.
État	Pour activer la règle lors de la création, activez l'option **État**.
Type d'interface	Sélectionnez l'interface sur laquelle appliquer la règle.
IP externe	Entrez l'adresse IP publique de la passerelle Edge pour laquelle vous configurez la règle DNAT. Les adresses IP que vous entrez doivent appartenir à la plage d'adresses IP sous-allouée de la passerelle Edge.
Application	(Facultatif) Sélectionnez un profil de port d'application spécifique auquel appliquer la règle. Le profil de port d'application inclut un port et un protocole que le trafic entrant utilise sur la passerelle Edge pour se connecter au réseau interne.
IP interne	Entrez l'adresse IP ou une plage d'adresses IP des machines virtuelles pour lesquelles vous configurez DNAT afin qu'elles puissent recevoir du trafic en provenance du réseau externe.
Port interne	(Facultatif) Sélectionnez le port ou la plage de ports vers lesquels la règle DNAT effectue la traduction pour les paquets entrants destinés aux machines virtuelles.
Activez la journalisation.	Pour que la traduction d'adresses effectuée par cette règle soit journalisée, activez l'option **Activer la journalisation** .

6 Cliquez sur **Enregistrer**.

7 Pour configurer des règles supplémentaires, répétez ces étapes.

Configurer un service de redirecteur DNS sur une passerelle Edge NSX-T

Pour transférer des requêtes DNS vers des serveurs DNS externes, configurez un redirecteur DNS.

Dans le cadre de la configuration du service de redirecteur DNS, vous pouvez également ajouter des zones de redirecteur conditionnelles. Une zone de redirecteur conditionnelle est configurée comme une liste contenant jusqu'à cinq zones DNS de nom de domaine complet. Si une requête DNS correspond à un nom de domaine de cette liste, la requête est transférée aux serveurs à partir de la zone de redirecteur correspondante.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis sur **Services**.

3 Cliquez sur **DNS** et, dans la section **Redirecteur DNS**, cliquez sur **Modifier**.

4 Pour activer le service Redirecteur DNS, activez l'option **État**.

5 Entrez le nom de la zone DNS par défaut et, éventuellement, une description.

6 Entrez une ou plusieurs adresses IP de serveurs en amont, séparées par des virgules.

7 Cliquez sur **Enregistrer**.

8 (Facultatif) Ajoutez une zone de redirecteur conditionnelle.

   a Dans la section **Zone de redirecteur conditionnelle**, cliquez sur **Ajouter**.

   b Entrez un nom pour la zone de redirecteur.

   c Entrez une ou plusieurs adresses IP de serveurs en amont, séparées par des virgules.

   d Entrez un ou plusieurs noms de domaine, séparés par des virgules, puis cliquez sur **Enregistrer**.

Modifier les allocations IP d'une passerelle Edge NSX-T

Vous pouvez allouer plusieurs adresses IP d'un réseau externe à une passerelle Edge.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis sur **Allocations IP**.

   Dans les grilles de gestion des adresses IP, vous pouvez voir les adresses IP qui sont allouées à la passerelle Edge et les adresses IP actuellement utilisées par la passerelle Edge.

3 Dans la section **Adresses IP allouées**, cliquez sur **Gestion des adresses IP**.

   Dans la grille **Gestion des adresses IP**, vous pouvez afficher l'utilisation d'adresses IP de chacun des réseaux externes dont dispose la passerelle Edge.

4 Entrez une plage d'adresses IP, puis cliquez sur **Ajouter**.

5 Cliquez sur **Enregistrer**.

Résultats

Les adresses IP sont allouées à la passerelle Edge.

Étape suivante

Affichez les adresses IP allouées à la passerelle Edge, ajoutez d'autres adresses IP ou supprimez-les si nécessaire.

Allocation d'adresses IP rapide

Vous pouvez allouer des adresses IP d'un sous-réseau de réseau externe à une passerelle Edge sans entrer d'adresses IP ou de plages d'adresses IP spécifiques à l'aide de l'allocation d'adresses IP rapide.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis sur **Allocations IP**.

   Dans les grilles de gestion des adresses IP, vous pouvez voir les adresses IP qui sont allouées à la passerelle Edge et les adresses IP actuellement utilisées par la passerelle Edge.

3 Dans la section **Adresses IP allouées**, cliquez sur **Allocation d'adresses IP rapide**.

4 Dans le menu déroulant, sélectionnez un sous-réseau depuis lequel attribuer des adresses IP.

   Si plusieurs sous-réseaux sont disponibles, la sélection de **Tous** entraîne l'allocation d'adresses IP à partir d'un ou de plusieurs sous-réseaux.

5 Entrez le nombre d'adresses IP à allouer à la passerelle Edge, puis cliquez sur **Enregistrer**.

   Le nombre ne doit pas être supérieur au nombre d'adresses IP disponibles dans le sous-réseau que vous avez sélectionné.

Résultats

Les adresses IP sont allouées à la passerelle Edge.

Étape suivante

Affichez les adresses IP allouées à la passerelle Edge, ajoutez d'autres adresses IP ou supprimez-les si nécessaire.

Créer des profils de port d'application personnalisés

Pour créer des règles de pare-feu et NAT, vous pouvez utiliser des profils de port d'application préconfigurés et des profils de port d'application personnalisés.

Les profils de port d'application incluent une combinaison d'un protocole et d'un port, ou un groupe de ports, qui est utilisée pour les services de pare-feu et NAT sur la passerelle Edge. Outres les profils de port par défaut qui sont préconfigurés pour NSX-T Data Center, vous pouvez créer des profils de port d'application personnalisés.

Lorsque vous créez un profil de port d'application personnalisé sur une passerelle Edge, il devient visible pour toutes les autres passerelles Edge NSX-T Data Center qui se trouvent dans le même VDC d'organisation.

Procédure

1 Ouvrez les services de passerelle Edge.

   a Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

   b Dans le panneau de gauche, cliquez sur **Passerelles Edge**.

   c Cliquez sur le bouton radio situé en regard du nom de la passerelle Edge cible, puis sur **Services**.

2 Cliquez sur la passerelle Edge, puis dans l'onglet **Sécurité**.

3 Cliquez sur **Profils de port d'application**.

4 Dans la section **Applications personnalisées**, cliquez sur **Nouveau**.

5 Entrez le nom et, éventuellement, la description du profil de port d'application.

6 Sélectionnez un protocole dans le menu déroulant.

7 Entrez un port ou une plage de ports, séparés par une virgule, puis cliquez sur **Enregistrer**.

Étape suivante

Utilisez des profils de port d'application pour créer des règles de pare-feu et NAT. Reportez-vous à Ajouter une règle de pare-feu de passerelle Edge NSX-T et à Ajouter une règle SNAT ou DNAT à une passerelle Edge NSX-T.

Gestion des instances de vCenter Server dédiées et des proxys

9

vCloud Director peut agir comme un serveur proxy HTTP entre les locataires et l'environnement vSphere sous-jacent. Avec des instances dédiées de vCenter Server, vous pouvez utiliser vCloud Director comme point central de gestion (CPOM) pour vos environnements vSphere.

Lorsque vous ajoutez une instance de vCenter Server à vCloud Director, vous pouvez spécifier l'objet de l'instance.

Instance dédiée de vCenter Server

L'infrastructure d'une instance attachée de vCenter Server est encapsulée en tant que SDDC (Software-Defined Data Center) et entièrement dédiée à un seul locataire. Vous créez une instance de vCenter Server dédiée en activant l'accès locataire pour cette instance. Après avoir activé l'accès locataire, vous pouvez publier une instance de vCenter Server dédiée vers un locataire.

Instance partagée de vCenter Server

Le fournisseur peut utiliser différents pools de ressources de l'instance partagée de vCenter Server sur plusieurs VDC fournisseurs, puis allouer ces pools de ressources à différents locataires. Une instance de vCenter Server partagée ne peut pas être publiée vers des locataires.

aucune

L'instance de vCenter Server n'a pas d'objet spécifique.

Avec des instances de vCenter Server dédiées, vous pouvez utiliser vCloud Director comme point central de gestion pour tous vos environnements vSphere.

- Vous pouvez dédier les ressources d'une instance de vCenter Server à un seul locataire en publiant l'instance de vCenter Server dédiée correspondant uniquement au niveau de son organisation. Le locataire ne partage pas ces ressources avec d'autres locataires. Le locataire peut accéder à cette instance dédiée de vCenter Server à l'aide d'une interface utilisateur ou d'un proxy d'API sans qu'un VPN soit requis.
- Vous pouvez utiliser vCloud Director comme annuaire léger pour enregistrer toutes vos instances de vCenter Server.
- Vous pouvez utiliser vCloud Director comme point de terminaison d'API pour toutes vos instances de vCenter Server.

Vous pouvez activer l'accès locataire et marquer une instance de vCenter Server comme étant dédiée pendant ou après l'attachement de l'instance cible de vCenter Server à vCloud Director. Reportez-vous à Attacher une instance de vCenter Server seule ou avec une instance de NSX Manager.

Avec une instance de vCenter Server associée, vous pouvez créer une instance de vCenter Server partagée ou une instance de vCenter Server dédiée. Si vous avez créé une instance de vCenter Serverpartagée, vous ne pouvez pas utiliser cette instance de vCenter Server pour créer une instance de vCenter Server, dédiée, et inversement.

Vous pouvez créer des proxys que les locataires peuvent utiliser pour accéder à l'environnement vSphere sous-jacent. Les utilisateurs peuvent se connecter à l'interface utilisateur ou à l'API des composants à l'aide de proxys en utilisant leurs comptes vCloud Director.

Avec les instances de vCenter Server dédiées dans vCloud Director, il n'est pas nécessaire que vCenter Server soit accessible de façon publique. Pour contrôler l'accès, vous pouvez activer et désactiver l'accès locataire à un SDDC dans vCloud Director.

Un proxy est un point d'accès à un composant à partir d'un SDDC, par exemple, une instance de vCenter Server, un hôte ESXi ou une instance de NSX Manager. En activant et en désactivant un proxy, vous pouvez autoriser et arrêter l'accès locataire via ce proxy.

Création et gestion d'instances de vCenter Server dédiées et de proxys

Pour créer et gérer des instances vCenter Server dédiées et des proxys, vous pouvez utiliser le portail d'administration de fournisseur de services ou vCloud OpenAPI. Pour vCloud OpenAPI, reportez-vous à *Démarrage de vCloud OpenAPI* à l'adresse https://code.vmware.com.

Important vCloud Director requiert une connexion réseau directe à chaque instance de vCenter Server dédiée. Si l'instance de vCenter Server utilise une instance externe de Platform Services Controller, vCloud Director nécessite également une connexion réseau directe à l'instance de Platform Services Controller.

Pour utiliser VMware OVF Tool dans une instance de vCenter Server proxy dédiée, vCloud Director nécessite une connexion directe à chaque hôte ESXi.

1 Créez une instance de vCenter Server dédiée.

   Lorsque vous ajoutez une instance de vCenter Server à l'environnement vCloud Director, vous pouvez créer une instance de vCenter Server dédiée en activant l'accès locataire dans l'Assistant **Ajouter un système vCenter Server**. Lors de l'attachement de l'instance de vCenter Server, vous pouvez également créer un proxy pour celle-ci. Reportez-vous au Ajouter l'instance de vCenter Server. Vous pouvez activer l'accès locataire des instances de vCenter Server qui sont déjà ajoutées à vCloud Director et n'ont pas d'utilisation spécifiée. Reportez-vous au Activer l'accès locataire d'une instance de vCenter Server associée. L'activation de l'accès locataire rend l'instance de vCenter Server disponible pour être publiée auprès des locataires.

2 Ajoutez un proxy.

Vous pouvez créer un proxy lorsque vous associez une instance de vCenter Server à vCloud Director ou ultérieurement. Si l'instance de vCenter Server utilise une instance externe de Platform Services Controller, vCloud Director crée également un proxy pour l'instance de Platform Services Controller. Avec des proxys parents et enfants, vous pouvez masquer certains proxys vis-à-vis des locataires ou vous pouvez activer et désactiver des groupes de proxys enfants via leurs proxys parents. Pour plus d'informations sur la création d'un proxy après l'ajout d'une instance de vCenter Server à vCloud Director, reportez-vous à Créer un proxy pour une instance dédiée de vCenter Server.

Vous pouvez modifier, activer, désactiver et supprimer des proxys dans l'onglet **Proxys** sous **Ressources vSphere**. Si une instance de vCenter Server dispose de plusieurs proxys, vous pouvez sélectionner le proxy par défaut.

Note Lorsque vous ajoutez un proxy à une instance de vCenter Server dédiée, vous devez télécharger le certificat et l'empreinte numérique, afin que les locataires puissent récupérer le certificat et l'empreinte numérique si le composant proxy utilise des certificats auto-signés.

Pour afficher et gérer les certificats et les listes de révocation de certificats (CRL), reportez-vous à Gérer les certificats de proxy et les listes de révocation de certificats.

3 Obtenez le certificat et l'empreinte numérique des proxys créés et vérifiez que le certificat et l'empreinte sont présents et corrects. Reportez-vous au Gérer les certificats de proxy et les listes de révocation de certificats.

4 Publiez l'instance de vCenter Server dédiée dans une ou plusieurs organisations.

Vous pouvez publier une instance dédiée de vCenter Server vers un locataire et la rendre visible via vCloud Director Tenant Portal. Dans la plupart des cas, une instance de vCenter Server ne doit être publiée que vers un seul locataire. Reportez-vous au Publier une instance de vCenter Server dédiée.

5 Pour permettre aux locataires d'accéder aux instances de vCenter Server dédiées et aux proxys à partir de vCloud Director Tenant Portal, vous devez publier le plug-in **Extension CPOM** vers leurs organisations. Reportez-vous à Publier ou annuler la publication d'un plug-in d'une organisation.

Ce chapitre contient les rubriques suivantes :

- Activer l'accès locataire d'une instance de vCenter Server associée
- Créer un proxy pour une instance dédiée de vCenter Server
- Gérer les certificats de proxy et les listes de révocation de certificats
- Publier une instance de vCenter Server dédiée

Activer l'accès locataire d'une instance de vCenter Server associée

Vous pouvez activer l'accès locataire des instances de vCenter Server qui sont déjà ajoutées à vCloud Director et n'ont pas d'utilisation spécifiée. L'activation de l'accès locataire crée une instance de vCenter Server dédiée et la rend disponible pour être publiée auprès des locataires.

Avec une instance de vCenter Server associée, vous pouvez créer une instance de vCenter Server partagée ou une instance de vCenter Server dédiée. Si vous avez créé une instance partagée de vCenter Server et que vous souhaitez l'utiliser comme instance de vCenter Server dédiée, vous devez d'abord supprimer tous les centres de données virtuels (VDC) fournisseurs qui utilisent les ressources de l'instance de vCenter Server. La suppression de tous les VDC fournisseurs liés à l'instance de vCenter Server partagée change son état en Aucun.

Conditions préalables

Vérifiez que vous disposez dans votre environnement d'au moins une instance de vCenter Server associée qui n'est pas dédiée ou partagée.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**.
3. Sélectionnez une instance de vCenter Server sans objectif spécifié dans la colonne **Utilisation**.
4. Cliquez sur **Activer l'accès locataire**.

Étape suivante

Publier une instance de vCenter Server dédiée.

Créer un proxy pour une instance dédiée de vCenter Server

Vous pouvez créer des proxys que les locataires peuvent utiliser pour accéder à l'environnement vSphere sous-jacent. Vous pouvez créer des serveurs proxy pour des instances dédiées de vCenter Server dans vCloud Director.

Conditions préalables

- Vérifiez que vous disposez d'au moins une instance de vCenter Server avec l'accès locataire activé dans votre environnement vCloud Director. Reportez-vous à la section Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le volet de gauche, cliquez sur **vCenter**.

3 Sélectionnez une instance dédiée de vCenter Server.

4 Sur la page contenant des informations détaillées sur vCenter Server, cliquez sur l'onglet **Proxy**, puis sur **Nouveau**.

5 Entrez un nom, un hôte cible et l'URL de l'interface utilisateur du nouveau proxy.

L'hôte cible est le nom d'hôte ou l'adresse IP du composant pour lequel vCloud Director doit être un proxy. L'URL de l'interface utilisateur du nouveau proxy est l'URL vers laquelle l'interface utilisateur de vCloud Director pointe lorsque le locataire ouvre le proxy.

6 Si vous souhaitez que le proxy soit visible par les locataires, activez l'option **Visible par les locataires**.

7 (Facultatif) Cliquez sur **Sélectionner un proxy parent** et sélectionnez un proxy dans la liste.

8 Cliquez sur **Enregistrer**.

Étape suivante

Gérer les certificats de proxy et les listes de révocation de certificats.

Gérer les certificats de proxy et les listes de révocation de certificats

Vous pouvez afficher et télécharger en aval et en amont les certificats de proxy et les listes de révocation de certificats (CRL).

Conditions préalables

- Vérifiez que vous disposez d'au moins une instance de vCenter Server avec l'accès locataire activé dans votre environnement vCloud Director. Reportez-vous à la section Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.

2 Dans le panneau de gauche, cliquez sur **Proxys**, puis sélectionnez un proxy.

3 Cliquez sur **Gérer le certificat**.

4 Téléchargez en amont ou en aval le certificat et la liste de révocation de certificats.

5 Cliquez sur **Enregistrer**.

Publier une instance de vCenter Server dédiée

Vous pouvez publier une instance de vCenter Server dédiée vers un locataire et le rendre visible via vCloud Director Tenant Portal. Par défaut, une instance de vCenter Server doit être publiée uniquement vers un seul locataire.

Par défaut, un SDDC est une instance de vCenter Server que vous dédiez à un seul locataire en publiant l'instance de vCenter Server dédiée correspondante uniquement vers son organisation. Le locataire ne partage pas les ressources de l'instance de vCenter Server dédiée avec d'autres locataires. La publication d'une instance de vCenter Server dédiée vers plusieurs locataires enfreint les limites de la location. Cependant, un locataire doit parfois avoir accès à plusieurs instances de vCenter Server dédiées. Dans ces cas-là, vous pouvez publier une instance de vCenter Server dédiée vers plusieurs locataires.

Conditions préalables

- Vérifiez que vous disposez d'au moins une instance de vCenter Server avec l'accès locataire activé dans votre environnement vCloud Director. Reportez-vous à la section Chapitre 9 Gestion des instances de vCenter Server dédiées et des proxys.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de vSphere**.
2. Dans le volet de gauche, cliquez sur **vCenter**.
3. Sélectionnez une instance de vCenter Server avec accès locataire activé.

   Les instances de vCenter Server avec accès locataire activé ont la valeur Dédié dans la colonne **Utilisation**.
4. Cliquez sur **Gérer les locataires**.
5. Sélectionnez le ou les locataires vers lesquels vous souhaitez publier l'instance de vCenter Server.

   La désélection d'un locataire de la liste annule la publication de vCenter Server.
6. Cliquez sur **Enregistrer**.

Étape suivante

Pour permettre aux utilisateurs d'accéder aux instances de vCenter Server dédiées et aux proxys à partir de vCloud Director Tenant Portal, vous devez publier le plug-in **Extension CPOM** vers leurs organisations. Reportez-vous à Publier ou annuler la publication d'un plug-in d'une organisation.

Gestion d'administrateurs système et de rôles

10

Le portail d'administration des fournisseurs de services vCloud Director vous permet d'ajouter des administrateurs système à vCloud Director individuellement ou dans le cadre d'un groupe LDAP. Vous pouvez également ajouter et modifier les rôles qui déterminent les droits détenus par un utilisateur au sein de son organisation.

Note À partir de vCloud Director 9.5, les fournisseurs de services peuvent créer des rôles de fournisseur et gérer les utilisateurs et les groupes fournisseurs à l'aide du portail d'administration des fournisseurs de services vCloud Director ou de vCloud OpenAPI. Pour plus d'informations sur la gestion des groupes, des utilisateurs et des rôles de fournisseur, consultez le *Guide du portail d'administration des fournisseurs de services vCloud Director*. Pour examiner la documentation sur l'OpenAPI vCloud, accédez à `https://vCloud_Director_IP_address_or_host_name/docs`.

Ce chapitre contient les rubriques suivantes :

- Gestion des droits et des rôles
- Gestion des utilisateurs et des groupes de fournisseur

Gestion des droits et des rôles

Un droit est l'unité fondamentale du contrôle d'accès dans vCloud Director. Un rôle associe un nom de rôle à un ensemble de droits. Chaque organisation peut avoir différents droits et rôles.

vCloud Director utilise des rôles et les droits qui leur sont associés pour déterminer si un utilisateur ou un groupe est autorisé à effectuer une opération. De nombreuses procédures documentées dans les guides vCloud Director incluent un rôle prérequis. Ces conditions préalables supposent que le rôle nommé est le rôle prédéfini non modifié ou un rôle incluant un ensemble de droits équivalent.

vCloud Director 9.5 introduit des bundles de droits et des rôles de locataire globaux que les administrateurs système peuvent utiliser pour gérer les droits et les rôles qui sont disponibles pour chaque organisation.

Après que vous avez installé vCloud Director, le système contient uniquement le bundle des droits système, qui inclut tous les droits qui sont disponibles dans le système. Le bundle des droits système n'est publié pour aucune organisation. Le système contient également des rôles de locataire globaux intégrés qui sont publiés pour toutes les organisations. Pour plus d'informations sur les rôles prédéfinis, reportez-vous à Rôles prédéfinis et leurs droits.

Après que vous avez mis à niveau vCloud Director 9.1 ou version antérieure, en plus du bundle des droits système, le système contient un bundle de droits hérités pour chaque organisation existante. Chaque bundle de droits hérités inclut les droits disponibles dans l'organisation associée au moment de la mise à niveau et est uniquement publié dans cette organisation.

Note Pour commencer à utiliser le modèle de bundle de droits pour une organisation existante, vous devez supprimer le bundle de droits hérités correspondant.

Si vous avez effectué une mise à niveau de vCloud Director depuis la version 9.1 ou une version antérieure, les modèles de rôle existants sont publiés pour toutes les organisations en tant que rôles de locataires globaux et les rôles existants qui ne sont pas liés à des modèles de rôle sont disponibles en tant que rôles spécifiques des locataires pour leurs organisations.

Terminologie des droits

Droite

Chaque droit fournit une vue ou donne accès à un type d'objet particulier dans vCloud Director. Les droits appartiennent à différentes catégories selon les objets auxquels ils sont liés, par exemple, vApp, catalogue, organisation, etc. L'organisation fournisseur contient tous les droits disponibles dans le système. L'administrateur système définit les droits qui sont disponibles pour chaque organisation. Vous ne pouvez ni créer ni modifier les droits inclus dans vCloud Director.

Bundle de droits

Les administrateurs système peuvent utiliser des bundles de droits pour gérer les droits disponibles pour chaque organisation. Un bundle de droits est un ensemble de droits que l'administrateur système peut publier pour une ou plusieurs organisations. L'administrateur système peut créer et publier des bundles de droits qui correspondent à des niveaux de service, à une fonctionnalité séparément monétisable ou à d'autres groupements de droits arbitraires. Seuls les administrateurs système peuvent afficher et gérer les bundles de droits. Vous pouvez publier plusieurs bundles pour la même organisation.

Droits de l'organisation

Les droits d'organisation constituent l'ensemble des droits disponibles pour une organisation. Les droits d'organisation peuvent comprendre plusieurs bundles de droits, mais les administrateurs et les utilisateurs de l'organisation voient l'ensemble de droits qu'ils peuvent utiliser pour créer et modifier des rôles spécifiques du locataire.

Terminologie des rôles

Rôle

Un rôle est un ensemble de droits pouvant être attribués à un ou plusieurs utilisateurs et groupes. Lorsque vous créez ou importez un utilisateur ou un groupe, vous devez lui attribuer un rôle.

Rôles de fournisseur

Les rôles de fournisseur constituent l'ensemble des rôles auxquels seule l'organisation fournisseur a accès. Les rôles de fournisseur peuvent uniquement être attribués aux utilisateurs fournisseurs. Les administrateurs système peuvent créer des rôles de fournisseur personnalisés.

Rôles de locataire

Les rôles de locataire constituent l'ensemble des rôles disponibles pour une organisation.

Les administrateurs système peuvent créer et modifier des rôles de locataire globaux et les publier pour une ou plusieurs organisations. Les rôles de locataire globaux peuvent être attribués aux utilisateurs locataires dans les organisations où ils sont publiés. Les administrateurs d'organisation ne peuvent pas modifier les rôles de locataire globaux.

Note Les utilisateurs locataires ne peuvent utiliser ces droits qu'à partir de leurs rôles qui sont publiés pour leurs organisations.

Rôles spécifiques des locataires

Les administrateurs d'organisation peuvent créer et modifier des rôles spécifiques des locataires, qui sont locaux pour leurs organisations. Les rôles spécifiques des locataires ne peuvent être attribués qu'aux utilisateurs locataires dans l'organisation à laquelle ils appartiennent. Les rôles spécifiques des locataires ne peuvent contenir qu'un sous-ensemble des droits d'organisation.

Pour plus d'informations sur la gestion des rôles spécifiques des locataires, reportez-vous à la section *Guide du portail de locataires de vCloud Director*.

Rôles prédéfinis et leurs droits

Chaque rôle vCloud Director prédéfini contient un ensemble de droits par défaut requis pour effectuer des opérations incluses dans les workflows communs. Par défaut, tous les rôles prédéfinis de locataire globaux sont publiés dans chaque organisation du système.

Rôles de fournisseur prédéfinis

Par défaut, les rôles de fournisseur qui sont uniquement locaux pour l'organisation de fournisseur sont les rôles **Administrateur système** et **Système multisite**. Les **administrateurs système** peuvent créer des rôles de fournisseur personnalisés supplémentaires.

Administrateur système

Le rôle **Administrateur système** existe uniquement dans l'organisation de fournisseur. Le rôle **Administrateur système** inclut tous les droits sur le système. Pour obtenir la liste des droits uniquement disponibles pour le rôle **Administrateur système**, consultez Droits d'administrateur système. Les informations d'identification du rôle **Administrateur système** sont établies pendant l'installation et la configuration. Un **administrateur système** peut créer des administrateurs système et des comptes d'utilisateurs supplémentaires dans l'organisation de fournisseur.

Système multisite

Utilisé pour exécuter le processus de pulsation pour les déploiements multisites. Ce rôle n'a qu'un seul droit, à savoir **Opérations système multisite**, qui donne l'autorisation d'effectuer une demande d'API vCloud qui récupère l'état du membre distant d'une association de sites.

Rôles de locataire globaux prédéfinis

Par défaut, les rôles de locataire globaux prédéfinis et les droits qu'ils contiennent sont publiés dans toutes les organisations. Les **administrateurs système** peuvent annuler la publication des droits et des rôles de locataire globaux dans des organisations individuelles. Les **administrateurs système** peuvent modifier ou supprimer des rôles de locataires globaux prédéfinis. Les **administrateurs système** peuvent créer et publier des rôles de locataire globaux supplémentaires.

Administrateur d'organisation

Après avoir créé une organisation, un **administrateur système** peut attribuer le rôle **Administrateur d'organisation** à n'importe quel utilisateur de l'organisation. Un utilisateur disposant du rôle **Administrateur de l'organisation** prédéfini peut gérer les utilisateurs et les groupes de son organisation et leur attribuer des rôles, y compris le rôle **Administrateur de l'organisation** prédéfini. Les rôles créés ou modifiés par un **administrateur d'organisation** ne sont pas visibles par les autres organisations.

Auteur de catalogue

Les droits associés au rôle prédéfini **Auteur de catalogue** permettent à un utilisateur de créer et de publier des catalogues.

Auteur de vApp

Les droits associés au rôle prédéfini **Auteur de vApp** permettent à un utilisateur d'utiliser les catalogues et de créer des vApp.

Utilisateur de vApp

Les droits associés au rôle prédéfini **Utilisateur de vApp** permettent à un utilisateur d'utiliser des vApp existants.

Accès via la console uniquement

Les droits associés au rôle prédéfini **Accès via la console uniquement** permettent à un utilisateur d'afficher les propriétés et l'état de la machine virtuelle, et d'utiliser le SE invité.

Différer vers le fournisseur d'identité

Les droits associés au rôle prédéfini **Différer vers le fournisseur d'identité** sont déterminés en fonction des informations reçues par le fournisseur d'identité OAuth ou SAML de l'utilisateur. Pour répondre aux critères d'inclusion lorsque le rôle **Différer vers le fournisseur d'identité** est attribué à un utilisateur ou à un groupe, le nom du rôle ou du groupe indiqué par le fournisseur d'identité doit correspondre exactement, casse comprise, à un nom de rôle ou de groupe défini dans votre organisation.

- Si l'utilisateur est défini par un fournisseur d'identité OAuth, il se voit attribuer les rôles indiqués dans le tableau `roles` de son jeton OAuth.
- Si l'utilisateur est défini par un fournisseur d'identité SAML, il se voit attribuer les rôles indiqués dans l'attribut SAML dont le nom est affiché dans l'élément `RoleAttributeName` situé dans l'élément `SamlAttributeMapping` de l'API `OrgFederationSettings` de l'organisation.

Si le rôle **Différer vers le fournisseur d'identité** est attribué à un utilisateur, mais qu'aucun nom de rôle ou de groupe correspondant n'est disponible dans votre organisation, l'utilisateur peut se connecter à l'organisation, mais sans droits. Si un fournisseur d'identité associe un utilisateur à un rôle correspondant à un niveau du système, par exemple **Administrateur système**, l'utilisateur peut se connecter, mais ne dispose d'aucun droit. Il vous faut attribuer manuellement un rôle à de tels utilisateurs.

À l'exception du rôle **Différer vers le fournisseur d'identité**, chaque rôle prédéfini inclut un ensemble de droits par défaut. Seul un **administrateur système** peut modifier les droits d'un rôle prédéfini. Si un **administrateur système** modifie un rôle prédéfini, les modifications sont appliquées à toutes les instances du rôle dans le système.

Droits des rôles de locataire globaux prédéfinis

Un **administrateur système** peut utiliser le Service Provider Admin Portal pour afficher la liste des droits inclus dans un rôle.

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, sélectionnez **Rôles**.

3 Cliquez sur le nom du rôle que vous souhaitez voir.

Un **administrateur d'organisation** peut utiliser le Service Provider Admin Portal ou l'OpenAPI vCloud pour afficher les droits d'un rôle ou créer des rôles locaux pour l'organisation.

Divers droits sont communs à plusieurs rôles globaux prédéfinis. Ces droits sont accordés par défaut à toutes les nouvelles organisations et peuvent être utilisés dans les autres rôles créés par l'**administrateur d'organisation**. Pour obtenir la liste des droits des rôles de locataire prédéfinis, consultez Droits des rôles de locataire globaux prédéfinis.

Droits d'administrateur système

Le rôle **Administrateur système** existe uniquement dans l'organisation de fournisseur. Par défaut, le rôle **Administrateur système** dispose de tous les droits vCloud Director.

Le rôle **Administrateur système** dispose de tous les droits vCloud Director. Cette liste se compose des droits dont disposent uniquement les **administrateurs système**. Le rôle **Administrateur système** a également le Droits des rôles de locataire globaux prédéfinis.

Tableau 10-1. Droits dont disposent uniquement les administrateurs système

Nouveautés dans cette version	Nom du droit
	Liste de contrôle d'accès : Gérer
	Liste de contrôle d'accès : Afficher
	Services supplémentaires : Exécuter des workflows
	Services supplémentaires : Afficher les workflows en cours d'exécution
	Services supplémentaires : Afficher les workflows
	Adopter le pool de ressources : Afficher
	Autre entité d'administration : Afficher
	Paramètres AMQP : Gérer
	Paramètres AMQP : Afficher
✓	**Explorateur d'API : Afficher**
	Catalogue : Importer le support depuis vSphere
	Catalogue : Vue VM fantôme
	Catalogue : Mise en cache des publications et abonnements VCSP
	Configuration de la cellule : Afficher
	Serveur de tunnel de cloud : Gérer
	Serveur de tunnel de cloud : Afficher
	Paramètres système de la bibliothèque de contenu : Gérer
	Paramètres système de la bibliothèque de contenu : Afficher
	Entité personnalisée : Créer des définitions d'entités personnalisées
	Entité personnalisée : Supprimer les définitions d'entités personnalisées
	Entité personnalisée : Modifier les définitions d'entités personnalisées
	Entité personnalisée : Afficher des définitions d'entités personnalisées
	Banque de données : Supprimer

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Banque de données : Modifier
	Banque de données : Activer ou désactiver
	Banque de données : Ouvrir dans vSphere
	Banque de données : Afficher
	Réseau VDC d'organisation direct
	Distributed Virtual Switch : Ouvrir dans vSphere
	Cluster Edge : Gérer
	Cluster Edge : Afficher
	Définition de l'API du service d'extension : Gérer
	Définition de l'API du service d'extension : Afficher
	Services d'extension : Afficher
	Extensions : Afficher
	Service externe : Gérer
	Service externe : Afficher
	Général : Afficher les détails d'erreur
	Rôle global : Modifier
	Rôle global : Afficher
	Hôte : Activer ou désactiver
	Hôte : Gérer
	Hôte : Ouvrir dans vSphere
	Hôte : Préparer ou annuler la préparation
	Hôte : Réparer
	Hôte : Mettre à niveau
	Hôte : Afficher
	Paramètres Kerberos : Gérer
	Paramètres Kerberos : Afficher
	Paramètres LDAP : Gérer
	Paramètres LDAP : Afficher

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Rapport de licence : Afficher
	Ressources de localisation : Gérer
	Multisite : Opérations système
	Pool de réseaux : Créer ou supprimer
	Pool de réseaux : Modifier
	Pool de réseaux : Ouvrir dans vSphere
	Pool de réseaux : Réparer
	Pool de réseaux : Afficher
	NSX-T : Modifier
	NSX-T : Afficher
	Extensions d'objet : Gérer
	Extensions d'objet : Afficher
	Réseau d'organisation : Créer ou supprimer
	Réseau d'organisation : Ouvrir dans vSphere
	Stratégie de calcul du vDC d'organisation : Vue admin
	Stratégie de calcul du vDC d'organisation : Gérer
	Pare-feu distribué de vDC d'organisation : Activer/désactiver
	Passerelle de vDC d'organisation : Configurer le routage BGP
	Passerelle de vDC d'organisation : Configurer VPN L2
	Passerelle de vDC d'organisation : Configurer le routage OSPF
	Passerelle de vDC d'organisation : Configurer l'accès à distance
	Passerelle de vDC d'organisation : Configurer VPN SSL
	Passerelle de vDC d'organisation : Configurer la journalisation système
	Passerelle de VDC d'organisation : Créer
	Passerelle de VDC d'organisation : Supprimer
	Passerelle de vDC d'organisation : Routage distribué
	Passerelle de VDC d'organisation : Importer
	Passerelle de vDC d'organisation : Modifier le facteur de forme

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Passerelle de VDC d'organisation : Mettre à jour
	Passerelle de vDC d'organisation : Mettre à jour les propriétés
	Passerelle de VDC d'organisation : Mettre à niveau
	Passerelle de vDC d'organisation : Afficher le routage BGP
	Passerelle de vDC d'organisation : Afficher le VPN L2
	Passerelle de vDC d'organisation : Afficher le routage OSPF
	Passerelle de vDC d'organisation : Afficher l'accès à distance
	Passerelle de vDC d'organisation : afficher le VPN SSL
	Réseau de VDC d'organisation : Importer
	Pool de ressources du VDC d'organisation : Ouvrir dans vSphere
	Pool de ressources du VDC d'organisation : Afficher
	Pool de ressources du VDC d'organisation : Modifier
	Stratégie de stockage du vDC d'organisation : Activer ou désactiver
	Stratégie de stockage du VDC d'organisation : Ouvrir dans vSphere
	Stratégie de stockage du VDC d'organisation : Supprimer
	VDC d'organisation : Créer
	VDC d'organisation : Supprimer
	VDC d'organisation : Activer ou désactiver
	VDC d'organisation : Modification étendue
	VDC d'organisation : Affichage étendu
	Organisation : Activer ou désactiver
	Organisation : Créer ou supprimer
	Organisation : Modifier les limites
	Organisation : Modifier le nom
	Organisation : Migrer le stockage des locataires
	Organisation : Effectuer des requêtes d'administrateur
	Organisation : Utiliser le fournisseur LDAP en tant que locataire
	Groupe de ports : Ouvrir dans vSphere

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Préférence : Gérer la définition des préférences
	Réseau du fournisseur : Créer ou supprimer
	Réseau du fournisseur : Modifier
	Réseau du fournisseur : Ouvrir dans vSphere
	Réseau du fournisseur : Afficher
	Stratégie de calcul du vDC fournisseur : Gérer
	Stratégie de calcul du vDC fournisseur : Afficher
	Pool de ressources du VDC fournisseur : Migrer les VM
	Pool de ressources du VDC fournisseur : Ouvrir dans vSphere
	Pool de ressources du VDC fournisseur : Afficher
	Stratégie de stockage du VDC fournisseur : Modifier
	Stratégie de stockage du vDC fournisseur : Activer ou désactiver
	Stratégie de stockage du VDC fournisseur : Ouvrir dans vSphere
	Stratégie de stockage du VDC fournisseur : Supprimer
	Stratégie de stockage du VDC fournisseur : Afficher
	VDC fournisseur : Ajouter un pool de ressources
	VDC fournisseur : Créer ou supprimer
	VDC fournisseur : Supprimer le pool de ressources
	VDC fournisseur : Modifier
	VDC fournisseur : Activer ou désactiver
	VDC fournisseur : Activer ou désactiver le pool de ressources
	VDC fournisseur : Activer vSphere VXLAN
	VDC fournisseur : Fusionner
	VDC fournisseur : Afficher
	Recharger la VM : Gérer
	Action de classe de ressource : Gérer
	Action de classe de ressource : Afficher
	Pool de ressources : Ouvrir

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Pool de ressources : Ouvrir dans vSphere
	Pool de ressources : Afficher
	Droit : Gérer
	Droit : Afficher
	Bundle de droits : Modifier
	Bundle de droits : Afficher
	SDDC : Gérer
	SDDC : Gérer le proxy
	SDDC : Afficher
	Extensions de sélecteur : Gérer
	Extensions de sélecteur : Afficher
	Applications de service : Gérer
	Applications de service : Afficher
	Autorisation de service : Gérer
	Configuration de service : Gérer
	Configuration de service : Afficher
	Bibliothèque de services : Créer des bibliothèques de services
	Bibliothèque de services : Supprimer les services de la bibliothèque de services
	Bibliothèque de services : Modifier les métadonnées de service
	Bibliothèque de services : Modifier le contenu d'un service
	Lien de service : Gérer
	Lien de service : Afficher
	Type de ressource de service : Gérer
	Type de ressource de service : Afficher
	Ressource de service : Gérer
	Ressource de service : Afficher
	Réseau vDC d'organisation partagé : Gérer
	Site : Modifier

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	Site : Afficher
	Élément bloqué : Gérer
	Élément bloqué : Afficher
	Opérations système : Exécuter les opérations système
	Organisation système : Gérer
	Organisation système : Afficher
	Paramètres système : Gérer
	Paramètres système : Afficher
	Tâche : Reprendre, abandonner ou échouer
	Tâche : Mettre à jour
	Tâche : Afficher les tâches
✓	**Jeton : Gérer**
✓	**Jeton : Gérer tous**
	Plug-ins d'interface utilisateur : Définir, télécharger, modifier, supprimer, associer ou dissocier
	Informations de marque du portail de l'interface utilisateur : Gérer
	Modèle de vApp : Forcer l'expiration du bail de stockage
	Modèle de vApp : Importer
	Modèle de vApp : Ouvrir dans vSphere
	vApp : Autoriser toute la configuration supplémentaire
	vApp : Autoriser la configuration supplémentaire de la fusion Ethernet
	vApp : Autoriser la configuration supplémentaire de la latence
	vApp : Autoriser la configuration supplémentaire correspondante
	vApp : Autoriser la configuration supplémentaire de l'affinité du nœud NUMA
	vApp : Modifier les paramètres de réservation de CPU et de mémoire de VM dans tous les types de VDC
	vApp : Entrer/quitter le mode de maintenance
	vApp : Forcer l'expiration du bail d'exécution
	vApp : Forcer l'expiration du bail de stockage

Tableau 10-1. Droits dont disposent uniquement les administrateurs système (suite)

Nouveautés dans cette version	Nom du droit
	vApp : Importer des options
	vApp : Gérer la maintenance
	vApp : Ouvrir dans vSphere
	vApp : Afficher la VM fantôme
	vApp : Vérification de conformité de VM
	vApp : Migrer, forcer l'annulation du déploiement, déplacer, consolider la VM
	Extension VCD : Enregistrer, annuler l'enregistrement, actualiser, associer ou dissocier
	Extension VCD : Afficher
	vCenter : Attacher ou détacher
	vCenter : Activer ou désactiver
	vCenter : Ouvrir dans vSphere
	vCenter : Actualiser
	vCenter : Afficher
	Groupe de vDC : Configurer
	Groupe de vDC : Afficher
	Modèle de VDC : Gérer la liste ACL
	Modèle de VDC : Vue étendue
	Modèle de VDC : Gérer
	VMC : Enregistrer le SDDC
	vRealize Orchestrator : Publier et annuler la publication de workflows pour les locataires
	vRealize Orchestrator : Inscrire et désinscrire les serveurs vRealize Orchestrator
	vRealize Orchestrator : Afficher les serveurs vRealize Orchestrator enregistrés
	vSphere Server : Gérer
	vSphere Server : Gérer le proxy
	vSphere Server : Afficher

Droits des rôles de locataire globaux prédéfinis

Divers droits sont communs à plusieurs rôles globaux prédéfinis. Ces droits sont accordés par défaut à toutes les nouvelles organisations et peuvent être utilisés dans les autres rôles créés par l'**administrateur d'organisation**.

Droits inclus dans les rôles de locataires globaux dans vCloud Director

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	Accéder à tous les VDC d'organisation	✓				
	Catalogue : Ajouter un vApp depuis Mon Cloud	✓	✓	✓		
	Catalogue : Changer le propriétaire	✓				
	Catalogue : Publications et abonnements CLSP	✓	✓			
	Catalogue : Créer/ supprimer un catalogue	✓	✓			
	Catalogue : Modifier des propriétés	✓	✓			
	Catalogue : Publier	✓	✓			
	Catalogue : Partage	✓	✓			
	Catalogue : Afficher la liste ACL	✓	✓			
	Catalogue : Afficher des catalogues privés et partagés	✓	✓	✓		
	Catalogue : Afficher des catalogues publiés	✓				
	Entité personnalisée : Afficher toutes les instances de l'entité personnalisée dans l'organisation	✓				
	Entité personnalisée : Afficher l'instance d'entité personnalisée	✓				
	Disque : Changer le propriétaire	✓	✓			

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	Disque : Créer	✓	✓	✓		
	Disque : Supprimer	✓	✓	✓		
	Disque : Modifier les propriétés	✓	✓	✓		
	Disque : Afficher les propriétés	✓	✓	✓	✓	
	Général : Contrôle administrateur	✓				
	Général : Vue administrateur	✓				
	Général : Envoyer une notification	✓				
	Groupe/utilisateur : Afficher	✓				
	Opérations de cloud hybride : Acquérir un ticket de contrôle	✓				
	Opérations de cloud hybride : Acquérir le ticket du tunnel depuis le cloud	✓				
	Opérations de cloud hybride : Acquérir un ticket de tunnel vers le cloud	✓				
	Opérations de cloud hybride : Créer un tunnel à partir du cloud	✓				
	Opérations de cloud hybride : Créer un tunnel vers le cloud	✓				
	Opérations de cloud hybride : Supprimer le tunnel depuis le cloud	✓				
	Opérations de cloud hybride : Supprimer le tunnel vers le cloud	✓				
	Opérations de cloud hybride : Mettre à jour la balise de point de terminaison du tunnel depuis le cloud	✓				

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	Opérations de cloud hybride : Afficher le tunnel depuis le cloud	✓				
	Opérations de cloud hybride : Afficher le tunnel vers le cloud	✓				
	Réseau d'organisation : Modifier les propriétés	✓				
	Réseau d'organisation : Afficher	✓				
	Stratégie de calcul de vDC d'organisation : Afficher	✓	✓	✓	✓	
	Pare-feu distribué de vDC d'organisation : Configurer les règles	✓				
	Pare-feu distribué de vDC d'organisation : Afficher les règles	✓				
	Passerelle de VDC d'organisation : Configurer DHCP	✓				
✓	**Passerelle de VDC d'organisation : Configurer DNS**	✓				
✓	**Passerelle de vDC d'organisation : Configurer le routage ECMP**	✓				
	Passerelle VDC d'organisation : Configurer pare-feu	✓				
	Passerelle de vDC d'organisation : Configurer le VPN IPSec	✓				
	Passerelle de vDC d'organisation : Configurer l'équilibrage de charge	✓				
	Passerelle de VDC d'organisation : Configurer NAT	✓				

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	Passerelle de vDC d'organisation : Configurer le routage statique	✓				
	Passerelle de VDC d'organisation : Configurer Syslog	✓				
	Passerelle de vDC d'organisation : Convertir en mise en réseau avancée	✓				
	Passerelle de VDC d'organisation : Afficher	✓				
	Passerelle de vDC d'organisation : Afficher DHCP	✓				
✓	**Passerelle de vDC d'organisation : Afficher DNS**	✓				
	Passerelle de vDC d'organisation : Afficher le pare-feu	✓				
	Passerelle de vDC d'organisation : Afficher le VPN IPSec	✓				
	Passerelle de vDC d'organisation : Afficher l'équilibrage de charge	✓				
	Passerelle de vDC d'organisation : Afficher NAT	✓				
	Passerelle de vDC d'organisation : Afficher le routage statique	✓				
	Réseau de VDC d'organisation : Modifier les propriétés	✓				
	Réseau de VDC d'organisation : Afficher les propriétés	✓		✓		
	Profil de stockage de VDC d'organisation : Définir la valeur par défaut	✓				

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	VDC d'organisation : Modifier	✓				
	VDC d'organisation : Modifier la liste ACL	✓				
	VDC d'organisation : Gérer le pare-feu	✓				
	VDC d'organisation : Afficher	✓	✓			
	Passerelle de vDC d'organisation : Afficher la liste ACL	✓				
	VDC d'organisation : Afficher les mesures	✓				
	VDC d'organisation : Modifier l'affinité VM-VM	✓	✓	✓		
	Organisation : Modifier les paramètres d'association	✓				
	Organisation : Modifier les paramètres de fédération	✓				
	Organisation : Modifier les paramètres LDAP	✓				
	Organisation : Modifier la stratégie relative aux baux	✓				
	Organisation : Modifier les paramètres OAuth	✓				
	Organisation : Modifier la stratégie de mot de passe	✓				
	Organisation : Modifier les propriétés	✓				
	Organisation : Modifier la stratégie relative aux quotas	✓				
	Organisation : Modifier les paramètres SMTP	✓				
	Organisation : Importer l'utilisateur/le groupe depuis le fournisseur d'identité lors de la modification de la liste ACL du VDC	✓				

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	Organisation : Afficher	✓	✓	✓		
	Organisation : Afficher les mesures	✓				
	Rôle : Créer, modifier, supprimer ou copier	✓				
	Bibliothèque de services : Afficher les bibliothèques de services	✓				
	Plug-ins d'interface utilisateur : Afficher	✓	✓	✓	✓	
	Modèle ou support de vApp : Copier	✓	✓	✓		
	Modèle ou support de vApp : Créer/télécharger	✓	✓			
	Modèle ou support de vApp : Modifier	✓	✓	✓		
	Modèle ou support de vApp : Afficher	✓	✓	✓	✓	
	Modèle de vApp : Changer le propriétaire	✓	✓			
	Modèle de vApp : Extraire	✓	✓	✓	✓	
	Modèle de vApp : Télécharger	✓	✓			
	vApp : Changer le propriétaire	✓				
	vApp : Copier	✓	✓	✓	✓	
	vApp : Créer ou reconfigurer	✓	✓	✓		
	vApp : Supprimer	✓	✓	✓	✓	
	vApp : Télécharger	✓	✓	✓		
	vApp : Modifier les propriétés	✓	✓	✓	✓	
	vApp : Modifier la stratégie de calcul de la VM	✓	✓	✓		
	vApp : Modifier le CPU de la VM	✓	✓	✓		

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	vApp : Modifier le disque dur de la VM	✓	✓	✓		
	vApp : Modifier la mémoire de la VM	✓	✓	✓		
	vApp : Modifier le réseau de la VM	✓	✓	✓	✓	
	vApp : Modifier les propriétés de la VM	✓	✓	✓	✓	
	vApp : Gérer les paramètres de mot de passe de la VM	✓	✓	✓	✓	✓
	vApp : Opérations d'alimentation	✓	✓	✓	✓	
	vApp : Partage	✓	✓	✓	✓	
	vApp : Opérations de snapshot	✓	✓	✓	✓	
	vApp : Charger	✓	✓	✓		
	vApp : Utiliser la console	✓	✓	✓	✓	✓
	vApp : Afficher la liste ACL	✓	✓	✓	✓	
	vApp : Afficher les mesures de la VM	✓		✓	✓	
	vApp : Options de démarrage de la VM	✓	✓	✓		
	vApp : Métadonnées de la VM vers vCenter	✓	✓	✓		
	Modèle de VDC : Instancier	✓				
	Modèle de VDC : Afficher	✓				

Gestion des bundles de droits

En tant qu'administrateur système, vous pouvez créer des bundles de droits et les publier dans une ou plusieurs organisations de votre cloud. Vous pouvez modifier et supprimer des bundles de droits existants. Vous pouvez annuler la publication des bundles de droits dans les organisations de votre cloud.

Créer un bundle de droits

Vous pouvez regrouper un ensemble de droits dans un bundle de droits que vous pouvez publier dans une ou plusieurs organisations de votre système.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Bundles de droits**.

3 Cliquez sur **Ajouter**.

4 Entrez un nom pour le nouveau bundle de droits et, éventuellement, une description.

5 Sélectionnez les droits que vous souhaitez associer à ce bundle.

Les droits sont regroupés en catégories et sous-catégories pour afficher ou gérer l'accès à l'objet auquel ils se rapportent.

Vous pouvez sélectionner les droits individuellement, les afficher ou les gérer par sous-catégorie, ou les afficher ou les gérer globalement.

Catégorie	Description
Contrôle d'accès	Contient des droits d'affichage et de gestion des organisations, des droits, des rôles et des utilisateurs.
Administration	Contient des droits d'affichage et de gestion des paramètres généraux et multisite.
Calculer	Contient des droits d'affichage et de gestion des VDC d'organisation et de fournisseur, des vApp, des modèles de VDC d'organisation et de la surveillance des machines virtuelles.
Extensions	Contient des droits d'affichage et de gestion des plug-ins et extensions vCloud Director.
Infrastructure	Contient des droits d'affichage et de gestion des ressources vSphere.
Bibliothèques	Contient des droits d'affichage et de gestion des catalogues et des éléments de catalogue.
Mise en réseau	Contient des droits d'affichage et de gestion des ressources réseau.

6 Cliquez sur **Enregistrer**.

Étape suivante

Vous pouvez publier le bundle de droits nouvellement créé dans une ou plusieurs organisations de votre système. Reportez-vous à Publier un bundle de droits ou en annuler la publication.

Publier un bundle de droits ou en annuler la publication

Vous pouvez publier un bundle de droits dans une ou plusieurs organisations dans votre système. Une fois que vous avez publié un bundle de droits pour une organisation, les droits de ce bundle deviennent partie intégrante de l'ensemble des droits de l'organisation.

Les droits d'organisation peuvent comprendre plusieurs bundles de droits, mais les administrateurs d'organisation et les utilisateurs voient un ensemble de droits qu'ils peuvent utiliser pour créer et modifier des rôles.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Bundles de droits**.
3. Cochez la case d'option en regard du bundle cible et cliquez sur **Publier**.
4. Pour publier le bundle :
   a. Cliquez sur **Publier pour les locataires**.
   b. Sélectionnez les organisations pour lesquelles vous souhaitez publier le rôle.
      - Si vous souhaitez publier le bundle pour les organisations existantes et les organisations récemment créées dans votre système, cliquez sur **Publier pour tous les locataires**.
      - Si vous souhaitez publier le bundle pour des organisations particulières dans votre système, sélectionnez ces organisations individuellement.
5. Pour annuler la publication du bundle :
   - Si vous souhaitez annuler la publication du bundle pour toutes les organisations de votre système, décochez la case d'option **Publier pour les locataires**.
   - Si vous voulez annuler la publication du bundle pour des organisations particulières de votre système, décochez la case **Publier pour tous les locataires** et décochez individuellement les organisations.
6. Cliquez sur **Enregistrer**.

Résultats

Les droits du bundle publié sont disponibles dans les organisations sélectionnées et peuvent être utilisés dans les rôles de ces organisations.

Les droits du rôle non publié sont retirés des organisations sélectionnées et ne peuvent pas être utilisés dans les rôles de ces organisations.

Afficher et modifier un bundle de droits

Vous pouvez afficher les droits qui sont inclus dans un bundle de droits. Vous pouvez modifier le nom, la description et les droits d'un bundle.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Bundles de droits**.

3 Cliquez sur le nom du bundle cible.

Vous pouvez afficher les droits associés au bundle en développant les catégories de droit.

4 Modifiez le bundle et cliquez sur **Conserver**.

Résultats

Si vous avez modifié les droits du bundle, le nouvel ensemble de droits s'applique à toutes les organisations sur lesquelles ce bundle de droits est publié.

Supprimer un bundle de droits

Vous pouvez supprimer un bundle de droits que vous n'utilisez plus dans vos organisations.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Bundles de droits**.

3 Sélectionnez le bouton radio en regard du bundle cible, puis cliquez sur **Supprimer**.

4 Pour confirmer, cliquez sur **OK**.

Gestion des rôles de locataire globaux

En tant qu'administrateur système, vous pouvez créer des rôles de locataire globaux et les publier dans une ou plusieurs organisations de votre cloud. Vous pouvez modifier et supprimer des rôles de locataire globaux existants. Vous pouvez annuler la publication des rôles de locataire globaux dans des organisations individuelles de votre cloud.

Après l'installation et la configuration initiale de vCloud Director, le système contient un ensemble de locataires globaux prédéfinis qui sont publiés sur toutes les organisations. Reportez-vous à Rôles prédéfinis et leurs droits.

Créer un rôle de locataire global

Vous pouvez créer un rôle de locataire global que vous pouvez publier pour une ou plusieurs organisations de votre système.

Après l'installation et la configuration initiale de vCloud Director, le système contient des rôles de locataire globaux prédéfinis qui sont publiés sur toutes les organisations. Pour plus d'informations sur les rôles prédéfinis, reportez-vous à Rôles prédéfinis et leurs droits.

Vous pouvez ajouter des rôles personnalisés globaux à votre système.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Rôles globaux**.

3 Cliquez sur **Ajouter**.

4 Entrez un nom pour le nouveau rôle et, éventuellement, une description.

5 Sélectionnez les droits que vous souhaitez associer au rôle.

Les droits sont regroupés en catégories et sous-catégories pour afficher ou gérer l'accès à l'objet auquel ils se rapportent.

Vous pouvez sélectionner les droits individuellement, les afficher ou les gérer par sous-catégorie, ou les afficher ou les gérer globalement.

Catégorie	Description
Contrôle d'accès	Contient des droits d'affichage et de gestion des organisations, des droits, des rôles et des utilisateurs.
Administration	Contient des droits d'affichage et de gestion des paramètres généraux et multisite.
Calculer	Contient des droits d'affichage et de gestion des VDC d'organisation et de fournisseur, des vApp, des modèles de VDC d'organisation et de la surveillance des machines virtuelles.
Extensions	Contient des droits d'affichage et de gestion des plug-ins et extensions vCloud Director.
Infrastructure	Contient des droits d'affichage et de gestion des ressources vSphere.
Bibliothèques	Contient des droits d'affichage et de gestion des catalogues et des éléments de catalogue.
Mise en réseau	Contient des droits d'affichage et de gestion des ressources réseau.

6 Cliquez sur **Conserver**.

Résultats

Lors de sa création, les nouveaux droits du locataire global sont uniquement disponibles pour l'organisation du fournisseur vCloud Director.

Étape suivante

Vous pouvez publier le rôle nouvellement créé dans une ou plusieurs organisations de votre système. Reportez-vous à Publier un rôle de locataire global ou annuler cette publication.

Publier un rôle de locataire global ou annuler cette publication

Vous pouvez publier un rôle de locataire global pour une ou plusieurs organisations dans votre système. Après que vous publiez un rôle pour une organisation, ce rôle devient partie intégrante de l'ensemble de rôles de locataire de l'organisation.

Conditions préalables

Si vous voulez annuler la publication d'un rôle de locataire global d'une organisation, vérifiez que ce rôle n'est attribué à aucun utilisateur dans l'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Rôles globaux**.
3. Cochez la case d'option en regard du rôle cible, puis cliquez sur **Publier**.
4. Pour publier le rôle :
   a. Cliquez sur **Publier pour les locataires**.
   b. Sélectionnez les organisations pour lesquelles vous souhaitez publier le rôle.
      - Si vous souhaitez publier le rôle pour toutes les organisations existantes et récemment créées dans votre système, sélectionnez **Publier pour tous les locataires**.
      - Si vous souhaitez publier le rôle pour des organisations particulières dans votre système, sélectionnez ces organisations individuellement.
5. Pour annuler la publication du rôle :
   - Si vous souhaitez annuler la publication du rôle pour toutes les organisations de votre système, décochez **Publier pour les locataires**.
   - Si vous voulez annuler la publication du rôle dans certaines organisations de votre système, décochez **Publier pour tous les locataires** et décochez individuellement ces organisations.
6. Cliquez sur **Enregistrer**.

Résultats

Le rôle publié est disponible dans les organisations sélectionnées et peut être attribué aux utilisateurs dans ces organisations. Les administrateurs d'organisation ne peuvent pas modifier les rôles de locataire globaux qui sont publiés pour leurs organisations.

Le rôle non publié est supprimé des organisations sélectionnées et ne peut pas être attribué aux utilisateurs dans ces organisations.

Afficher et modifier un rôle de locataire global

Vous pouvez afficher les droits qui sont inclus dans un rôle de locataire global. Vous pouvez modifier le nom, la description et les droits d'un rôle de locataire global.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Rôles globaux**.
3. Cliquez sur le nom du rôle cible.

   Vous pouvez afficher les droits associés au rôle en développant les catégories de droit.
4. Pour modifier le nom, la description ou les droits du rôle, cliquez sur **Modifier**.
5. Modifiez le rôle, puis cliquez sur **Conserver**.

Résultats

Si vous avez modifié les droits du rôle, le nouvel ensemble de droits s'applique aux utilisateurs de toutes les organisations auxquelles ce rôle est attribué.

Supprimer un rôle de locataire global

Vous pouvez supprimer un rôle de locataire global que vous n'utilisez plus dans vos organisations.

Conditions préalables

Le rôle de locataire global que vous souhaitez supprimer ne doit pas être attribué à aucun utilisateur dans toutes les organisations.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au locataire**, cliquez sur **Rôles globaux**.
3. Sélectionnez le bouton radio en regard du rôle cible, puis cliquez sur **Supprimer**.
4. Pour confirmer, cliquez sur **OK**.

Gestion des rôles de fournisseur

Vous pouvez créer et gérer des rôles dans votre organisation de fournisseur vCloud Director.

Pour plus d'informations sur la gestion des rôles de locataire, consultez le *Guide du portail de locataires de vCloud Director*.

Créer un rôle de fournisseur

Vous pouvez créer un rôle dans votre organisation de fournisseur vCloud Director.

Après l'installation et la configuration initiale de vCloud Director, le système contient des rôles prédéfinis qui sont des rôles locaux pour l'organisation du fournisseur et des rôles globaux pour toutes les organisations. Pour plus d'informations sur les rôles prédéfinis, reportez-vous à Rôles prédéfinis et leurs droits.

Vous pouvez ajouter des rôles de fournisseur personnalisés à votre organisation de fournisseur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Rôles**.

3 Cliquez sur **Nouveau**.

4 Entrez un nom pour le nouveau rôle et, éventuellement, une description.

5 Sélectionnez les droits que vous souhaitez associer au rôle.

Les droits sont regroupés en catégories et sous-catégories pour afficher ou gérer l'accès à l'objet auquel ils se rapportent.

Vous pouvez sélectionner les droits individuellement, les afficher ou les gérer par sous-catégorie, ou les afficher ou les gérer globalement.

Catégorie	Description
Contrôle d'accès	Contient des droits d'affichage et de gestion des organisations, des droits, des rôles et des utilisateurs.
Administration	Contient des droits d'affichage et de gestion des paramètres généraux et multisite.
Calculer	Contient des droits d'affichage et de gestion des VDC d'organisation et de fournisseur, des vApp, des modèles de VDC d'organisation et de la surveillance des machines virtuelles.
Extensions	Contient des droits d'affichage et de gestion des plug-ins et extensions vCloud Director.
Infrastructure	Contient des droits d'affichage et de gestion des ressources vSphere.
Bibliothèques	Contient des droits d'affichage et de gestion des catalogues et des éléments de catalogue.
Mise en réseau	Contient des droits d'affichage et de gestion des ressources réseau.

6 Cliquez sur **Enregistrer**.

Résultats

Les rôles récemment créés sont disponibles pour l'attribution aux utilisateurs de votre organisation de fournisseur.

Afficher ou modifier un rôle de fournisseur

Vous pouvez afficher les droits inclus dans un rôle qui est local pour votre organisation fournisseur vCloud Director. Vous pouvez modifier le nom, la description et les droits d'un rôle.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Rôles**.
3. Cliquez sur le nom du rôle cible.

   Vous pouvez afficher les droits associés au rôle en développant les catégories de droit.
4. Pour modifier le nom, la description ou les droits du rôle, cliquez sur **Modifier**.
5. Modifiez le rôle, puis cliquez sur **Enregistrer**.

Résultats

Si vous avez modifié les droits du rôle, le nouvel ensemble de droits s'applique aux utilisateurs auxquels ce rôle est attribué.

Supprimer un rôle de fournisseur

Vous pouvez supprimer un rôle que vous n'utilisez plus de votre organisation de fournisseur vCloud Director.

Conditions préalables

Le rôle que vous souhaitez supprimer ne doit être attribué à aucun utilisateur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Rôles**.
3. Sélectionnez le bouton radio en regard du rôle cible, puis cliquez sur **Supprimer**.
4. Pour confirmer, cliquez sur **OK**.

Gestion des utilisateurs et des groupes de fournisseur

Vous pouvez ajouter et importer des utilisateurs et des groupes dans votre organisation de fournisseur vCloud Director.

Pour plus d'informations sur la gestion des groupes et des utilisateurs de l'organisation, consultez le *Guide du portail de locataires de vCloud Director*.

Gestion des utilisateurs de fournisseur

Vous pouvez gérer les utilisateurs de votre organisation de fournisseur à l'aide de Service Provider Admin Portal.

Pour plus d'informations sur la gestion des utilisateurs de locataire dans les organisations, consultez le *Guide du portail de locataires de vCloud Director*.

Créer un utilisateur de fournisseur

Vous pouvez créer un utilisateur dans votre organisation de fournisseur vCloud Director.

Pendant l'installation et la configuration de vCloud Director, vous créez un compte d'**administrateur système**. Après la configuration initiale, vous pouvez créer des administrateurs et des utilisateurs supplémentaires dans l'organisation de fournisseur.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.
3. Cliquez sur **Nouveau**.
4. Entrez un nom d'utilisateur et un mot de passe pour le nouvel utilisateur.

   Le mot de passe doit contenir au moins six caractères.
5. Choisissez d'activer ou non l'utilisateur lors de la création.
6. Dans le menu déroulant **Rôles disponibles**, sélectionnez un rôle pour l'utilisateur.

   La liste des rôles disponibles comprend les rôles globaux et les rôles locaux propres à l'organisation de votre système.
7. (Facultatif) Entrez les informations de contact de l'utilisateur.

   Vous pouvez entrer le nom complet, l'adresse e-mail, le numéro de téléphone et l'ID de messagerie instantanée.
8. (Facultatif) Définissez les quotas de l'utilisateur.
   a. Vous pouvez définir une limite pour les machines virtuelles appartenant à l'utilisateur ou sélectionner l'option **Illimité**.
   b. Vous pouvez définir une limite pour les machines virtuelles en cours d'exécution appartenant à l'utilisateur ou sélectionner l'option **Illimité**.

Importer des utilisateurs de fournisseur

Vous pouvez importer des utilisateurs dans votre organisation de fournisseur vCloud Director à partir d'un fournisseur d'identité LDAP ou SAML précédemment configuré.

Conditions préalables

Configurer une connexion LDAP système ou Configurer votre système pour utiliser un fournisseur d'identité SAML.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.

3 Cliquez sur **Importer des utilisateurs**.

4 Dans le menu déroulant **Source**, sélectionnez le type de fournisseur d'identité.

Le type peut être **LDAP** ou **SAML**.

Si vous avez uniquement configuré un fournisseur d'identité, cette option est codée de manière irréversible.

5 Spécifiez des utilisateurs.

Option	Description
LDAP	a Entrez le nom complet ou partiel d'un utilisateur, puis cliquez sur **Rechercher**. b Dans les résultats de la recherche, sélectionnez les utilisateurs que vous souhaitez importer. c Dans le menu déroulant **Attribuer un rôle**, sélectionnez un rôle pour les utilisateurs importés.
SAML	a Entrez les noms d'utilisateur des utilisateurs que vous souhaitez importer au format d'identifiant de nom pris en charge par le fournisseur d'identité SAML. Utilisez une nouvelle ligne pour chaque nom d'utilisateur. b Dans le menu déroulant **Attribuer un rôle**, sélectionnez un rôle pour les utilisateurs importés.

6 Cliquez sur **Enregistrer**.

Résultats

Vous pouvez voir les utilisateurs importés dans la liste des utilisateurs.

Modifier un utilisateur de fournisseur

Vous pouvez modifier le mot de passe, le rôle, les informations de contact et les quotas d'un utilisateur dans votre organisation de fournisseur. Vous ne pouvez toutefois pas modifier le nom d'utilisateur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.

3 Cliquez sur le bouton radio en regard du nom de l'utilisateur cible, puis cliquez sur **Modifier**.

4 Modifiez les détails de l'utilisateur, puis cliquez sur **Enregistrer**.

Désactiver ou activer un utilisateur de fournisseur

Après avoir désactivé un utilisateur, celui-ci ne peut pas se connecter à vCloud Director.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.

3 Cliquez sur le bouton radio en regard du nom de l'utilisateur cible, puis sur **Désactiver** ou **Activer**.

4 Si vous désactivez un utilisateur, cliquez sur **OK** pour confirmer.

Supprimer un utilisateur de fournisseur

Vous pouvez supprimer un utilisateur de l'organisation de fournisseur vCloud Director en supprimant le compte d'utilisateur.

Conditions préalables

Désactivez l'utilisateur que vous souhaitez supprimer. Reportez-vous à Désactiver ou activer un utilisateur de fournisseur.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.

3 Cliquez sur le bouton radio en regard du nom de l'utilisateur cible, puis cliquez sur **Supprimer**.

4 Pour confirmer, cliquez sur **OK**.

Déverrouiller un utilisateur fournisseur

Si vous avez activé le verrouillage de compte dans vos paramètres système de stratégie de mot de passe, les utilisateurs peuvent verrouiller leurs comptes après un certain nombre de tentatives de connexion non valides. Même si le verrouillage est configuré avec un intervalle de verrouillage de compte, vous pouvez déverrouiller un compte d'utilisateur sans attendre l'expiration du verrou.

Pour plus d'informations sur la configuration de la stratégie de verrouillage de compte, reportez-vous à la section Configurer la stratégie de mot de passe.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Utilisateurs**.

3 Cliquez sur la case d'option en regard du nom de l'utilisateur cible et cliquez sur **Déverrouiller**.

Gestion des groupes de fournisseurs

Service Provider Admin Portalvous permet d'importer des groupes dans votre organisation de fournisseur, de les modifier et de les supprimer.

Pour plus d'informations sur la gestion des groupes dans les organisations, consultez le *Guide du portail de locataires de vCloud Director*.

importer un groupe de fournisseurs

Vous pouvez importer des groupes dans votre organisation de fournisseur vCloud Director à partir d'un fournisseur d'identité LDAP ou SAML précédemment configuré.

Conditions préalables

Configurer une connexion LDAP système ou Configurer votre système pour utiliser un fournisseur d'identité SAML.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Groupes**.
3. Cliquez sur **Importer des groupes**.
4. Dans le menu déroulant **Source**, sélectionnez le type de fournisseur d'identité.

   Le type peut être **LDAP** ou **SAML**.

   Si vous avez uniquement configuré un fournisseur d'identité, cette option est codée de manière irréversible.
5. Spécifiez des utilisateurs.

Option	Description
LDAP	a Entrez le nom complet ou partiel d'un groupe, puis cliquez sur **Rechercher**. b Dans les résultats de la recherche, sélectionnez les groupes que vous souhaitez importer. c Dans le menu déroulant **Attribuer un rôle**, sélectionnez un rôle pour les utilisateurs des groupes importés.
SAML	a Entrez les noms des groupes que vous souhaitez importer au format d'identifiant de nom pris en charge par le fournisseur d'identité SAML. Utilisez une nouvelle ligne pour chaque nom de groupe. b Dans le menu déroulant **Attribuer un rôle**, sélectionnez un rôle pour les utilisateurs des groupes importés.

6. Cliquez sur **Enregistrer**.

Modifier un groupe de fournisseurs

Vous pouvez modifier la description d'un groupe que vous avez précédemment importé dans votre organisation de fournisseur vCloud Director et modifier le rôle de ses membres.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Groupes**.
3. Cliquez sur le bouton radio en regard du nom du groupe cible, puis cliquez sur **Modifier**.
4. Modifiez les détails du groupe, puis cliquez sur **Enregistrer**.

Supprimer un groupe de fournisseurs

Vous pouvez supprimer un groupe de votre organisation de fournisseur vCloud Director.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès au fournisseur**, cliquez sur **Groupes**.
3. Cliquez sur le bouton radio en regard du nom du groupe cible, puis cliquez sur **Supprimer**.
4. Pour confirmer, cliquez sur **OK**.

Gestion de paramètres système 11

Un administrateur système de vCloud Director peut contrôler des paramètres associés à LDAP au niveau du système, la notification par e-mail, la gestion des licences et les préférences système générales.

Ce chapitre contient les rubriques suivantes :

- Modifier des paramètres système généraux
- Paramètres système généraux
- Configurer les paramètres de messagerie du système
- Modifier la licence vCloud Director
- Configurez les paramètres de synchronisation du catalogue.
- Configuration des tâches bloquantes et des notifications
- Configurer des adresses publiques
- Gestion des fournisseurs d'identité
- Gestion des plug-ins
- Personnalisation des portails vCloud Director
- Configurer la stratégie de mot de passe
- Configurer les services vSphere

Modifier des paramètres système généraux

vCloud Director inclut des paramètres système généraux liés aux journaux d'activité, à la mise en réseau, aux délais d'expiration de session, aux certificats, aux limites d'organisation, aux limites d'opérations, etc. Les paramètres par défaut conviennent à de nombreux environnements, mais vous pouvez les modifier pour les adapter à vos besoins.

Pour obtenir la liste des propriétés que vous pouvez modifier, reportez-vous à la section Paramètres système généraux.

Note Pour plus d'informations sur la modification de la date, de l'heure ou du fuseau horaire du dispositif vCloud Director, reportez-vous à la section https://kb.vmware.com/kb/59674.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Général**.
3. Cliquez sur **Modifier** pour la section que vous souhaitez modifier, modifiez les propriétés, puis cliquez sur **Enregistrer**.

Paramètres système généraux

vCloud Director inclut des paramètres système généraux que vous pouvez modifier selon vos besoins.

Tableau 11-1. Paramètres système généraux

Nom	Catégorie	Description
`Activity log history to keep`	Journal d'activité	Nombre de jours de conservation du journal d'activité avant sa suppression. Entrez `0` pour ne jamais supprimer les journaux.
`Activity log history shown`	Journal d'activité	Nombre de jours d'affichage du journal d'activité. Entrez `0` pour afficher toutes les activités.
`Display debug information`	Journal d'activité	Activez ce paramètre pour afficher des informations de débogage dans le journal des tâches de vCloud Director.
`IP address release timeout`	Mise en réseau	Nombre de secondes pendant lesquelles retenir les adresses IP libérées avant de pouvoir les réaffecter. Ce paramètre par défaut est de 2 heures (7 200 secondes) pour permettre aux anciennes entrées d'expirer dans les tables ARP du client.
`Allow Overlapping External Networks`	Mise en réseau	Pour ajouter des réseaux externes qui s'exécutent sur le même segment de réseau, cochez cette case. Activez ce paramètre uniquement si vous n'utilisez pas de méthodes VLAN pour isoler les réseaux externes.
`Allow FIPS mode`	Mise en réseau	Permet l'activation du mode FIPS sur les passerelles Edge. Nécessite NSX 6.3 ou une version ultérieure. Consultez Mode FIPS dans la documentation *VMware NSX for vSphere*.
`Default syslog server settings for networks`	Mise en réseau	Entrez les adresses IP de deux serveurs Syslog au maximum à utiliser pour les réseaux. Ce paramètre ne s'applique pas aux serveurs Syslog utilisés par les cellules du Cloud.

Tableau 11-1. Paramètres système généraux (suite)

Nom	Catégorie	Description
Provider Locale	Localisation	Sélectionnez un lieu concernant l'activité du fournisseur, y compris des entrées de journal, des e-mails d'alerte, etc.
Idle session timeout	Délais d'expiration	Durée pendant laquelle l'application vCloud Director demeure active sans interaction avec l'utilisateur.
Maximum session timeout	Délais d'expiration	Durée maximale pendant laquelle l'application vCloud Director demeure active.
Host refresh frequency	Délais d'expiration	Fréquence à laquelle vCloud Director vérifie si ses hôtes ESXi sont accessibles ou inaccessibles.
Host hung timeout	Délais d'expiration	Sélectionnez la durée d'attente avant d'indiquer un hôte comme interrompu.
Transfer session timeout	Délais d'expiration	Délai d'attente avant l'échec d'une tâche de transfert suspendue ou annulée, par exemple le transfert d'un support ou d'un modèle de vApp. Le délai d'expiration ne concerne pas les tâches de transfert en cours.
Enable upload quarantine with a timeout of __ seconds	Délais d'expiration	Cochez cette case et saisissez un délai d'expiration correspondant à la durée de mise en quarantaine des fichiers transférés.
Verify vCenter and vSphere SSO certificates	Certificats	Cochez cette case pour permettre à vCloud Director de communiquer uniquement avec des serveurs vCenter approuvés. Cliquez sur **Parcourir** pour localiser un keystore JCEKS et entrez le mot de passe du keystore.
Verify NSX Manager certificates	Certificats	Pour permettre à vCloud Director de communiquer uniquement avec des instances de NSX Manager approuvées, cochez cette case. Cliquez sur **Parcourir** pour localiser un keystore JCEKS et entrez le mot de passe du keystore.
Edit Organization Limits	Limites du VDC d'organisation	Entrez le nombre maximal de centres de données virtuels d'organisation par organisation ou sélectionnez **Illimité**.
Number of resource intensive operations running per user	Limites des opérations	Entrez le nombre maximal d'opérations simultanées exigeantes en ressources par utilisateur ou sélectionnez **Illimité**.
Number of resource intensive operations to be queued per user (in addition to running)	Limites des opérations	Entrez le nombre maximal d'opérations exigeantes en ressources à mettre en file d'attente par utilisateur ou sélectionnez **Illimité**.
Number of resource intensive operations running per organization	Limites des opérations	Entrez le nombre maximal d'opérations simultanées exigeantes en ressources par organisation ou sélectionnez **Illimité**.
Number of resource intensive operations to be queued per organization	Limites des opérations	Entrez le nombre maximal d'opérations exigeantes en ressources à mettre en file d'attente par organisation ou sélectionnez **Illimité**.

Tableau 11-1. Paramètres système généraux (suite)

Nom	Catégorie	Description
`Provide default vApp names`	Autre	Cochez cette case pour configurer vCloud Director afin qu'il fournisse des noms par défaut pour les nouveaux vApp.
`Make Allocation pool Org VDCs elastic`	Autre	Cochez cette case pour activer un pool d'allocations élastique, rendant tous les centres de données virtuels d'organisation à pool d'allocation élastiques. Avant de décocher cette option, assurez-vous que toutes les machines virtuelles de chaque centre de données virtuel d'organisation ont été migrées vers un seul cluster.
`VM discovery enabled`	Autre	Par défaut, chaque VDC d'organisation découvre automatiquement les machines virtuelles de vCenter qui ont été créées sur un pool de ressources soutenant le VDC. Décochez cette case pour désactiver ce paramètre pour tous les VDC du système.

Configurer les paramètres de messagerie du système

Vous pouvez modifier les paramètres de messagerie du système, y compris la configuration des paramètres du serveur SMTP et des paramètres de notification vCloud Director.

vCloud Director nécessite un serveur SMTP pour envoyer des e-mails de notification d'utilisateur et d'alerte système aux utilisateurs système.

vCloud Director envoie des e-mails d'alerte système lorsque le programme doit communiquer des informations importantes. Par exemple, vCloud Director envoie une alerte lorsqu'une banque de données commence à manquer d'espace. Vous pouvez configurer vCloud Director de manière à envoyer des e-mails d'alerte à tous les administrateurs système ou à une liste d'adresses e-mail spécifiques.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le volet de gauche, sous **Paramètres**, sélectionnez **E-mail**, puis cliquez sur **Modifier**.
3. Entrez le nom d'hôte DNS ou l'adresse IP du serveur de messagerie SMTP.
4. Entrez le numéro de port du serveur SMTP.
5. (Facultatif) Si le serveur SMTP exige un nom d'utilisateur, activez l'option **Authentification requise** et entrez le nom d'utilisateur et le mot de passe du compte SMTP.
6. Sélectionnez l'onglet **Paramètres de notification**.
7. Entrez une adresse e-mail devant s'afficher comme expéditeur des e-mails vCloud Director.

   vCloud Director utilise l'adresse e-mail de l'expéditeur pour envoyer des alertes d'exécution et d'expiration de bail de stockage.

8 (Facultatif) Entrez le texte du préfixe de l'objet.

9 Sélectionnez les destinataires des notifications.

Par défaut, seuls les administrateurs d'organisation reçoivent les notifications SMTP.

10 Cliquez sur **Enregistrer**.

11 (Facultatif) Testez les paramètres SMTP.

a Cliquez sur **Tester**.

b Si vous avez activé l'option **Authentification requise**, entrez le mot de passe du serveur SMTP.

c Entrez une adresse e-mail de destination et cliquez sur **Tester**.

Modifier la licence vCloud Director

vCloud Director nécessite une licence valide, spécifiée en tant que numéro de série, pour son exécution. Vous pouvez modifier les informations de licence que vous avez entrées lors de la configuration initiale de vCloud Director.

Le numéro de série du produit vCloud Director est différent de la clé de licence de vCenter Server. Vous pouvez obtenir un numéro de série vCloud Director depuis le portail de licence VMware.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le volet de gauche, sélectionnez **Licence** et cliquez sur **Modifier**.

3 Entrez un nouveau numéro de série et cliquez sur **Enregistrer**.

Configurez les paramètres de synchronisation du catalogue.

Vous pouvez modifier les paramètres de synchronisation du catalogue pour toutes les organisations et tous les catalogues, y compris la fréquence d'actualisation des abonnements au catalogue.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le volet de gauche, sous **Paramètres**, sélectionnez **Catalogue**.

3 Cliquez sur **Modifier**.

4 Activez la synchronisation du catalogue.

5 Définissez les temps de démarrage et d'arrêt de la synchronisation.

6 Définissez l'intervalle de synchronisation.

   L'intervalle de synchronisation est la fréquence d'actualisation des abonnements au catalogue.

7 Cliquez sur **Enregistrer**.

Étape suivante

Pour plus d'informations sur la configuration de la limitation de la synchronisation du catalogue, consultez le *Guide d'installation, de configuration et de mise à niveau de vCloud Director*.

Configuration des tâches bloquantes et des notifications

Vous pouvez utiliser des tâches bloquantes et des notifications pour configurer vCloud Director afin d'envoyer des messages AMQP déclenchés par certains événements.

Certains messages notifient simplement que l'événement s'est produit. D'autres messages publient des informations à un point de terminaison AMQP désigné indiquant qu'une action demandée a été bloquée et attend une action par une application cliente liée à ce point de terminaison. Ces messages sont des tâches bloquantes.

Un **administrateur système** peut configurer un ensemble de tâches bloquantes à l'échelle du système soumises à une action programmée par un client AMQP.

Configurer un Broker AMQP

Si vous souhaitez que vCloud Director envoie des messages AMQP déclenchés par certains événements, vous devez configurer un Broker AMQP. Vous pouvez utiliser les messages AMQP pour automatiser le traitement d'une demande d'utilisateur sous-jacente.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans **Paramètres**, sélectionnez **Extensibilité**.

   L'onglet **Broker AMQP** s'ouvre.

3 Cliquez sur le bouton **Modifier** de la section **Broker AMQP**.

4 Entrez le nom d'hôte DNS ou l'adresse IP de l'hôte AMQP.

   Le nom de domaine complet de l'hôte du serveur RabbitMQ, par exemple *amqp.example.com*.

5 Entrez le port AMQP.

   Le port par défaut sur lequel le Broker écoute les messages est 5672.

6 Entrez l'échange.

7 Entrez l'instance de vHost.

   La valeur par défaut est /.

8 Entrez le préfixe.

9 (Facultatif) Pour utiliser SSL, activez le bouton bascule **Utiliser SSL** et sélectionnez l'une des options de certificat.

   Par défaut, le service AMQP de vCloud Director envoie des messages non chiffrés. Vous pouvez configurer le service AMQP pour chiffrer ces messages en utilisant SSL. Vous pouvez également configurer le service afin de vérifier le certificat du Broker à l'aide du magasin d'approbations JCEKS par défaut de l'environnement d'exécution Java sur la cellule VMware Cloud Director, généralement situé dans `$VCLOUD_HOME/jre/lib/security/cacerts`.

Option	Description
Accepter tous les certificats	L'enregistrement CN dans le champ du propriétaire de certificat doit correspondre au nom d'hôte du courtier AMQP. Pour utiliser des certificats qui ne correspondent pas au nom d'hôte du Broker, activez le bouton bascule **Accepter tous les certificats**.
Certificat SSL	Téléchargez le certificat SSL.
Keystore SSL (JCEKS)	Téléchargez le keystore SSL et entrez le mot de passe du keystore.

10 Entrez un nom d'utilisateur et un mot de passe pour vous connecter à l'hôte AMQP.

11 Cliquez sur **Enregistrer**.

12 (Facultatif) Pour tester les paramètres, cliquez sur le bouton **Tester** sous la section **Broker AMQP** et fournissez le mot de passe.

13 (Facultatif) Pour publier des événements d'audit sur le Broker AMQP, cliquez sur le bouton **Modifier** sous la section **Notifications AMQP non bloquantes** et activez le bouton bascule **Activer les notifications**.

Configurer les paramètres des tâches bloquantes

Vous pouvez configurer certaines opérations en tant que tâches bloquantes. Ces opérations sont interrompues jusqu'à ce qu'un **administrateur système** prenne des mesures ou qu'un délai d'attente préconfiguré expire. Vous pouvez spécifier les paramètres du délai d'attente et les actions par défaut des tâches bloquantes. Les paramètres s'appliquent à toutes les organisations dans l'installation.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans **Paramètres**, sélectionnez **Extensibilité**.

3 Sélectionnez l'onglet **Tâches bloquantes**.

4 Pour modifier le délai d'expiration de l'extension par défaut et l'action de délai d'expiration par défaut, cliquez sur le bouton **Modifier** sous la section **Général**.

   a Modifiez le **Délai d'expiration de tâche bloquante par défaut**.

   b Modifiez l'**Action de délai d'expiration par défaut**.

      L'**Action de délai d'expiration par défaut** est l'action après l'expiration d'un **Délai d'expiration de tâche bloquant par défaut**.

   c Cliquez sur **Enregistrer**.

5 Pour modifier la liste des opérations, considérées comme tâches bloquantes, cliquez sur le bouton **Modifier** sous la section **Opérations**.

   a Sélectionnez ou désélectionnez des opérations dans la liste des tâches bloquantes.

   b Cliquez sur **Enregistrer**.

Configurer des adresses publiques

Pour répondre aux conditions requises en matière d'équilibrage de charge ou de proxy, vous pouvez modifier les adresses Web du point de terminaison par défaut pour le portail Web de vCloud Director, l'API vCloud Director et le proxy de console.

Les adresses publiques sont des adresses Web exposées aux clients de vCloud Director. Les valeurs par défaut de ces adresses sont spécifiées pendant l'installation. Si nécessaire, vous pouvez mettre à jour les adresses.

Si vCloud Director se compose d'une cellule unique, le programme d'installation crée des points de terminaison publics qui fournissent généralement un accès suffisant pour les clients d'API et Web. Les installations et les déploiements qui incluent plusieurs cellules placent généralement un équilibrage de charge entre les cellules et les clients. Les clients accèdent au système à l'adresse de l'équilibrage de charge. L'équilibrage de charge distribue les demandes des clients entre les cellules disponibles. Les autres configurations réseau qui incluent un serveur proxy ou placent les cellules dans une zone DMZ nécessitent également des points de terminaison personnalisés. Les détails des URL de point de terminaison sont spécifiques à votre configuration réseau.

Les points de terminaison de vCloud Director Tenant Portal et la console Web de vCloud Director nécessitent des certificats SSL, de préférence signés. Vous devez spécifier un chemin d'accès à ces certificats lorsque vous installez ou déployez vCloud Director. Si vous personnalisez l'un de ces points de terminaison après l'installation ou le déploiement, vous devrez peut-être installer de nouveaux certificats qui correspondent à des détails des points de terminaison tels que `hostname` et `subject alternative name`.

Pour le dispositif vCloud Director, vous devez configurer l'adresse proxy de console publique vCloud Director, car le dispositif utilise une adresse IP unique avec le port personnalisé `8443` pour le service de proxy de console. Reportez-vous à Étape 6.

Conditions préalables

Vérifiez que vous êtes connecté en tant qu'**administrateur système**. Seul un **administrateur système** peut personnaliser les points de terminaison publics.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Adresses publiques**.
3. Pour personnaliser les points de terminaison publics, cliquez sur **Modifier**.
4. Pour personnaliser les URL vCloud Director, modifiez les points de terminaison du **portail Web**.
   a. Entrez une URL publique vCloud Director personnalisée pour les connexions HTTP (non sécurisées).
   b. Entrez une URL publique vCloud Director personnalisée pour les connexions HTTPS (sécurisées) et cliquez sur **Télécharger** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

      La chaîne de certificats doit correspondre au certificat utilisé par le point de terminaison de service, qui est le certificat téléchargé vers chaque keystore de cellule vCloud Director avec l'alias `consoleproxy`. Les terminaisons SSL des connexions de proxy de console sur un équilibrage de charge ne sont pas prises en charge. La chaîne de certificats doit inclure un certificat de point de terminaison, des certificats intermédiaires et un certificat racine au format `PEM` sans clé privée.

5 (Facultatif) Pour personnaliser les URL REST API et OpenAPI de Cloud Director, désactivez le bouton bascule **Utiliser les paramètres de portail Web**.

   a Entrez une URL de base HTTP personnalisée.

   Par exemple, si vous définissez l'URL de base HTTP sur **http://vcloud.example.com**, vous pouvez accéder à l'API vCloud Director à l'adresse `http://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI vCloud Director à l'adresse `http://vcloud.example.com/cloudapi`.

   b Entrez une URL de base HTTPS personnalisée pour l'API REST et cliquez sur **Télécharger** pour télécharger les certificats qui établissent la chaîne d'approbation pour ce point de terminaison.

   Par exemple, si vous définissez l'URL de base HTTPS de REST API sur **https://vcloud.example.com**, vous pouvez accéder à l'API vCloud Director à l'adresse `https://vcloud.example.com/api`, et vous pouvez accéder à l'OpenAPI vCloud Director à l'adresse `https://vcloud.example.com/cloudapi`.

   La chaîne de certificats doit correspondre au certificat utilisé par le point de terminaison de service, qui est le certificat téléchargé vers chaque keystore de la cellule vCloud Director avec l'alias `http` ou le certificat VIP de l'équilibrage de charge si une terminaison SSL est utilisée. La chaîne de certificats doit inclure un certificat de point de terminaison, des certificats intermédiaires et un certificat racine au format `PEM` sans clé privée.

6 Entrez une adresse proxy de console publique vCloud Director personnalisée.

   - Personnalisez l'adresse proxy de la console publique du dispositif vCloud Director.

     Cette adresse est le nom de domaine complet (FQDN) de la carte réseau `eth0` du dispositif vCloud Director, spécifiée par le nom de domaine complet ou l'adresse IP, avec le port personnalisé `8443` pour le service de proxy de la console.

   - Personnalisez l'adresse proxy de la console publique de vCloud Director sur Linux.

     Cette adresse est le nom de domaine complet (FQDN) du serveur vCloud Director ou de l'équilibrage de charge avec le numéro de port. Le port par défaut est `443`.

   Par exemple, pour une instance de dispositif vCloud Director ayant le nom de domaine complet `vcloud.example.com`, entrez **vcloud.example.com:8443**.

   vCloud Director utilise l'adresse proxy de la console lors de l'ouverture d'une fenêtre de console distante sur une machine virtuelle.

7 Cliquez sur **Enregistrer**.

Gestion des fournisseurs d'identité

Vous pouvez intégrer votre cloud à un fournisseur d'identité externe et importer des utilisateurs et des groupes dans vos organisations. Vous pouvez configurer une connexion au serveur LDAP au niveau du système ou de l'organisation. Vous pouvez configurer une intégration SAML au niveau de l'organisation.

Gestion des connexions LDAP

En tant qu'administrateur système, vous pouvez configurer votre organisation système vCloud Director et n'importe quelle autre organisation dans le système afin qu'elles utilisent un serveur LDAP en tant que source d'utilisateurs et de groupes. Les organisations peuvent utiliser la connexion LDAP système ou une connexion LDAP privée.

Configurer une connexion LDAP système

Pour fournir à vCloud Director et à ses organisations un accès partagé à des utilisateurs et des groupes, vous pouvez configurer une connexion LDAP au niveau du système.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le panneau de gauche, sous **Fournisseurs d'identité**, cliquez sur **LDAP**.

Les paramètres LDAP actuels sont affichés.

Étape suivante

Configurer, tester et synchroniser une connexion LDAP.

Configurer une connexion LDAP d'organisation

Vous pouvez configurer une organisation pour utiliser une connexion LDAP système comme source partagée d'utilisateurs et de groupes. Vous pouvez configurer une organisation pour utiliser une connexion LDAP distincte comme source privée d'utilisateurs et de groupes.

Procédure

1 Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.

2 Dans le panneau de gauche, cliquez sur **Organisations**.

3 Cliquez sur le nom de l'organisation cible.

Vous êtes redirigé vers le portail de locataires de vCloud Director de l'organisation.

4 Dans le menu principal (☰), sélectionnez **Administration**.

5 Dans le panneau de gauche, sous **Fournisseurs d'identité**, cliquez sur **LDAP**.

Les paramètres LDAP actuels sont affichés.

6 Sous l'onglet **Options LDAP**, cliquez sur **Modifier**.

7 Configurez la source LDAP des utilisateurs et des groupes pour cette organisation, puis cliquez sur **Enregistrer**.

Option	Description
Ne pas utiliser LDAP	L'organisation n'utilise pas de serveur LDAP en tant que source d'utilisateurs et de groupes d'organisation.
Service LDAP du système vCD	L'organisation utilise la connexion LDAP du système vCloud Director que vous avez configurée précédemment. Reportez-vous à Configurer une connexion LDAP système.
Service LDAP personnalisé	L'organisation utilise un serveur LDAP privé comme source d'utilisateurs et de groupes d'organisation. Cliquez sur l'onglet **LDAP personnalisé** et suivez la procédure décrite dans la section Configurer, tester et synchroniser une connexion LDAP.

Configurer, tester et synchroniser une connexion LDAP

Pour configurer une connexion LDAP système ou d'organisation, vous définissez les détails de votre serveur LDAP. Vous pouvez tester la connexion pour vous assurer que vous avez entré les paramètres appropriés et que les attributs d'utilisateur et de groupe sont correctement mappés. Lorsqu'une connexion LDAP est établie, vous pouvez synchroniser vCloud Director et le serveur LDAP à tout moment.

Conditions préalables

Si vous prévoyez de vous connecter à un serveur LDAPS, vérifiez que vous disposez d'un certificat conçu pour la prise en charge LDAP améliorée dans Java 8 Update 181. Pour plus d'informations, consultez les *Modifications de version de Java 8* sur https://www.java.com.

Procédure

1 Sous l'onglet **Connexion**, entrez les informations requises pour la connexion LDAP.

Informations requises	Description
Serveur	Nom d'hôte ou adresse IP du serveur LDAP.
Port	Numéro de port sur lequel le serveur LDAP effectue ses écoutes. Pour LDAP, le numéro de port par défaut est 389. Pour LDAPS, le numéro de port par défaut est 636.

Informations requises	Description
Nom unique de base	Le nom unique de base (DN) est l'emplacement dans l'annuaire LDAP que vCloud Director utilise pour la connexion. Pour vous connecter à la racine, entrez uniquement les composants de domaine. Par exemple, **DC=example,DC=com**. Pour vous connecter à un nœud dans l'arborescence, entrez le nom unique de ce nœud. Par exemple, **OU=ServiceDirector,DC=example,DC=com**. La connexion à un nœud limite la portée de l'annuaire disponible pour vCloud Director.
Type de connecteur	Type du serveur LDAP. Il peut s'agir d'**Active Directory** ou d'**OpenLDAP**.
Utiliser SSL	Si votre serveur est LDAPS, cochez cette case.
Accepter tous les certificats	Si votre serveur est LDAPS, cochez cette case ou téléchargez le certificat SSL LDAP.
Truststore personnalisé	Si votre serveur est LDAPS, cliquez sur l'icône de téléchargement ( ) et importez un certificat SSL LDAP, ou sélectionnez **Accepter tous les certificats**.
Méthode d'authentification	L'authentification simple consiste à envoyer le nom distinct et le mot de passe de l'utilisateur au serveur LDAP. Si vous utilisez LDAP, le mot de passe LDAP est transmis sur le réseau en texte clair. Si vous souhaitez utiliser Kerberos, vous devez configurer la connexion LDAP à l'aide de vCloud API.
Nom d'utilisateur	Nom d'utilisateur unique LDAP complet pour la connexion au serveur LDAP. Si la prise en charge de la lecture anonyme est activée sur votre serveur LDAP, vous pouvez laisser ces zones de texte vierges.
Mot de passe	Mot de passe pour la connexion au serveur LDAP. Si la prise en charge de la lecture anonyme est activée sur votre serveur LDAP, vous pouvez laisser ces zones de texte vierges.

2 Cliquez sur l'onglet **Attributs des utilisateurs**, examinez les valeurs par défaut pour les attributs utilisateur et, si votre annuaire LDAP utilise un schéma différent, modifiez les valeurs.

3 Cliquez sur l'onglet **Attributs des groupes**, examinez les valeurs par défaut pour les attributs des groupes et, si votre annuaire LDAP utilise un schéma différent, modifiez les valeurs.

4 Cliquez sur **Enregistrer**.

5 Pour tester les paramètres de connexion LDAP et les mappages d'attributs LDAP :

   a Cliquez sur **Tester**.

   b Entrez le mot de passe de l'utilisateur du serveur LDAP que vous avez configuré et cliquez sur **Tester**.

      Si la connexion est établie, une coche verte s'affiche.

      Les valeurs d'attribut utilisateur et de groupe récupérées sont affichées dans une table. Celles qui sont correctement mappées aux attributs LDAP sont indiquées par des coches vertes. Les valeurs qui ne sont pas mappées aux attributs LDAP sont vides et indiquées par des points d'exclamation rouges.

   c Pour quitter la fenêtre active, cliquez sur **Annuler**.

6 Pour synchroniser vCloud Director et le serveur LDAP configuré, cliquez sur **Synchroniser**.

   vCloud Director synchronise les informations de groupe et d'utilisateur avec le serveur LDAP régulièrement selon l'intervalle de synchronisation défini dans les paramètres généraux du système.

   Patientez quelques minutes jusqu'à la fin de la synchronisation.

Résultats

Vous pouvez désormais importer des utilisateurs et des groupes à partir du serveur LDAP récemment configuré.

Configurer votre système pour utiliser un fournisseur d'identité SAML

Si vous souhaitez importer des utilisateurs et des groupes à partir d'un fournisseur d'identité SAML vers votre organisation système, vous devez configurer celle-ci avec ce fournisseur d'identité SAML. Les utilisateurs importés peuvent se connecter à l'organisation système avec les informations d'identification établies dans le fournisseur d'identité SAML.

Pour configurer vCloud Director avec un fournisseur d'identité SAML, vous établissez une approbation mutuelle en échangeant les métadonnées du fournisseur de services SAML et celles du fournisseur d'identité.

Lorsqu'un utilisateur importé tente de se connecter, le système extrait les attributs suivants du jeton SAML, le cas échéant, et les utilise pour interpréter les informations correspondant à l'utilisateur.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"` (Cet attribut est configurable.)

Les informations sur le groupe sont utilisées si l'utilisateur n'est pas importé directement, mais doit se connecter en raison de son appartenance aux groupes importés. Un utilisateur peut appartenir à plusieurs groupes, donc avoir plusieurs rôles pendant une session.

Si un utilisateur importé ou un groupe est affecté au rôle Différer vers le fournisseur d'identité, les rôles sont affectés en fonction des informations collectées à partir de l'attribut Roles dans le jeton. Si un autre attribut est utilisé, ce nom d'attribut peut être configuré uniquement à l'aide de l'API et seul l'attribut Roles est configurable. Si le rôle Différer vers le fournisseur d'identité est utilisé, mais qu'aucune information de rôle ne peut être extraite, l'utilisateur peut se connecter, mais ne dispose d'aucun droit pour effectuer des activités.

Conditions préalables

- Vérifiez que vous avez accès à un fournisseur d'identité compatible SAML 2.0.
- Obtenez un fichier XML avec les métadonnées suivantes à partir de votre fournisseur d'identité SAML.
  - L'emplacement du service single sign-on
  - L'emplacement du service single logout
  - L'emplacement du certificat X.509 du service

  Pour plus d'informations sur la configuration et l'acquisition des métadonnées depuis un fournisseur SAML, consultez la documentation de votre fournisseur SAML.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous Fournisseurs d'identité, cliquez sur **SAML**, puis sur **Modifier**.

   Les paramètres SAML actuels sont affichés.

3 Sous l'onglet **Fournisseur de services**, téléchargez les métadonnées de fournisseur de services SAML vCloud Director.

   a Entrez un ID d'entité pour l'organisation système.

   L'ID d'entité identifie de manière unique votre organisation système auprès du fournisseur d'identité.

   b Examinez la date d'expiration du certificat et, si la date d'expiration est proche, regénérez le certificat en cliquant sur **Générer de nouveau**.

   Le certificat est inclus dans les métadonnées SAML, et est utilisé pour le chiffrement et la signature. Une de ces opérations ou les deux peuvent être nécessaires en fonction du mode d'approbation établi entre votre organisation et votre fournisseur d'identité SAML.

   c Cliquez sur le lien **Métadonnées**.

   Le lien est semblable à `https://`*`nom_hôte_VCD`*`/cloud/org/System/saml/metadata/alias/vcd`.

   Votre navigateur télécharge les métadonnées du fournisseur de services SAML sous la forme d'un fichier XML que vous devez fournir à votre fournisseur d'identité.

4 Dans l'onglet **Fournisseur d'identité**, téléchargez les métadonnées SAML que vous avez précédemment reçues de votre fournisseur d'identité.

   a Sélectionnez **Utiliser le fournisseur d'identité SAML**.

   b Cliquez sur l'icône **Parcourir** ( ) et téléchargez le fichier, ou copiez et collez son contenu dans la zone de texte **XML de métadonnées**.

5 Cliquez sur **Enregistrer**.

Résultats

Gestion des plug-ins

Les plug-ins vCloud Director étendent les fonctions du Service Provider Admin Portal et du vCloud Director Tenant Portal. Vous pouvez télécharger, désactiver et supprimer des plug-ins à partir du Service Provider Admin Portal. Vous pouvez publier un plug-in au niveau du fournisseur de services et des organisations individuelles.

Certains plug-ins sont installés dans le cadre de vCloud Director.

Extension CPOM

Offre la possibilité d'afficher et de gérer des instances dédiées et des serveurs proxy de vCenter Server à l'aide de vCloud Director Tenant Portal.

Personnaliser le portail

Offre la possibilité de personnaliser le vCloud Director Service Provider Admin Portal et le vCloud Director Tenant Portal.

vCloud Availability

Le plug-in VMware vCloud® Availability™ permet d'accéder à vCloud Availability Portal directement à partir de l'interface utilisateur de vCloud Director. Pour plus d'informations, consultez la Documentation vCloud Availability.

Télécharger un plug-in

Vous pouvez télécharger des plug-ins supplémentaires sur vCloud Director Service Provider Admin Portal pour une utilisation par le fournisseur de services et les organisations du cloud.

Conditions préalables

Téléchargez le fichier d'installation du plug-in.

Procédure

1. Dans le menu principal (☰), sélectionnez **Personnaliser le portail**.
2. Cliquez sur **Télécharger**.
3. Cliquez sur **Sélectionner le fichier de plug-in**, accédez au fichier d'installation cible, puis cliquez sur **Ouvrir**.
4. Cliquez sur **Suivant**.
5. Sélectionnez la portée de ce plug-in.

Option	Description
Fournisseurs de services	La fonction du plug-in devient disponible dans vCloud Director Service Provider Admin Portal.
Locataires	La fonction du plug-in devient disponible dans vCloud Director Service Provider Admin Portal des organisations que vous sélectionnez.

6. Si vous avez définit la portée du plug-in aux locataires, sélectionnez les organisations auxquelles vous souhaitez publier ce plug-in.
7. Vérifiez la page **Vérifier et terminer**, puis cliquez **Terminer**.

Activer ou désactiver un plug-in

Pour empêcher toutes les organisations d'utiliser un plug-in, vous pouvez désactiver ce plug-in.

Procédure

1. Dans le menu principal (☰), sélectionnez **Personnaliser le portail**.
2. Sélectionnez le bouton radio situé en regard du nom des plug-ins cibles, puis cliquez sur **Activer** ou **Désactiver**.

Supprimer un plug-in

Vous pouvez supprimer un ou plusieurs plug-ins du vCloud Director Service Provider Admin Portal.

Procédure

1. Dans le menu principal (☰), sélectionnez **Personnaliser le portail**.
2. Cochez les cases situées en regard du nom des plug-ins à supprimer, puis cliquez sur **Supprimer**.
3. Pour confirmer, cliquez sur **Enregistrer**.

Publier ou annuler la publication d'un plug-in d'une organisation

Vous pouvez modifier l'ensemble d'organisations qui peuvent utiliser la fonction fournie par un plug-in.

Vous pouvez modifier l'ensemble d'organisations pour plusieurs plug-ins.

Procédure

1. Dans le menu principal (☰), sélectionnez **Personnaliser le portail**.
2. Cochez les cases situées en regard des noms des plug-ins cibles, puis cliquez sur **Publier**.
3. Sélectionnez l'étendue de ce plug-in.

Option	Description
Fournisseurs de services	La fonction de plug-in devient disponible dans le vCloud Director Service Provider Admin Portal.
Locataires	La fonction de plug-in devient disponible dans le vCloud Director Service Provider Admin Portal des organisations que vous sélectionnez.

4. Si vous avez étendu le plug-in aux locataires, sélectionnez les organisations au niveau desquelles vous souhaitez publier ce plug-in.
5. Cliquez sur **Enregistrer**.

Personnalisation des portails vCloud Director

Pour associer vos normes de marque d'entreprise et créer une expérience Cloud entièrement personnalisée, vous pouvez définir le logo et le thème de votre vCloud Director Service Provider Admin Portal et du vCloud Director Tenant Portal de chaque organisation. En outre, vous pouvez

modifier et ajouter des liens personnalisés dans les deux menus situés en haut à droite sur les portails vCloud Director.

Note Pour personnaliser vos attributs et vos liens de marque, vous devez utiliser les méthodes `branding` vCloud OpenAPI. Reportez-vous à *Démarrage de vCloud OpenAPI* sur https://code.vmware.com.

Informations de marque du portail

Dans le cadre de l'installation, vCloud Director contient deux thèmes : un thème par défaut et un thème sombre. Vous pouvez créer, gérer et appliquer des thèmes personnalisés. En outre, vous pouvez modifier le nom du portail, le logo et l'icône du navigateur. En outre, le titre du navigateur adopte le nom du portail que vous avez défini.

Vous définissez les attributs de marque au niveau du système, afin de personnaliser le vCloud Director Service Provider Admin Portal. Le vCloud Director Tenant Portal de chaque organisation adopte les attributs de marque du système, sauf si vous avez configuré des attributs de marque pour le locataire particulier.

Pour un locataire particulier, vous pouvez remplacer de manière sélective n'importe quelle combinaison du nom du portail, de la couleur d'arrière-plan, du logo, de l'icône, du thème et des liens personnalisés. Une valeur que vous ne définissez pas utilise la valeur par défaut du système correspondante.

Note Par défaut, la marque de locataire spécifique n'est pas affichée en dehors d'une session ouverte. La marque de locataire spécifique ne s'affiche pas sur les pages de connexion et de déconnexion, afin que les locataires ne puissent pas découvrir l'existence d'autres locataires. Vous pouvez activer la marque en dehors des sessions ouvertes à l'aide de l'outil de gestion des cellules :

```
manage-config -n backend.branding.requireAuthForBranding -v false
```

Pour plus d'informations sur l'utilisation de l'outil de gestion des cellules, reportez-vous au *Guide d'installation, de configuration et de mise à niveau de vCloud Director*.

Liens personnalisés

Les liens personnalisés sont un composant de la marque du portail. Il existe deux types de liens personnalisés :

- Les éléments de menu `override` remplacent les liens existants pour les éléments de menu **Aide**, **À propos de** et **Télécharger VMRC**. Par défaut, **Télécharger VMRC** redirige les utilisateurs vers https://my.vmware.com pour télécharger VMRC, ce qui nécessite que les utilisateurs disposent de comptes enregistrés pour le téléchargement. En remplaçant ce lien, vous pouvez déplacer le programme d'installation de VMRC vers votre propre serveur.

- Les éléments de menu `link` sont de nouveaux liens que vous ajoutez à votre élément de menu **Se déconnecter** dans le coin supérieur droit du portail. Les nouveaux liens personnalisés s'affichent dans l'ordre indiqué dans l'appel d'API.

  Vous pouvez organiser ces liens personnalisés à l'aide des éléments de menu `section` et `separator`. Un élément de menu `section` ajoute un en-tête au menu, et un élément de menu `separator` lui ajoute une ligne.

Les liens personnalisés prennent en charge les variables personnalisées, que vous pouvez utiliser pour transmettre des informations d'identification à d'autres applications sous la forme de paramètres de requête.

vCloud Director prend en charge les variables personnalisées suivantes dans la valeur `url` pour un lien personnalisé :

Tableau 11-2. Variables personnalisées pour les liens personnalisés

Variable	Description
`${TENANT_NAME}`	Nom de l'organisation
`${TENANT_ID}`	ID de l'organisation
`${SESSION_TOKEN}`	Jeton x-vcloud-authorization

Par exemple,

```
url: https://host:port/tenant/${TENANT_NAME}/vdcs
```

dans le vCloud Director Tenant Portal pour l'organisation, myorg est converti vers :

```
url: https://host:port/tenant/myorg/vdcs
```

Configurer la stratégie de mot de passe

Pour empêcher un utilisateur de se connecter à vCloud Director après un certain nombre de tentatives infructueuses, vous pouvez activer le verrouillage de compte.

Les modifications apportées à la politique de verrouillage de compte système s'appliquent à toutes les nouvelles organisations. Les organisations créées avant la modification de la politique de verrouillage de compte doivent être modifiées au niveau de l'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Paramètres**, cliquez sur **Stratégie de mot de passe**.
3. Cliquez sur **Modifier**.
4. Pour activer le verrouillage de compte, activez **Verrouillage de compte**.

5 Sélectionnez le nombre de tentatives de connexion non valides acceptées avant le verrouillage d'un compte.

6 Sélectionnez l'intervalle de verrouillage.

7 Pour activer le verrouillage du compte **Administrateur système**, activez l'option **Le compte Administrateur système peut être verrouillé**.

8 Cliquez sur **Enregistrer**.

Configurer les services vSphere

Vous pouvez configurer et activer vCloud Director pour utiliser vCenter Single Sign-On afin que le fournisseur d'identité vSphere authentifie les administrateurs système.

vCenter Lookup Service contient des informations de topologie sur l'infrastructure vSphere, ce qui permet aux composants vSphere de se connecter entre eux en toute sécurité.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.

2 Dans le volet de gauche, sous **Paramètres**, sélectionnez **Services vSphere**.

3 Configurez les services vSphere.

- Pour enregistrer vCloud Director dans vCenter Lookup Service, cliquez sur **Enregistrer**.
- Pour annuler l'enregistrement de vCloud Director dans vCenter Lookup Service, cliquez sur **Annuler l'enregistrement**.

4 Entrez l'URL de vCenter Lookup Service, par exemple, `https://hostname:7444/lookupservice/sdk`.

5 Entrez le nom d'utilisateur et le mot de passe d'un utilisateur vCenter Single Sign-On disposant de privilèges administratifs, par exemple l'utilisateur `administrator@your_domain_name`.

Résultats

Si vous avez enregistré vCloud Director dans vCenter Lookup Service, les **administrateurs système** doivent se connecter à vCloud Director avec leurs informations d'identification de vCenter Single Sign-On.

Surveillance de vCloud Director 12

Les administrateurs système peuvent surveiller les opérations terminées et en cours, et afficher les informations d'utilisation des ressources au niveau du centre de données virtuel fournisseur, du centre de données virtuel d'organisation et de la banque de données.

À partir de la version 9.1, vCloud Director ne prend pas en charge VMware vCenter Chargeback Manager. Reportez-vous à la section Matrices d'interopérabilité des produits VMware

Ce chapitre contient les rubriques suivantes :

- vCloud Director et rapport de coût
- Afficher les informations d'utilisation d'un centre de données virtuel fournisseur

vCloud Director et rapport de coût

Vous pouvez utiliser VMware vRealize Operations Tenant App pour permettre à vCloud Director de configurer un système de génération de rapports de coût pour vCloud Director.

VMware vRealize Operations Tenant App dispose de capacités de mesure qui permettent aux fournisseurs de services de fournir à leur base de clients des services de rétrofacturation.

VMware vRealize Operations Tenant App est également une application locataire qui fournit aux administrateurs de locataires une visibilité sur leur environnement et sur leurs données de facturation.

Pour plus d'informations sur la compatibilité entre vCloud Director et VMware vRealize Operations Tenant App, consultez les *Matrices d'interopérabilité des produits VMware* à l'adresse http://partnerweb.vmware.com/comp_guide/sim/interop_matrix.php.

Vous pouvez télécharger VMware vRealize Operations Tenant App à l'adresse https://marketplace.vmware.com/vsx/solutions/management-pack-for-vcloud-director.

Pour plus d'informations sur l'utilisation de VMware vRealize Operations Tenant App, reportez-vous à *Utilisation de vRealize Operations Tenant App pour vCloud Director en tant que fournisseur de services* et à *Utilisation de vRealize Operations Tenant App pour vCloud Director en tant que locataire*.

Afficher les informations d'utilisation d'un centre de données virtuel fournisseur

Les centres de données virtuels fournisseur fournissent des ressources de calcul, de mémoire et de stockage aux centres de données virtuels d'organisation. Vous pouvez surveiller l'utilisation des ressources des centres de données virtuel fournisseur afin d'ajouter des ressources lorsque vous jugez cela nécessaire.

Procédure

1. Dans le menu principal (☰), sélectionnez **Ressources de Cloud**.
2. Dans le volet de gauche, cliquez sur **VDC fournisseur**, puis sur le nom du centre de données virtuel fournisseur cible.
3. Cliquez sur l'onglet **Configurer > Mesures**.
4. Pour plus d'informations sur chaque paramètre, cliquez sur chaque icône d'information.

Gestion des services

13

La vue Bibliothèques de contenus de vCloud Director Service Provider Admin Portal fournit une interface d'intégration à vRealize Orchestrator. Les workflows vRealize Orchestrator sont disponibles sous forme de catalogue de services que les administrateurs du fournisseur de services peuvent publier pour les locataires ou d'autres fournisseurs de services, et ainsi étendre l'ensemble des fonctionnalités et des capacités de gestion qu'ils offrent.

Ce chapitre contient les rubriques suivantes :

- Intégration de vRealize Orchestrator à vCloud Director
- Créer une catégorie de service
- Modifier une catégorie de service
- Importer un service
- Rechercher un service
- Exécuter un service
- Modifier une catégorie de service
- Annuler l'inscription d'un service
- Publier un service

Intégration de vRealize Orchestrator à vCloud Director

Pour intégrer vRealize Orchestrator à vCloud Director, passez par vCloud Director Service Provider Admin Portal.

L'intégration de vRealize Orchestrator à vCloud Director étend la fonctionnalité de base de vCloud Director en autorisant les administrateurs du fournisseur de services à développer des tâches d'automatisation complexes par l'orchestration du workflow et l'utilisation de plug-ins tiers.

Grâce à vCloud Director Service Provider Admin Portal, les administrateurs du fournisseur de services peuvent afficher, importer et exécuter des workflows dans les instances de serveur vRealize Orchestrator inscrites.

Sur vCloud Director Service Provider Admin Portal, les workflows de vRealize Orchestrator peuvent être publiés à l'attention des fournisseurs de services ou des locataires, ce qui permet un contrôle d'accès rapide et l'exécution des services personnalisés et intégrés.

vRealize Orchestrator dispose d'une bibliothèque de workflows étendue contenant des tâches prêtes à l'utilisation conçues pour relever des défis spécifiques et effectuer des tâches administratives courantes. Des plug-ins tiers sont également disponibles sur le site VMware Solution Exchange.

Inscrire une instance de vRealize Orchestrator auprès de vCloud Director

Pour exploiter l'orchestration de workflows et l'automatisation des tâches via vRealize Orchestrator dans vCloud Director, vous inscrivez une instance de vRealize Orchestrator sur le vCloud Director Service Provider Admin Portal.

Conditions préalables

- Déployez et configurez une instance du serveur vRealize Orchestrator. Pour plus d'informations, reportez-vous à la section *Installation et configuration de VMware vRealize Orchestrator* de la documentation vRealize Orchestrator.
- Configurez vRealize Orchestrator pour utiliser vSphere comme fournisseur d'authentification.
- Vérifiez que vCloud Director est inscrit auprès du service de recherche du même Platform Services Controller que l'authentification vCenter Single Sign-On utilisé par vRealize Orchestrator pour l'authentification.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**

   a Sur le panneau de gauche, sélectionnez **Gestion des services**.

   Une liste des serveurs vRealize Orchestrator inscrits s'affiche.

2 Pour inscrire un nouveau serveur vRealize Orchestrator, cliquez sur le bouton +.

   La boîte de dialogue **Enregistrer vRealize Orchestrator** s'affiche.

3 Entrez les valeurs suivantes.

Option	Description
Nom	Nom de l'instance vRealize Orchestrator inscrite.
Description	Description de l'instance du serveur vRealize Orchestrator inscrit.
Nom d'hôte	Nom de domaine complet et port du serveur vRealize Orchestrator. La valeur du port HTTPS par défaut est 8281. **Note** vCloud Director se connecte à l'interface API de vRealize Orchestrator.
Nom d'utilisateur	Compte d'utilisateur membre du groupe d'administrateurs vRealize Orchestrator.

Option	Description
Mot de passe	Mot de passe du compte administrateur vRealize Orchestrator.
Ancre d'approbation	Certificat SSL du serveur vRealize Orchestrator au format PEM. Cliquez sur l'icône de téléchargement ( ) pour rechercher et sélectionner le fichier `.pem`.

4 Cliquez sur **OK** pour terminer l'inscription.

Le serveur vRealize Orchestrator est inscrit auprès de vCloud Director.

Créer une catégorie de service

Vous pouvez organiser les services en catégories de services.

Procédure

1 Dans le menu principal ( ), sélectionnez **Bibliothèques de contenu**

a Sur le panneau de gauche, sélectionnez **Gestion des services**.

b Accédez à l'onglet **Catégories de services**.

Une liste des catégories de serveurs existantes s'affiche.

2 Pour créer une catégorie de service, cliquez sur le bouton ( ).

La boîte de dialogue **Nouvelle catégorie de service** s'affiche.

3 Entrez les valeurs suivantes.

Option	Description
Nom	Nom de la catégorie de service.
Icône	Importez l'icône affichée pour la catégorie de service.
Description	Brève description de la catégorie de service.

Modifier une catégorie de service

Vous pouvez modifier les catégories de services existantes.

Procédure

1 Dans le menu principal ( ), sélectionnez **Bibliothèques de contenu**

a Sur le panneau de gauche, sélectionnez **Gestion des services**.

b Accédez à l'onglet **Catégories de services**.

Une liste des catégories de serveurs existantes s'affiche.

2 Utilisez la barre de liste (⋮) à gauche d'une catégorie de service sélectionnée et cliquez sur **Modifier**.

3 Modifiez les valeurs suivantes.

Option	Description
Nom	Nom de la catégorie de service.
Icône	Importez l'icône affichée pour la catégorie de service.
Description	Brève description de la catégorie de service.

Importer un service

Vous pouvez importer des services depuis la bibliothèque de workflows d'une instance de vRealize Orchestrator inscrite auprès de vCloud Director.

Conditions préalables

- Inscrire une instance de vRealize Orchestrator. Reportez-vous à Inscrire une instance de vRealize Orchestrator auprès de vCloud Director.
- Créez une catégorie de service. Reportez-vous à Créer une catégorie de service.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Pour importer un nouveau service, cliquez sur le bouton **Importer**.

3 Suivez les étapes de l'assistant **Importer**.

Option	Description
Importer dans la bibliothèque cible	Sélectionnez la catégorie de service dans laquelle importer le service.
Sélectionner une source	Sélectionnez l'instance de vRealize Orchestrator à partir de laquelle importer les workflows.
Sélectionner les workflows	Développez la vue de l'arborescence hiérarchique pour sélectionner un ou plusieurs workflows à importer.
Vérifier	Vérifiez les informations et cliquez sur **Terminé** pour terminer l'importation.

Les workflows importés s'affichent dans la vue de fiche **Bibliothèque de services**.

Rechercher un service

Vous pouvez rechercher un service par son nom ou la catégorie de services à laquelle il appartient.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Dans la zone de texte **Recherche** en haut de la page, entrez un mot ou un caractère du nom du service ou de la catégorie de services que vous souhaitez rechercher.

   a Indiquez si vous souhaitez effectuer une recherche parmi les noms du service ou parmi les catégories.

   Les résultats de la recherche s'affichent dans une vue de fiche comportant douze éléments par page, triés par nom dans l'ordre alphabétique.

Exécuter un service

Vous pouvez exécuter des workflows vRealize Orchestrator en tant que services importés.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Pour exécuter un service, dans la fiche du service sélectionné, cliquez sur **Exécuter**.

   L'assistant **Exécuter un service** s'affiche.

3 Renseignez les paramètres d'entrée requis du service et cliquez sur **Terminer**.

Résultats

Vous pouvez surveiller l'état de l'exécution dans la vue **Tâches récentes**. Pour plus d'informations, reportez-vous à la section Afficher les tâches.

Note Lorsque vous démarrez un workflow vRealize Orchestrator en tant que service vCloud Director, vCloud Director ajoute quelques paramètres personnalisés au contexte d'exécution du workflow.

Propriété personnalisée	Description
`_vcd_orgName`	Nom de l'organisation à laquelle appartient l'utilisateur qui exécute le service.
`_vcd_orgId`	ID de l'organisation à laquelle appartient l'utilisateur qui exécute le service.
`_vcd_userName`	Nom de l'utilisateur qui exécute le service.
`_vcd_isAdmin`	La valeur est `True` si l'utilisateur qui exécute le service est un **administrateur**.
`_vdc_isAdmin`	Obsolète. La valeur est `True` si l'utilisateur qui exécute le service est un **administrateur**.
`_vdc_userName`	Obsolète. Nom de l'utilisateur qui exécute le service.
`_vcd_sessionToken`	Jeton d'authentification que vous avez reçu après une authentification réussie pour vCloud Director
`_vcd_apiEndpoint`	Point de terminaison de vCloud Director REST API

Modifier une catégorie de service

Vous pouvez modifier la catégorie à laquelle appartient un service.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Dans la fiche du service sélectionné, sélectionnez **Gérer > Modifier la catégorie**.

   La boîte de dialogue **Modifier la catégorie** s'ouvre.

3 Sélectionnez la catégorie dans laquelle placer le service et cliquez sur **Enregistrer**.

Annuler l'inscription d'un service

Vous pouvez supprimer l'accès à un service aux fournisseurs de services et aux locataires en annulant l'inscription du service.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Dans la fiche du service spécifié, sélectionnez **Gérer > Annuler l'inscription du workflow**.

   La boîte de dialogue **Annuler l'inscription du workflow** s'ouvre.

3 Pour supprimer le service de la bibliothèque de services, cliquez sur **Supprimer**.

Publier un service

Vous pouvez contrôler l'accès aux services du fournisseur de services et du locataire en publiant un service.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Bibliothèque de services**.

   Les services disponibles s'affichent dans une vue de fiche composée de 12 éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique que l'élément est un workflow vRealize Orchestrator et affiche le nom du service et une balise correspondant à la catégorie de service, dans laquelle le workflow est importé.

2 Sur la fiche du service sélectionné, sélectionnez **Gérer > Publier le workflow**.

   La boîte de dialogue **Publier le workflow** s'affiche.

3 Pour publier pour les fournisseurs de services, cliquez sur **Publier pour les fournisseurs de services** et cliquez sur **Enregistrer**.

4 Pour publier pour l'organisation d'un locataire spécifique, sélectionnez le bouton **Publier pour les locataires**.

   a Une liste des organisations de locataires disponibles s'affiche. Sélectionnez l'organisation du locataire pour laquelle vous souhaitez publier le workflow et cliquez sur **Enregistrer**.

5 Pour publier pour toutes les organisations de locataires, cliquez sur **Publier pour tous les locataires**, puis sur **Enregistrer**.

Gestion des entités personnalisées

14

Les définitions d'entités personnalisées de vCloud Director sont des types d'objets liés aux types d'objets vRealize Orchestrator. Lorsqu'un fournisseur de services publie les définitions d'une entité personnalisée pour un autre fournisseur de services ou pour un ou plusieurs locataires, les utilisateurs de vCloud Director peuvent posséder, gérer et modifier ces types en fonction de leurs besoins. En exécutant les services, les utilisateurs du fournisseur de services et les utilisateurs de l'organisation peuvent instancier les entités personnalisées et appliquer des actions aux instances des objets.

Ce chapitre contient les rubriques suivantes :

- Rechercher une entité personnalisée
- Modifier la définition d'une entité personnalisée
- Ajouter une définition d'entité personnalisée
- Instances d'entité personnalisée
- Associer une action à une entité personnalisée
- Dissocier une action depuis une entité personnalisée
- Publier une entité personnalisée
- Supprimer une entité personnalisée

Rechercher une entité personnalisée

Vous pouvez rechercher une entité personnalisée par son nom.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la zone de texte **Recherche** en haut de la page, entrez un mot ou un caractère du nom de l'entité que vous souhaitez rechercher.

   Les résultats de la recherche s'affichent dans une vue de fiche comportant douze éléments par page, triés par nom dans l'ordre alphabétique.

Modifier la définition d'une entité personnalisée

Vous pouvez modifier le nom et la description d'une entité personnalisée. Vous ne pouvez pas modifier le type de l'entité ou le type d'objet vRealize Orchestrator auquel l'entité est liée. Ce sont des propriétés par défaut de l'entité personnalisée. Si vous souhaitez modifier les propriétés par défaut, vous devez supprimer la définition de l'entité personnalisée et la recréer.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la fiche de l'entité personnalisée sélectionnée, sélectionnez **Actions > Modifier**.

   Une nouvelle boîte de dialogue s'ouvre.

3 Modifiez le nom ou la description de la définition de l'entité personnalisée.

4 Cliquez sur **OK** pour confirmer la modification.

Ajouter une définition d'entité personnalisée

Vous pouvez créer une entité personnalisée et la mapper à un type d'objet vRealize Orchestrator existant.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Cliquez sur l'icône + pour ajouter une nouvelle entité personnalisée.

   Une nouvelle boîte de dialogue s'ouvre.

3 Suivez les étapes de l'assistant **Définition de l'entité personnalisée**.

Étape	
Nom et description	Entrez un nom et une description (facultative) pour la nouvelle entité. Entrez un nom pour le type d'entité, par exemple `sshHost`.
vRO	Dans le menu déroulant, sélectionnez l'instance de vRealize Orchestrator que vous utiliserez pour mapper la définition d'entité personnalisée. **Note** Si vous disposez de plusieurs serveurs vRealize Orchestrator, vous devez créer une définition d'entité personnalisée distincte pour chacun d'eux.
Type	Cliquez sur l'icône d'affichage de liste ( ) pour accéder aux types d'objets vRealize Orchestrator disponibles regroupés par plug-ins. Par exemple, **SSH > Hôte**. Si vous connaissez le nom du type, vous pouvez l'entrer directement dans la zone de texte. Par exemple, `SSH:Host`.
Vérifier	Vérifiez les informations que vous avez spécifiées et cliquez sur **Terminé** pour terminer la création.

Résultats

La nouvelle définition d'entité personnalisée s'affiche dans la vue de fiche.

Instances d'entité personnalisée

L'exécution d'un workflow vRealize Orchestrator avec un type d'objet en guise de paramètre d'entrée déjà défini en tant que définition d'entité personnalisée dans vCloud Director affiche le paramètre de sortie en tant qu'instance d'une entité personnalisée.

Procédure

1 Dans le menu principal ( ), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la fiche de l'entité personnalisée sélectionnée, cliquez sur **Instances**.

   Les instances disponibles s'affichent dans une vue de grille.

3 Cliquez sur la barre de liste ( ) à gauche de chaque entité pour afficher les workflows associés.

   Cliquer sur un workflow initie l'exécution d'un workflow qui utilise l'instance de l'entité comme paramètre d'entrée.

Associer une action à une entité personnalisée

L'association d'une action à une définition d'entité personnalisée vous permet d'exécuter un ensemble de workflows vRealize Orchestrator sur les instances d'une entité personnalisée spécifique.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la fiche de l'entité personnalisée sélectionnée, sélectionnez **Actions > Associer une action**.

   Une nouvelle boîte de dialogue s'ouvre.

3 Suivez les étapes de l'assistant **Associer une entité personnalisée au workflow VRO**.

Étape	Détails
Sélectionner un workflow VRO	Sélectionnez l'un des workflows répertoriés. Ces workflows sont disponibles sur la page **Bibliothèque de services**.
Sélectionner un paramètre d'entrée de workflow	Sélectionnez un paramètre d'entrée disponible dans la liste. Associez le type du workflow vRealize Orchestrator au type de la définition d'entité personnalisée.
Vérifier l'association	Vérifiez les informations que vous avez spécifiées et cliquez sur **Terminé** pour terminer l'association.

Exemple

Par exemple, si vous disposez d'une entité personnalisée de type `SSH:Host`, vous pouvez l'associer au workflow `Add a Root Folder to SSH Host` en sélectionnant le paramètre d'entrée `sshHost`, qui correspond au type de l'entité personnalisée.

Dissocier une action depuis une entité personnalisée

Vous pouvez supprimer un workflow vRealize Orchestrator de la liste des actions associées.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la fiche de l'entité personnalisée sélectionnée, sélectionnez **Actions > Dissocier une action**.

Une nouvelle boîte de dialogue s'ouvre.

3 Sélectionnez le workflow à supprimer et cliquez sur **Dissocier l'action**.

Le workflow vRealize Orchestrator n'est plus associé à l'entité personnalisée.

Publier une entité personnalisée

Vous devez publier une entité personnalisée pour que les utilisateurs d'autres locataires ou fournisseurs de services puissent exécuter des workflows à l'aide des instances de l'entité personnalisée en guise de paramètres d'entrée.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Sur la fiche de l'entité personnalisée sélectionnée, cliquez sur **Actions > Publier**.

Une nouvelle boîte de dialogue s'ouvre.

3 Choisissez si vous souhaitez publier la définition de l'entité personnalisée pour les fournisseurs de service, tous les locataires, ou uniquement des locataires sélectionnés.

4 Cliquez sur **Enregistrer** pour confirmer la modification.

La définition de l'entité personnalisée devient disponible pour les parties sélectionnées.

Supprimer une entité personnalisée

Vous pouvez supprimer une définition d'entité personnalisée si l'entité personnalisée n'est plus utilisée, si elle a été configurée de manière incorrecte, ou si vous souhaitez mapper le type vRealize Orchestrator à une autre entité personnalisée.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques de contenu**.

   a Sur le panneau de gauche, sélectionnez **Définitions d'entités personnalisées**.

   La liste des entités personnalisées s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche indique le nom de l'entité personnalisée, le type vRealize Orchestrator auquel l'entité est mappée, le type de l'entité et éventuellement une description.

2 Dans la fiche de l'entité personnalisée sélectionnée, sélectionnez **Actions > Supprimer**.

3 Confirmez la suppression.

   L'entité personnalisée est supprimée de la vue de fiche.