Guide du portail de locataires de vCloud Director

19 septembre 2019
VMware Cloud Director 10.0

vmware®

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 © 2017-2020 VMware, Inc. Tous droits réservés. Informations relatives aux copyrights et marques commerciales.

Table des matières

Guide du portail de locataires de vCloud Director 11

1 Démarrage du portail de locataires de vCloud Director 12
- Comprendre VMware vCloud Director 12
- Se connecter au portail de locataires de vCloud Director 14
- Droits et rôles du portail de locataires vCloud Director 14
- Utilisation du portail de locataires vCloud Director 15
- Utiliser la recherche globale de vCloud Director 16
- Afficher les tâches 17
- Arrêter une tâche en cours 18
- Afficher les événements 19

2 Utilisation des machines virtuelles 21
- Architecture de la machine virtuelle 22
- Afficher et modifier les machines virtuelles 23
- Créer une machine virtuelle autonome 24
- Ouverture d'une console de machine virtuelle 26
  - Installer VMware Remote Console sur un client 26
  - Ouvrir une console distante de machine virtuelle 27
  - Ouvrir une console Web 27
- Exécution des opérations d'alimentation sur les machines virtuelles 28
  - Mettre une machine virtuelle sous tension 28
  - Mettre une machine virtuelle hors tension 29
  - Arrêter un système d'exploitation invité 29
  - Réinitialiser une machine virtuelle 30
  - Suspendre une machine virtuelle 30
  - Ignorer l'état interrompu d'une machine virtuelle 31
- Installer VMware Tools sur une machine virtuelle 32
- Mettre à niveau la version matérielle virtuelle pour une machine virtuelle 33
- Modifier les propriétés d'une machine virtuelle 34
  - Changer les propriétés générales d'une machine virtuelle 34
  - Changer les propriétés matérielles d'une machine virtuelle 35
  - Modifier les propriétés de personnalisation du système d'exploitation invité d'une machine virtuelle 38
  - Changer les propriétés avancées d'une machine virtuelle 42
- Insérer un support 45
- Éjecter un support 46
- Copier une machine virtuelle vers un autre vApp 46

Déplacer une machine virtuelle vers un autre vApp 47
Affinité et anti-affinité des machines virtuelles 49
Afficher des règles d'affinité et des règles d'anti-affinité 49
Créer une règle d'affinité 49
Créer une règle d'anti-affinité 50
Modifier une règle d'affinité ou d'anti-affinité 50
Supprimer une règle d'affinité ou d'anti-affinité 51
Surveiller les machines virtuelles 51
Utilisation des snapshots 53
Prendre un snapshot d'une machine virtuelle 53
Restaurer une machine virtuelle à un snapshot 54
Supprimer un snapshot d'une machine virtuelle 55
Renouveler le bail d'une machine virtuelle 55
Supprimer une machine virtuelle 56

3 Utilisation des vApp 57
Afficher les vApp 58
Construire un nouveau vApp 58
Créer un vApp depuis un module OVF 61
Créer un vApp à partir d'un modèle de vApp 63
Ouvrir un vApp 65
Exécution des opérations d'alimentation sur les vApp 66
Mettre sous tension un vApp 66
Mettre hors tension un vApp 66
Arrêter un vApp 67
Réinitialiser un vApp 67
Interrompre un vApp 68
Ignorer l'état interrompu d'un vApp 68
Modifier les propriétés d'un vApp 69
Modifier les propriétés générales du vApp 69
Modifier les propriétés avancées d'un vApp 70
Partager un vApp 71
Afficher un diagramme du réseau vApp 72
Utilisation des réseaux dans un vApp 73
Afficher les réseaux vApp 73
Clôturer un réseau vApp 74
Ajouter un réseau à un vApp 75
Configuration des services réseau pour un réseau vApp 76
Supprimer un réseau vApp 81
Utilisation des snapshots 82
Prendre un snapshot d'un vApp 82

Restaurer un vApp à un snapshot 83
Supprimer un snapshot d'un vApp 84
Changer le propriétaire d'un vApp 84
Déplacer un vApp vers un autre centre de données virtuel 85
Copier un vApp arrêté vers un autre centre de données virtuel 85
Copier un vApp activé 86
Ajouter une machine virtuelle à un vApp 87
Enregistrer un vApp en tant que modèle de vApp dans un catalogue 88
Télécharger un vApp comme module OVF 89
Renouveler le bail d'un vApp 90
Supprimer un vApp 90

4 Gestion des réseaux de centre de données virtuel d'organisation 92
Afficher les réseaux VDC d'organisation disponibles 94
Ajouter un réseau de centre de données virtuel d'organisation isolé 94
Ajouter un réseau de centre de données virtuel d'organisation acheminé 96
Ajouter un réseau de centre de données virtuel d'organisation direct 98
Ajouter un réseau VDC d'organisation avec un commutateur logique NSX-T importé 99
Modifier les paramètres généraux d'un réseau de centre de données virtuel d'organisation 100
Convertir un réseau de centre de données virtuel d'organisation 100
Convertir l'interface d'un réseau VDC d'organisation acheminé 101
Afficher les adresses IP utilisées pour un réseau de centre de données virtuel d'organisation 102
Ajouter des adresses IP à un pool d'adresses IP de réseau de centre de données virtuel d'organisation 103
Modifier ou supprimer des plages d'adresses IP utilisées dans un réseau de centre de données virtuel d'organisation 103
Modifier les paramètres DNS d'un réseau de centre de données virtuel d'organisation 104
Configurer les paramètres DHCP pour un réseau de centre de données virtuel d'organisation isolé 105
Modifier ou supprimer un pool DHCP existant pour un réseau 106
Réinitialiser un réseau de centre de données virtuel d'organisation 107
Supprimer un réseau de centre de données virtuel d'organisation 107

5 Gestion de la mise en réseau entre centres de données virtuels 108
Gestion des groupes de centres de données 109
Créer et configurer un groupe de centres de données avec une configuration de sortie commune 109
Créer et configurer un groupe de centres de données avec une configuration de sortie de domaine d'erreur 112
Afficher un groupe de centres de données 114
Ajouter un centre de données virtuel à un groupe de centres de données 115
Supprimer un centre de données virtuel d'un groupe de centres de données 116

Synchroniser un groupe de centres de données 117
Échanger les points de sortie dans un groupe de centres de données avec une configuration commune de sortie 117
Remplacer la passerelle Edge d'un point de sortie 118
Supprimer un point de sortie 119
Synchroniser les routes et les points de sortie 120
Gestion des réseaux étirés 121
Ajouter un réseau étiré 121
Afficher ou modifier un réseau étiré 122
Supprimer un réseau étiré 123
Synchroniser un réseau étiré 123

6 Capacités de mise en réseau avancées pour les locataires vCloud Director 125
Démarrage de la mise en réseau avancée de vCloud Director 126
Configuration du pare-feu à l'aide du portail de locataires 127
Pare-feu de passerelle Edge 128
Gestion d'un pare-feu de passerelle Edge NSX Data Center for vSphere 128
Pare-feu distribué 132
Activer le pare-feu distribué sur le centre de données virtuel d'une organisation à l'aide du portail de locataires 133
Gestion des règles de pare-feu distribué à l'aide du portail de locataires 134
Gestion du protocole DHCP de la passerelle Edge 139
Ajouter un pool d'adresses IP DHCP 139
Ajouter des liaisons DHCP 141
Configuration du relais DHCP pour les passerelles Edge NSX Data Center for vSphere 142
Spécifier une configuration de relais DHCP pour une passerelle Edge NSX Data Center for vSphere 143
Gestion de la traduction d'adresses réseau à l'aide du portail de locataires 144
Ajouter une règle SNAT ou DNAT 145
Configuration de routage avancée 148
Spécifier les configurations de routage par défaut pour la passerelle Edge NSX Data Center for vSphere 148
Ajouter une route statique 149
Configurer OSPF 151
Configurer BGP 154
Configurer les redistributions de route 156
Équilibrage de charge 157
À propos de l'équilibrage de charge 157
Sécuriser l'accès à l'aide de réseaux privés virtuels 171
Configurer VPN-Plus SSL 171
Configurer la fonction VPN IPSec 186
Configurer le VPN L2 193
Supprimer la configuration du service VPN L2 depuis une passerelle Edge 197

Gestion des certificats SSL 198
Générer une demande de signature de certificat pour une passerelle Edge 199
Importer le certificat signé par une autorité de certification correspondant à la demande de signature de certificat générée pour une passerelle Edge 200
Configuration d'un certificat de service autosigné 201
Ajouter un certificat d'autorité de certification à la passerelle Edge pour la vérification de l'approbation des certificats SSL 202
Ajouter une liste de révocation des certificats à une passerelle Edge 203
Ajouter un certificat de service à la passerelle Edge 204
Personnaliser le regroupement d'objets 205
Créer un ensemble d'adresses IP à utiliser dans les règles de pare-feu et la configuration du relais DHCP 205
Créer un ensemble d'adresses MAC à utiliser dans les règles de pare-feu 206
Afficher les services disponibles pour les règles de pare-feu 207
Afficher les groupes de services disponibles pour les règles de pare-feu 208
Statistiques et journaux pour une passerelle Edge 209
Afficher les statistiques 209
Activer la journalisation 209
Activer l'accès de ligne de commande SSH à une passerelle Edge 211
Utilisation des balises de sécurité 211
Créer et attribuer des balises de sécurité 212
Modifier l'attribution de balises de sécurité 213
Afficher les balises de sécurité appliquées 214
Modifier une balise de sécurité 214
Supprimer une balise de sécurité 215
Utilisation des groupes de sécurité 216
Créer un groupe de sécurité 216
Modifier un groupe de sécurité 218
Supprimer un groupe de sécurité 219

7 Gestion de passerelles Edge NSX-T Data Center 221
Ajouter un groupe de pare-feu à une passerelle Edge NSX-T 221
Ajouter une règle de pare-feu de passerelle Edge NSX-T 222
Ajouter une règle SNAT ou DNAT à une passerelle Edge NSX-T 223
Configurer un service de redirecteur DNS sur une passerelle Edge NSX-T 224
Créer des profils de port d'application personnalisés 225

8 Utilisation de disques nommés et vérification des stratégies de stockage 227
Création et utilisation des disques nommés 227
Créer un disque nommé 227
Modifier un disque nommé 228
Associer un disque nommé à une machine virtuelle 228

Supprimer un disque nommé 229
Vérifier les propriétés de la stratégie de stockage 229

9 Vérification des propriétés du centre de données virtuel 231
Vérifier les propriétés du centre de données virtuel 231
Vérifier les métadonnées du centre de données virtuel 231

10 Utilisation d'instances de vCenter Server dédiées et de proxys 233
Configurer votre navigateur avec vos paramètres de proxy 233
Se connecter à l'interface utilisateur d'un composant proxy 234

11 Utilisation des modèles de vApp 236
Afficher un modèle de vApp 236
Créer un modèle de vApp à partir d'un fichier OVF 237
Attribuer une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle à un modèle de vApp 238
Télécharger un modèle de vApp 239
Supprimer un modèle de vApp 240

12 Utilisation des fichiers de support 241
Télécharger des fichiers de support 241
Supprimer un fichier de support 242
Télécharger un fichier de support 242

13 Utilisation des catalogues 244
Afficher les catalogues 245
Créer un catalogue 245
Partager un catalogue 246
Supprimer un catalogue 247
Gérer les métadonnées pour un catalogue 248
Publier un catalogue 249
S'abonner à un catalogue externe 249
Mettre à jour l'URL d'emplacement et le mot de passe d'un catalogue abonné 250
Synchroniser un catalogue abonné 251

14 Utilisation des modèles de centre de données virtuel d'organisation 252
Afficher les modèles de centre de données virtuel disponibles 252
Créer un centre de données virtuel à partir d'un modèle 253

15 Gestion des utilisateurs, groupes et rôles 255
Gestion des utilisateurs 255
Créer un utilisateur 255

Importer des utilisateurs 257
Modifier un utilisateur 258
Désactiver ou activer un compte d'utilisateur 258
Supprimer un utilisateur 259
Déverrouiller un compte utilisateur verrouillé 259
Gestion des groupes 260
Importer un groupe 260
Supprimer un groupe 261
Modifier un groupe 261
Rôles et droits 262
Rôles prédéfinis et leurs droits 262
Droits des rôles de locataire globaux prédéfinis 264
Créer un rôle de locataire personnalisé 271
Modifier un rôle de locataire personnalisé 272
Supprimer un rôle 272

16 Permettre à votre organisation d'utiliser un fournisseur d'identité SAML 274

17 Gestion de votre organisation 277
Modifier le nom et la description de l'organisation 277
Modifier vos paramètres d'e-mail 278
Tester les paramètres SMTP 279
Modifier les paramètres de domaine des machines virtuelles de votre organisation 279
Utilisation sur plusieurs sites 280
Configurer et gérer les déploiements multisite 280
Comprendre comment fonctionnent les baux 281
Modifier les stratégies vApp et Bail de modèle de vApp au sein de votre organisation 282
Modifier les quotas par défaut des machines virtuelles de votre organisation 283
Modifier les stratégies de mot de passe et de compte d'utilisateur au sein de votre organisation 284

18 Utilisation de la bibliothèque de services 285
Rechercher un service 285
Exécuter un service 286

19 Utilisation des définitions d'entités personnalisées 287
Rechercher une entité personnalisée 287
Modifier la définition d'une entité personnalisée 288
Ajouter une définition d'entité personnalisée 288
Instances d'entité personnalisée 289
Associer une action à une entité personnalisée 290
Dissocier une action d'une définition d'entité personnalisée 291

Publier une entité personnalisée 291
Supprimer une entité personnalisée 292

Guide du portail de locataires de vCloud Director

Le *Guide du portail de locataires de VMware vCloud Director* fournit des informations sur l'utilisation du portail de locataires de VMware vCloud Director. Dans cette version, vous utilisez le portail de locataires pour administrer votre organisation, créer et configurer des machines virtuelles, des vApp et des réseaux au sein des vApp. Vous pouvez également configurer les capacités de mise en réseau avancées fournies par VMware NSX® for vSphere® dans un environnement vCloud Director. Le portail de locataires de vCloud Director vous permet également de créer et de gérer des catalogues, des vApp et des modèles de VDC, et de créer et gérer des réseaux intercentre de données virtuel.

Public cible

Ce guide est destiné à toute personne souhaitant utiliser les capacités fournies par le portail de locataires de vCloud Director. Les informations sont principalement destinées aux **administrateurs d'organisation** qui utilisent le portail de locataires pour administrer leur organisation, gérer des machines virtuelles, des vApp, des réseaux, etc.

Glossaire VMware Technical Publications

VMware Technical Publications fournit un glossaire des termes qui pourraient vous être inconnus. Pour consulter la définition des termes utilisés dans la documentation technique VMware, visitez le site Web http://www.vmware.com/support/pubs.

Démarrage du portail de locataires de vCloud Director

1

Lorsque vous vous connectez au portail de locataires, vous devez effectuer un certain nombre de tâches allant de la création de machines virtuelles et de vApp à la configuration d'une mise en réseau avancée et l'exécution de workflows vRealize Orchestrator.

Ce chapitre contient les rubriques suivantes :

- Comprendre VMware vCloud Director
- Se connecter au portail de locataires de vCloud Director
- Droits et rôles du portail de locataires vCloud Director
- Utilisation du portail de locataires vCloud Director
- Utiliser la recherche globale de vCloud Director
- Afficher les tâches
- Arrêter une tâche en cours
- Afficher les événements

Comprendre VMware vCloud Director

VMware vCloud Director offre un accès basé sur des rôles à un portail de locataires Web permettant aux membres d'une organisation d'interagir avec les ressources de l'organisation afin de créer et d'utiliser des vApp et des machines virtuelles.

Pour que vous puissiez accéder à votre organisation, un **administrateur système** vCloud Director doit créer l'organisation, lui attribuer des ressources et fournir l'URL permettant d'accéder au portail de locataires. Chaque organisation compte un ou plusieurs **administrateurs d'organisation** qui finalisent la configuration de l'organisation en ajoutant des membres, et en définissant des stratégies et des préférences. Une fois l'organisation configurée, les utilisateurs non-administrateur peuvent se connecter pour créer, utiliser et gérer des machines virtuelles et des vApp.

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 informations d'identification établies 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.

Utilisateurs et groupes

Une organisation peut contenir un nombre arbitraire d'utilisateurs et de groupes. Des utilisateurs peuvent être créés localement par l'administrateur d'organisation ou être importés à partir d'un service d'annuaire. Les groupes doivent être importés à partir du service d'annuaire. Les autorisations au sein d'une organisation sont contrôlées via l'attribution de droits et de rôles à des utilisateurs et des groupes.

Centres de données virtuels

Un centre de données virtuel d'organisation fournit des ressources à une organisation. Les centres de données virtuels fournissent un environnement dans lequel des systèmes virtuels peuvent être stockés, déployés et exécutés. Ils fournissent également un stockage pour les supports CD et DVD virtuels. Une organisation peut avoir plusieurs centres de données virtuels.

Réseaux de centre de données virtuel d'organisation

Un réseau de centre de données virtuel d'organisation se trouve dans 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. Un réseau de centre de données virtuel d'organisation peut être connecté à un réseau externe ou isolé et interne à l'organisation. Seuls les **administrateurs système** peuvent créer des réseaux de centres de données virtuels d'organisation, mais les **administrateurs d'organisation** peuvent gérer les réseaux de centres de données virtuels d'organisation, notamment les services réseau qu'ils fournissent.

Réseaux vApp

Un réseau vApp réside dans un vApp et permet aux machines virtuelles contenues dans le vApp de communiquer entre elles. Vous pouvez connecter un réseau vApp à un réseau de centre de données virtuel d'organisation pour permettre au vApp de communiquer avec les autres vApp de l'organisation et en dehors de l'organisation, si le réseau de centre de données virtuel d'organisation est connecté à un réseau externe.

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 de ce catalogue afin de créer leurs propres vApp. Les **administrateurs d'organisation** peuvent copier des éléments de catalogues publics vers leur catalogue d'organisation.

Instances de vCenter Server dédiées (SDDC) et proxys

Un SDDC (Software-Defined Data Center) encapsule un environnement vCenter Server entier. Une instance de vCenter Server dédiée peut inclure un ou plusieurs proxys qui fournissent un accès à différents composants de l'environnement sous-jacent. L'**administrateur système** peut publier une ou plusieurs instances de vCenter Serverdédiées vers votre organisation. Vous pouvez utiliser les proxys conteneurs pour accéder à l'interface utilisateur ou à l'API des composants proxy.

Se connecter au portail de locataires de vCloud Director

Vous pouvez accéder au portail de locataires de vCloud Director en utilisant une URL spécifique de votre organisation.

Contactez l'**administrateur de votre organisation** si vous ne connaissez pas l'URL du portail de locataires de l'organisation. Reportez-vous aux *Notes de mise à jour de vCloud Director* pour plus d'informations sur les navigateurs et les configurations pris en charge.

Procédure

1. Dans un navigateur Web, accédez au portail de locataire URL de votre organisation.

   Par exemple, *https://vcloud.example.com/tenant/myOrg*.

2. Entrez votre nom d'utilisateur et votre mot de passe, puis cliquez sur **Se connecter**.

Droits et rôles du portail de locataires vCloud Director

vCloud Director inclut un ensemble préconfiguré de rôles d'utilisateur et leurs droits. Les rôles qui sont en mesure d'accéder au portail de locataires vCloud Director sont les rôles créés par défaut dans une organisation ou d'autres rôles créés par l'administrateur de l'organisation.

Les utilisateurs qui sont affectés aux rôles d'organisation suivants peuvent accéder au portail de locataires. Les éléments qu'ils voient et les actions qu'ils peuvent effectuer dépendent des droits associés à un rôle particulier.

- **Administrateur d'organisation**
- **Auteur de catalogue**
- **Auteur de vApp**
- **Utilisateur de vApp**

- **Accès via la console uniquement**

Pour plus d'informations sur les rôles prédéfinis et leurs droits, reportez-vous à Rôles prédéfinis et leurs droits.

Utilisation du portail de locataires vCloud Director

Si vous disposez de plusieurs centres de données virtuels, lorsque vous vous connectez au portail de locataires de vCloud Director, vous êtes redirigé vers l'écran du tableau de bord **Centres de données virtuels**. Si vous n'avez qu'un seul centre de données virtuel, lorsque vous vous connectez au portail de locataires de vCloud Director, vous êtes directement redirigé vers le centre de données.

L'écran du tableau de bord **Centres de données virtuels** fait partie de la fonctionnalité multisite vCloud Director qui permet aux locataires de voir leur environnement de cloud géographiquement distribué comme une seule entité. Pour plus d'informations sur le multisite, reportez-vous au Utilisation sur plusieurs sites.

Le tableau de bord est une vue unifiée des centres de données virtuels vCloud Director et des sites, mais pas uniquement dans une seule organisation. Dans un environnement comportant plusieurs cellules et plusieurs organisations, vous pouvez également voir les centres de données virtuels pour toutes les autres organisations associées.

Note En fonction de leurs droits, les utilisateurs locataires peuvent voir tous les sites membres d'une organisation ou uniquement un sous-ensemble des sites.

Les informations sur l'organisation s'affichent en haut du ruban récapitulatif.

Si vous vous connectez en tant qu'**administrateur d'organisation**, vous pouvez voir :

- Nombre de sites, d'organisations et de centres de données virtuels
- Le nombre total de vApp et machines virtuelles en cours d'exécution
- Les ressources matérielles utilisées telles que le CPU, la mémoire et le stockage

Les centres de données virtuels s'affichent dans une vue de carte. Chaque carte contient des informations indiquant l'organisation à laquelle appartient le centre de données virtuel, le nombre de vApp, le nombre total de machines virtuelles et le nombre de machines virtuelles qui sont en cours d'exécution. La carte affiche également la capacité de processeur, de mémoire et de stockage disponible pour le centre de données et affiche des mesures en temps réel sur les allocations en cours et les réservations de ressources.

Depuis le menu principal (☰), vous pouvez accéder aux différentes options de menu.

Élément de menu	Description
Centres de données	Permet d'accéder à l'écran **Centres de données virtuels** qui affiche les centres de données virtuels dans l'organisation.
Groupes de centres de données	Vous permet d'accéder à l'écran **Groupes de centres de données** pour gérer des réseaux entre centres de données virtuels. Par défaut, seul l'**administrateur système** peut afficher cet élément de menu.
Bibliothèques	Permet d'accéder à une vue consolidée des modèles vApp, des catalogues, des supports et autres types de fichiers. Vous utilisez ces modèles et ces fichiers pour déployer des machines virtuelles ou des vApp.
Administration	Permet d'accéder à l'écran de gestion multisite dans lequel les **administrateurs d'organisation** peuvent créer une association de confiance avec une autre organisation.
Tâches	Vous permet d'accéder à l'écran **Tâches** qui affiche les tâches signalées par vCloud Director.
Événements	Vous permet d'accéder à l'écran **Événements** qui affiche les événements signalés par vCloud Director.
Opérations	Vous permet d'accéder à l'écran **Bibliothèque de services**. La **Bibliothèque de services** contient des groupes de composants vCloud Director, pour lesquels vous pouvez exécuter des workflows vRealize Orchestrator.

Vous pouvez personnaliser votre portail de locataires vCloud Director à l'aide des OpenAPI vCloud `Branding`. Pour plus d'informations sur l'utilisation de l'OpenAPI vCloud, reportez-vous au document *Démarrage de vCloud OpenAPI* à l'adresse https://code.vmware.com.

Utiliser la recherche globale de vCloud Director

Vous pouvez utiliser la recherche globale de vCloud Director pour effectuer une recherche en fonction d'un nom ou d'une partie d'un nom parmi les noms d'objet de votre environnement. Vous pouvez également rechercher une machine virtuelle en fonction de son adresse IP si celle-ci est statique.

La liste des objets prédéfinis est la suivante :

- Centres de données
- modèles de vApp
- vApp
- Machines virtuelles
- Réseaux vApp
- Catalogues

Si une machine virtuelle utilise une adresse IP attribuée par DHCP, la recherche ne renvoie pas son adresse IP. Si vous souhaitez rechercher une machine virtuelle comportant une adresse IP attribuée par DHCP, vous devez effectuer une recherche par nom.

Par défaut, vous pouvez effectuer une recherche uniquement dans les objets de votre site local. Si vous disposez d'un environnement multisite, vous pouvez effectuer une recherche sur plusieurs sites.

Procédure

1 Dans le coin supérieur droit du portail de locataires vCloud Director, cliquez sur l'icône **Rechercher** ( ).

2 (Facultatif) Épinglez le panneau de recherche en cliquant sur l'icône **Épingler** ( ).

3 Dans la zone de texte **Rechercher**, entrez un symbole, une partie d'un nom ou une adresse IP pour rechercher des adresses IP statiques ou des noms d'objet de machines virtuelles correspondants.

4 Si vous utilisez un environnement multisite, sélectionnez les sites dans lesquels vous souhaitez effectuer la recherche.

5 Appuyez sur **Entrée**.

Résultats

Les cinq premiers résultats correspondants par type d'objet s'affichent. Les résultats sont triés par ordre alphabétique.

Étape suivante

- Pour afficher plus de résultats, le cas échéant, cliquez sur **Charger plus** sous chaque type d'objet.
- Pour afficher plus d'informations sur un objet spécifique dans les résultats de la recherche, pointez vers l'objet.
- Pour gérer un objet spécifique, par exemple, pour afficher ou modifier les paramètres d'un objet, cliquez sur cet objet. Les détails concernant l'objet s'affichent sur la gauche.

Afficher les tâches

Depuis le portail des locataires, vous pouvez consulter la liste des tâches récentes, ainsi que leurs détails et leur état. En outre, vous pouvez également voir la liste de toutes les tâches.

Par défaut, le panneau **Tâches récentes** s'affiche en bas du portail de locataires et contient une liste des tâches récemment exécutées. Lorsque vous démarrez une opération, par exemple pour créer une machine virtuelle, la tâche s'affiche dans le panneau. Si vous réduisez le panneau **Tâches récentes**, vous voyez toujours le nombre de tâches récentes en cours d'exécution ou ayant échoué. Vous pouvez toujours ouvrir à nouveau le panneau **Tâches récentes** en cliquant sur les doubles flèches.

La vue des tâches répertorie toutes les tâches et indique à quel moment elles ont été exécutées et si elles ont été exécutées avec succès. Cette vue est la première étape pour le dépannage des problèmes dans votre environnement. La vue des tâches contient des opérations de longue durée, telles que la création d'une machine virtuelle ou d'un vApp.

Procédure

1 Dans le menu principal (☰), sélectionnez **Tâches** ou cliquez sur **Plus de tâches** sous le panneau **Tâches récentes**.

   La liste de toutes les tâches s'affiche, ainsi que la durée d'exécution de la tâche et son état.

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

3 (Facultatif) Pour afficher les détails de la tâche, cliquez sur le nom de la tâche.

   Les détails de la tâche comprennent des informations telles que la raison de l'échec, quand la tâche a échoué, et ainsi de suite.

Détails	Description
Opération	Nom de l'opération effectuée.
Identifiant de la tâche	ID de la tâche.
Type	L'objet sur lequel la tâche a été effectuée. Par exemple, si vous avez créé une machine virtuelle, le type est `vm`.
Organisation	Nom de l'organisation.
État	État de la tâche, tel que Réussite, Exécution ou Échec.
Initiateur	Utilisateur qui a démarré l'opération.
Heure de début	Date et heure de début de l'opération.
Heure de fin	Date et heure auxquelles l'opération a réussi ou échoué.
Espace de noms de service	Nom du service, tel que *com.vmware.vcloud*.
Détails	Raison de l'échec de la tâche. Par exemple, si vous essayez de créer un snapshot d'une machine virtuelle, et que l'opération échoue, parce que le stockage est insuffisant, les détails de la tâche sont du type : `L'opération demandée dépassera le quota de stockage du VDC : la stratégie de stockage "*" a 8,693 Mo restants, 41,472 Mo requis.`

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 la tâche.
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*.

Détails	Description
État	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.

Utilisation des machines virtuelles 2

Une machine virtuelle est un ordinateur logiciel qui exécute un système d'exploitation et des applications, comme un ordinateur physique. La machine virtuelle se compose d'un ensemble de fichiers de spécification et de configuration, et repose sur les ressources physiques d'un hôte. Chaque machine virtuelle dispose de périphériques virtuels qui fournissent la même fonctionnalité que le matériel physique, mais qui sont plus portables, plus sécurisés et plus faciles à gérer.

Outre les opérations que vous pouvez exécuter sur une machine physique, les machines virtuelles vCloud Director prennent en charge les opérations d'infrastructure virtuelle (par exemple, prendre un snapshot de l'état de la machine virtuelle et déplacer une machine virtuelle d'un hôte vers un autre).

À partir de vCloud Director 9.5, les machines virtuelles prennent en charge la connectivité IPv6. Vous pouvez attribuer des adresses IPv6 aux machines virtuelles connectées à des réseaux IPv6.

Important Toutes les étapes de l'utilisation des machines virtuelles sont documentées dans la vue de carte, en partant du principe que vous avez plusieurs centres de données virtuels. Il est également possible de suivre les mêmes procédures à partir de la vue grille, mais les étapes peuvent varier légèrement.

Ce chapitre contient les rubriques suivantes :

- Architecture de la machine virtuelle
- Afficher et modifier les machines virtuelles
- Créer une machine virtuelle autonome
- Ouverture d'une console de machine virtuelle
- Exécution des opérations d'alimentation sur les machines virtuelles
- Installer VMware Tools sur une machine virtuelle
- Mettre à niveau la version matérielle virtuelle pour une machine virtuelle
- Modifier les propriétés d'une machine virtuelle
- Insérer un support
- Éjecter un support
- Copier une machine virtuelle vers un autre vApp

- Déplacer une machine virtuelle vers un autre vApp
- Affinité et anti-affinité des machines virtuelles
- Surveiller les machines virtuelles
- Utilisation des snapshots
- Renouveler le bail d'une machine virtuelle
- Supprimer une machine virtuelle

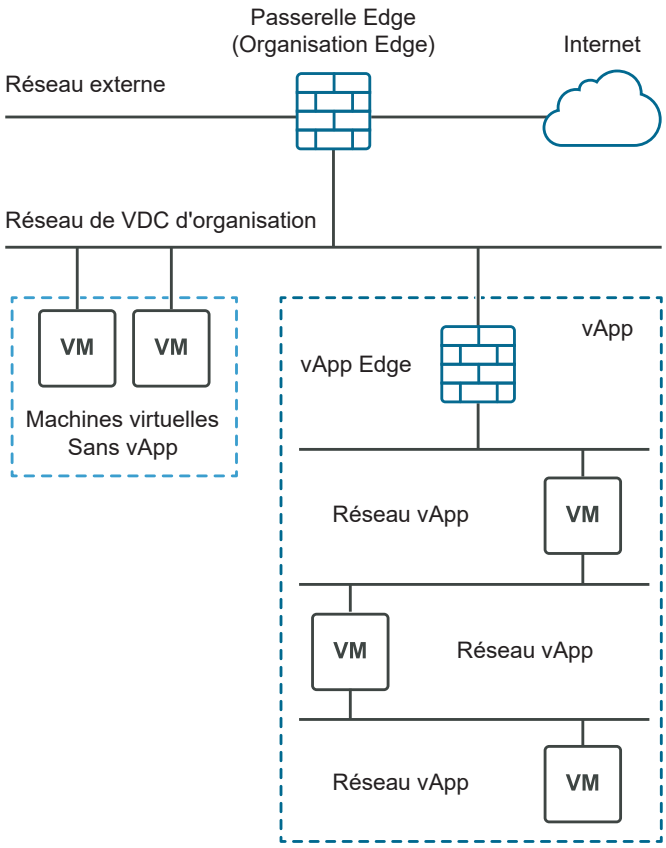
Architecture de la machine virtuelle

Une machine virtuelle peut exister en tant que machine autonome ou au sein d'un vApp.

Une machine virtuelle est un ordinateur logiciel qui exécute un système d'exploitation et des applications, comme un ordinateur physique. La machine virtuelle se compose d'un ensemble de fichiers de spécification et de configuration, et repose sur les ressources physiques d'un hôte. Chaque machine virtuelle dispose de périphériques virtuels qui fournissent la même fonctionnalité que le matériel physique, mais qui sont plus portables, plus sécurisés et plus faciles à gérer. Les machines virtuelles peuvent être autonomes ou elles peuvent exister au sein d'un vApp. Un vApp est un objet composé qui est constitué d'une ou plusieurs machines virtuelles, ainsi que d'un ou plusieurs réseaux.

La figure suivante présente les différentes options possibles lors de la création d'une machine virtuelle. Vous pouvez créer une machine virtuelle autonome ou une machine virtuelle au sein d'un vApp. La machine virtuelle autonome est directement connectée au centre de données virtuel d'organisation. Vous pouvez également créer une machine virtuelle au sein d'un vApp. En créant une machine virtuelle à l'intérieur d'un vApp, vous pouvez regrouper plusieurs machines virtuelles et leurs réseaux associés. Les vApp vous permettent de créer des applications complexes et de les enregistrer dans un catalogue pour une utilisation future.

Figure 2-1. Les machines virtuelles sont autonomes ou au sein d'un vApp



Afficher et modifier les machines virtuelles

Vous pouvez afficher les machines virtuelles autonomes ou intégrées à un vApp. Vous pouvez afficher les machines virtuelles dans une vue de grille ou dans une vue de carte.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Pour afficher les machines virtuelles dans une vue grille, cliquez sur . Ou pour les afficher dans une vue carte, cliquez sur .

   La liste des machines virtuelles s'affiche dans une vue grille ou comme une liste de cartes.

4 (Facultatif) Configurez la vue grille pour qu'elle contienne les détails que vous voulez voir sur chaque machine virtuelle.

   a Dans la vue de grille, cliquez sur l'icône de **Éditeur de grille** ( ).

   b Sélectionnez les détails de la machine virtuelle que vous voulez inclure dans la vue grille en cochant la case à côté de chaque détail que vous voulez voir.

   Les détails comprennent des informations sur la version du matériel, VMware Tools, la mémoire, etc.

   c Cliquez sur **OK** pour enregistrer les modifications.

   Les détails sélectionnés apparaissent sous forme de colonnes pour chaque machine virtuelle.

5 (Facultatif) Dans la vue grille, cliquez sur à gauche d'une machine virtuelle, pour afficher les actions que vous pouvez entreprendre pour la machine virtuelle sélectionnée.

   Par exemple, vous pouvez arrêter une machine virtuelle.

6 Pour accéder à l'interface du système d'exploitation invité de la machine virtuelle, cliquez sur l'icône de poste de travail dans le coin supérieur droit de la vue de carte.

Créer une machine virtuelle autonome

Vous pouvez créer une machine virtuelle autonome.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Cliquez sur **Nouvelle VM**.

4 Entrez le nom de la machine virtuelle et le nom de l'ordinateur pour celle-ci.

   Important Le nom de l'ordinateur ne peut contenir que des caractères alphanumériques et des traits d'union. Un nom d'ordinateur ne peut pas être composé de chiffres uniquement et ne peut pas contenir d'espaces.

5 (Facultatif) Entrez une description significative.

6 Indiquez si vous souhaitez que la machine virtuelle se mette sous tension après sa création.

7 Sélectionnez la manière dont vous souhaitez déployer la machine virtuelle.

Option	Action
Nouveau	Vous déployez une nouvelle machine virtuelle avec des paramètres personnalisables. a Sélectionnez une famille de systèmes d'exploitation et le système d'exploitation. b (Facultatif) Sélectionnez une image de démarrage. c (Facultatif) Sélectionnez une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle. Les menus déroulants de stratégie de positionnement et de dimensionnement de machine virtuelle ne sont visibles que si le fournisseur de services a publié de telles stratégies sur le VDC d'organisation. d (Facultatif) Sélectionnez la taille de la machine virtuelle parmi les options de dimensionnement prédéfinies ou cliquez sur **Options de dimensionnement personnalisées** pour entrer manuellement le nombre de CPU virtuels, de cœurs par socket et de paramètres de mémoire. Si vous sélectionnez une stratégie de dimensionnement de machine virtuelle qui définit la taille de la machine virtuelle, cette option n'est pas visible. Les tailles prédéfinies de la machine virtuelle sont **Petite**, **Moyenne** et **Grande**. e Spécifiez les paramètres de stockage de la machine virtuelle, comme la stratégie de stockage et la taille en Go. f Spécifiez les paramètres réseau de la machine virtuelle, comme le réseau, le mode IP, l'adresse IP et la carte réseau principale.
À partir du modèle	Vous déployez une machine virtuelle à partir d'un modèle que vous sélectionnez dans le catalogue de modèles. a Sélectionnez un modèle de machine virtuelle dans la liste des modèles disponibles. b (Facultatif) Sélectionnez une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle. Les menus déroulants de stratégie de positionnement et de dimensionnement de machine virtuelle ne sont visibles que si le fournisseur de services a publié de telles stratégies sur le VDC d'organisation. Si des stratégies sont attribuées au modèle sélectionné, vous pouvez être limité aux stratégies de modèle prédéfinies. c (Facultatif) Sélectionnez cette option pour utiliser une stratégie de stockage personnalisée et sélectionnez la stratégie de stockage à utiliser dans le menu déroulant **Stratégie de stockage personnalisée à utiliser**. d Lisez et acceptez le contrat de licence d'utilisateur final, le cas échéant.

8 Cliquez sur **OK** pour enregistrer les paramètres de la machine virtuelle et démarrer le processus de création.

Vous pouvez voir la carte de la machine virtuelle dans le catalogue. Tant que la machine virtuelle est en cours de création, son état est Occupé.

Ouverture d'une console de machine virtuelle

L'accès à votre console de machine virtuelle vous permet d'afficher des informations sur la machine virtuelle, de travailler avec le système d'exploitation invité et d'effectuer des opérations qui ont une incidence sur le système d'exploitation invité.

Conditions préalables

La machine virtuelle est sous tension.

Installer VMware Remote Console sur un client

La console distante VMware permet une interaction intégrée entre l'utilisateur et l'invité dans toutes les machines virtuelles provisionnées et gérées par vCloud Director. Cette section détaille les tâches requises pour installer la console distante VMware sous Windows, Apple OS X et Linux.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Utilisateur de vApp** ou un ensemble de droits équivalent.

Procédure

1. Téléchargez le programme d'installation.
   - Accédez à la page de téléchargement de VMware Remote Console, puis sélectionnez le lien vers votre plate-forme.

     www.vmware.com/go/download-vmrc
   - Sur l'écran de tableau de bord **Centres de données virtuels** du portail de locataires de vCloud Director, cliquez sur la fiche du centre de données virtuel que vous souhaitez explorer. Sélectionnez une machine virtuelle et, dans le menu **Actions**, sélectionnez **Télécharger VMRC**.
2. Procédez à l'installation de votre plate-forme.
   - Windows

     Double-cliquez sur le programme d'installation `.msi` et suivez les invites.
   - Linux

     Avec des privilèges racine, exécutez le programme d'installation `.bundle` et suivez les invites.
   - Mac

     Double-cliquez sur le fichier `.dmg` pour l'ouvrir, puis double-cliquez sur l'icône de la console distante VMware qu'il contient pour effectuer une copie dans le dossier Applications.

Résultats

Après l'installation, VMware Remote Console s'ouvre lorsque vous cliquez sur des URI (Uniform Resource Identifier) commençant par le schéma `vmrc://`. VMware Workstation, Player et Fusion gèrent également le schéma `vmrc://`.

Ouvrir une console distante de machine virtuelle

Vous pouvez ouvrir une console de machine virtuelle à l'aide de VMware Remote Console via le portail de locataires de vCloud Director.

Conditions préalables

- Vérifiez que VMware Remote Console est installé sur votre système local.
- Assurez-vous que la machine virtuelle sélectionnée est sous tension.
- Cette opération nécessite les droits inclus dans le rôle prédéfini **Utilisateur de vApp** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle, sélectionnez **Lancer la console distante de machine virtuelle**.

   Note Si vous n'avez pas installé VMware Remote Console, une fenêtre contextuelle vous invite à installer VMware Remote Console ou à utiliser la console Web.

Résultats

La console de machine virtuelle s'ouvre en tant que console distante virtuelle externe.

Note Lorsque vous vous connectez à une machine virtuelle vCloud Director à l'aide de VMware Remote Console, vous êtes limité à l'interaction de console (envoi de `Ctrl+Alt+Del`). Vous ne pouvez pas effectuer d'opérations de périphérique, d'opérations d'alimentation ou de gestion de paramètres.

Ouvrir une console Web

Vous pouvez vous connecter à la console d'une machine virtuelle, même si vous n'avez pas installé VMware Remote Console sur votre système local.

Conditions préalables

- Vérifiez que la machine virtuelle est sous tension.
- Cette opération nécessite les droits inclus dans le rôle prédéfini **Utilisateur de vApp** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle, sélectionnez **Lancer la console Web**.

Résultats

La console de machine virtuelle s'ouvre dans un nouvel onglet du navigateur à l'aide du SDK de la console HTML VMware.

Étape suivante

Cliquez n'importe où dans la fenêtre de la console pour commencer à utiliser la souris, le clavier et les autres périphériques d'entrée de la console.

Note Pour plus d'informations sur les claviers internationaux pris en charge, reportez-vous à la documentation sur le SDK de la console HTML VMware sur https://www.vmware.com/support/developer/html-console/.

Exécution des opérations d'alimentation sur les machines virtuelles

Vous pouvez effectuer des opérations d'alimentation sur les machines virtuelles, telles que la mise sous tension ou hors tension d'une machine virtuelle, l'interruption ou la réinitialisation d'une machine virtuelle, ou encore l'arrêt du système d'exploitation invité d'une machine virtuelle.

Mettre une machine virtuelle sous tension

La mise sous tension d'une machine virtuelle correspond à la mise sous tension d'une machine physique.

Vous ne pouvez pas mettre sous tension une machine virtuelle avec la personnalisation de l'invité activée, à moins que la machine virtuelle possède une version courante de VMware Tools installée.

Conditions préalables

La machine virtuelle est hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle que vous voulez démarrer, sélectionnez **Mettre sous tension**.

Résultats

Une machine virtuelle sous tension affiche un état Sous tension en vert.

Mettre une machine virtuelle hors tension

La mise hors tension d'une machine virtuelle correspond à la mise hors tension d'une machine physique.

Conditions préalables

La machine virtuelle est sous tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle que vous souhaitez mettre hors tension, sélectionnez **Mettre hors tension**.

Résultats

Une machine virtuelle hors tension affiche un état Hors tension en rouge.

Arrêter un système d'exploitation invité

L'arrêt du système d'exploitation invité d'une machine virtuelle équivaut à mettre hors tension une machine physique.

Conditions préalables

La machine virtuelle et le système d'exploitation invité doivent être sous tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle, sélectionnez **Arrêter le SE invité**.

Résultats

Le système d'exploitation invité est arrêté.

Réinitialiser une machine virtuelle

La réinitialisation d'une machine virtuelle efface l'état (mémoire, cache, etc.), mais la machine virtuelle continue à s'exécuter. La réinitialisation d'une machine virtuelle équivaut à appuyer sur le bouton de réinitialisation d'une machine physique. Elle lance une réinitialisation matérielle du système d'exploitation sans changer l'état d'alimentation de la machine virtuelle.

Conditions préalables

La machine virtuelle est sous tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle que vous souhaitez réinitialiser, sélectionnez **Réinitialiser**.

Résultats

L'état de la machine virtuelle est effacé.

Suspendre une machine virtuelle

L'interruption d'une machine virtuelle préserve son état actuel en écrivant la mémoire sur le disque.

La fonctionnalité d'interruption et de reprise est utile lorsque vous souhaitez enregistrer l'état actuel de votre machine virtuelle et reprendre votre travail ultérieurement à partir de ce même état.

Conditions préalables

La machine virtuelle est sous tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle que vous souhaitez interrompre, sélectionnez **Interrompre**.

Résultats

La machine virtuelle est interrompue, mais son état est préservé.

Ignorer l'état interrompu d'une machine virtuelle

Si une machine virtuelle est à l'état d'interruption et que vous n'avez plus besoin de recommencer à utiliser cette machine, vous pouvez ignorer l'état d'interruption. Lorsque vous ignorez l'état d'interruption, vous supprimez la mémoire enregistrée et ramenez la machine à un état hors tension.

Conditions préalables

Une machine virtuelle qui est interrompue.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle, sélectionnez **Ignorer l'état d'interruption**.

Résultats

L'état est ignoré et la machine virtuelle est mise hors tension.

Installer VMware Tools sur une machine virtuelle

vCloud Director dépend de VMware Tools pour personnaliser le SE invité.

VMware Tools améliore la gestion et les performances de la machine virtuelle en remplaçant les pilotes génériques du système d'exploitation par des pilotes VMware adaptés au matériel virtuel. Vous installez VMware Tools dans le système d'exploitation invité. Bien que le système d'exploitation invité puisse fonctionner sans VMware Tools, vous perdez beaucoup en fonctionnalité et en commodité.

Conditions préalables

- La machine virtuelle doit être sous tension.
- Si la machine virtuelle que vous venez de créer n'a pas de système d'exploitation invité, vous devez d'abord en installer un si vous voulez installer VMware Tools.
- La personnalisation de l'invité doit être désactivée avant d'installer VMware Tools.
- Si la version de VMware Tools est antérieure à 7299 sur une machine virtuelle de votre vApp, vous devez procéder à une mise à niveau.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle sur laquelle vous souhaitez installer VMware Tools, sélectionnez **Installer VMware Tools**.

   VMware Tools est installé sur le système d'exploitation invité cible. Si une erreur se produit lors de l'installation, un message d'erreur s'affiche. Vous pouvez également afficher la progression de l'installation dans la fenêtre **Tâches**.
4. Pour ouvrir la console Web de la machine virtuelle, dans le menu **Actions**, sélectionnez **Lancer la console Web**.
5. Suivez les instructions de l'article 1014294 de la base de connaissances VMware pour configurer VMware Tools en fonction de votre système d'exploitation particulier.

Résultats

VMware Tools est installé et configuré sur le système d'exploitation invité.

Mettre à niveau la version matérielle virtuelle pour une machine virtuelle

Vous pouvez mettre à niveau la version matérielle virtuelle pour une machine virtuelle. Les versions ultérieures du matériel virtuel prennent en charge davantage de fonctionnalités.

Vous ne pouvez pas rétrograder la version matérielle des machines virtuelles dans un vApp.

vCloud Director prend en charge les versions matérielles en fonction des ressources vSphere sous-jacentes. La version matérielle prise en charge dépend de la dernière version du matériel virtuel prise en charge dans le VDC fournisseur sous-jacent. Un **administrateur d'organisation** ou un **administrateur système** peut définir la version matérielle sur une version antérieure à la dernière version prise en charge par le matériel sous-jacent. Le portail de locataires vCloud Director définit dynamiquement la liste des versions du matériel virtuel pouvant être sélectionné en fonction du matériel sous-jacent du VDC d'organisation ou fournisseur.

Pour plus d'informations sur les fonctions matérielles disponibles avec les paramètres de compatibilité de machine virtuelle, consultez le document *Administration d'une machine virtuelle vSphere*.

Pour plus d'informations sur les produits VMware et la version de leur matériel virtuel, consultez l'article https://kb.vmware.com/s/article/1003746.

Conditions préalables

- Arrêtez la machine virtuelle ou le vApp qui contient la machine virtuelle.
- Vérifiez que la dernière version de VMware Tools est installée sur la machine virtuelle.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle que vous souhaitez mettre à niveau, sélectionnez **Mettre à niveau la version du matériel virtuel**.
4. Cliquez sur **OK**.

Résultats

La machine virtuelle est mise à niveau vers la dernière version.

Modifier les propriétés d'une machine virtuelle

Vous pouvez modifier les propriétés d'une machine virtuelle, y compris le nom et la description de la machine virtuelle, les paramètres de matériel et de réseau, les paramètres du système d'exploitation invité, etc.

Changer les propriétés générales d'une machine virtuelle

Vous pouvez vérifier et changer le nom, la description et les autres propriétés générales d'une machine virtuelle.

Conditions préalables

La modification de propriétés telles que le système d'exploitation nécessite que la machine soit hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans la fiche de la machine virtuelle que vous souhaitez modifier, cliquez sur **Détails**.
4. La liste des propriétés que vous pouvez afficher ou modifier sous **Général** est développée par défaut.

Option	Action
Nom de la machine virtuelle	Modifiez le nom de la machine virtuelle. Vous pouvez modifier cette propriété lorsque la machine virtuelle est sous tension.
Nom de l'ordinateur	Modifiez le nom de l'ordinateur ou de l'hôte défini dans le système d'exploitation invité qui identifie la machine virtuelle sur un réseau. Ce champ est limité à 15 caractères en raison d'une restriction du SE Windows sur les noms d'ordinateur. Vous pouvez modifier cette propriété lorsque la machine virtuelle est sous tension.
Description	Modifiez la description facultative de la machine virtuelle. Vous pouvez modifier cette propriété lorsque la machine virtuelle est sous tension.
Famille de système d'exploitation	Sélectionnez une famille de systèmes d'exploitation dans le menu déroulant. Vous pouvez modifier cette propriété lorsque la machine virtuelle est hors tension. En outre, vous ne pouvez pas modifier cette propriété si un système d'exploitation est déjà présent sur la machine virtuelle.

Option	Action
Système d'exploitation	Sélectionnez un système d'exploitation dans le menu déroulant. Vous pouvez modifier cette propriété lorsque la machine virtuelle est hors tension. En outre, vous ne pouvez pas modifier cette propriété si un système d'exploitation est déjà présent sur la machine virtuelle.
Délai de démarrage	Indiquez le délai en millisecondes du report de démarrage. Le temps entre l'activation de la machine virtuelle et de sa sortie du BIOS et le lancement du logiciel de système d'exploitation invité peut être court. Vous pouvez modifier le délai de démarrage pour allouer plus de temps.
Stratégie de stockage	Dans le menu déroulant, sélectionnez la stratégie de stockage que doit utiliser la machine virtuelle. Vous pouvez modifier cette propriété lorsque la machine virtuelle est sous tension.
Centre de données virtuel	Affichez le nom du centre de données virtuel auquel cette machine virtuelle appartient.
VMware Tools	Vérifiez que VMware Tools est installé sur la machine virtuelle.
Version matérielle virtuelle	Affichez la version du matériel virtuel de la machine virtuelle.
Mettre à niveau vers :	Pour effectuer la mise à niveau, sélectionnez une version dans le menu déroulant.
Synchroniser l'heure	Cochez cette case pour activer la synchronisation de l'heure entre le système d'exploitation invité de la machine virtuelle et le centre de données virtuel sur lequel elle s'exécute.
Accéder à la configuration du BIOS	Décidez de forcer ou non l'entrée dans l'écran de configuration du BIOS au prochain démarrage de la machine virtuelle. Vous pouvez modifier cette propriété lorsque la machine virtuelle est hors tension.

5 Une fois que vous avez terminé vos modifications, cliquez sur **Enregistrer**.

Changer les propriétés matérielles d'une machine virtuelle

Vous pouvez vérifier et modifier les propriétés matérielles d'une machine virtuelle.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Dans la fiche de la machine virtuelle que vous souhaitez modifier, cliquez sur **Détails**.

4 Cliquez sur **Matériel** pour développer la liste des propriétés matérielles que vous pouvez afficher et modifier.

Option	Description
Nombre de processeurs virtuels	Modifiez le nombre de processeurs. Le nombre maximal de processeurs virtuels pouvant être attribués à une machine virtuelle dépend du nombre de processeurs logiques sur l'hôte et du type de système d'exploitation invité installé sur la machine virtuelle.
Cœurs par socket	Modifiez les cœurs par socket. Vous pouvez configurer la façon dont les processeurs virtuels sont attribués en matière de cœurs et de cœurs par socket. Déterminez le nombre de CPU que la machine virtuelle doit avoir, puis sélectionnez le nombre de cœurs de chaque socket, selon que vous désirez un processeur monocœur, double cœur, triple cœur, etc.
Exposer la virtualisation de processeur assistée par le matériel au système d'exploitation client	Vous pouvez afficher la virtualisation complète du CPU au système d'exploitation invité afin que les applications qui exigent une virtualisation du matériel puissent uniquement s'exécuter sans traduction binaire ou paravirtualisation.
Mémoire totale	Modifiez les paramètres de ressources mémoire d'une machine virtuelle. La taille de la mémoire de la machine virtuelle doit être un multiple de 4 Mo. Ce paramètre détermine la quantité de mémoire de l'hôte ESXi allouée à la machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications qui s'exécutent dans la machine virtuelle. Une machine virtuelle ne peut pas bénéficier de plus de ressources mémoire que sa taille de mémoire matérielle virtuelle configurée.
Ajout de mémoire à chaud	Si vous activez l'ajout de mémoire à chaud, vous pouvez ajouter des ressources de mémoire à une machine virtuelle lorsque la machine est sous tension. Cette fonctionnalité est prise en charge uniquement sur certains systèmes d'exploitation invités et sur certaines versions matérielles de machine virtuelle ultérieures à la version 7.
Ajout à chaud de processeur virtuel	Si vous activez l'ajout de processeur virtuel à chaud, vous pouvez ajouter des processeurs virtuels à la machine virtuelle lorsqu'elle est sous tension. Vous pouvez ajouter uniquement des multiples du nombre de cœurs par socket. Cette fonctionnalité est prise en charge uniquement sur certains systèmes d'exploitation invités et sur certaines versions matérielles de machine virtuelle.
Nombre de sockets	Affichez le nombre de sockets. Le nombre de sockets est déterminé par le nombre de CPU virtuels disponibles. Ce nombre est modifié lorsque vous mettez à jour le nombre de processeurs virtuels.
Support amovible	Affichez les supports amovibles disponibles, comme un lecteur de CD/DVD ou un lecteur de disquettes associé.

5 Sous **Disques durs**, cliquez sur **Ajouter** pour ajouter un disque dur.

Option	Description
Taille	Entrez la taille de disque dur en Mo. Vous pourrez augmenter la taille du disque dur ultérieurement. **Note** Vous pouvez augmenter la taille d'un disque dur existant si la machine virtuelle n'est pas un clone lié et qu'elle n'a pas de snapshot.
Stratégie	La stratégie de stockage pour la machine virtuelle est utilisée par défaut. Par défaut, tous les disques durs associés à une machine virtuelle utilisent la stratégie de stockage spécifiée pour la machine virtuelle. Vous pouvez remplacer ce paramètre par défaut pour l'un de ces disques lorsque vous créez une machine virtuelle ou modifiez ses propriétés. La colonne Taille de chaque disque dur inclut un menu déroulant qui répertorie toutes les stratégies de stockage disponibles pour cette machine virtuelle.
IOPS	Sélectionnez un IOPS spécifique pour le disque. Utilisez cette option pour limiter le nombre d'opérations d'E/S par seconde par disque.
Type de bus	Sélectionnez le type de bus. Les options disponibles sont **Paravirtuel (SCSI)**, **Parallèle LSI Logic (SCSI)**, **LSI Logic SAS (SCSI)**, **IDE** et **SATA**. Pour plus d'informations sur les types et la compatibilité des contrôleurs de stockage, reportez-vous au *Guide d'administration de machine virtuelle vSphere*.
Numéro de bus	Entrez le numéro de bus.
Numéro d'unité	Entrez le numéro d'unité logique pour le disque dur.

6 Sous **Cartes réseau**, cliquez sur **Ajouter** pour ajouter une nouvelle carte réseau.

Vous pouvez ajouter jusqu'à 10 cartes réseau. Pour plus d'informations sur le nombre de cartes réseau prises en charge en fonction de la version matérielle de la machine virtuelle, reportez-vous à l'article suivant : http://kb.vmware.com/s/article/2051652. vCloud Director prend en charge la modification des cartes réseau de machine virtuelle pendant l'exécution de la machine virtuelle. Pour plus d'informations sur les types de cartes réseau pris en charge, consultez l'article http://kb.vmware.com/kb/1001805.

Option	Description
Carte réseau principale	Un indicateur s'affiche lorsque la carte réseau principale est sélectionnée. Sélectionnez une carte réseau principale. Le paramètre de carte réseau principale détermine la passerelle unique par défaut de la machine virtuelle. La machine virtuelle peut utiliser n'importe quelle carte réseau pour se connecter à des machines virtuelles et physiques qui sont directement connectées au même réseau que la carte réseau, mais elle peut uniquement utiliser la carte principale pour se connecter à des machines sur des réseaux qui nécessitent une connexion de passerelle.
Carte réseau	Numéro de la carte réseau.
Connectée	Cochez la case pour connecter une carte réseau.
Réseau	Sélectionnez un réseau dans le menu déroulant.

Option	Description
Mode IP	Sélectionnez un mode IP : ■ **Statique - Pool IP** Récupère une adresse IP statique depuis le pool d'adresses IP réseau. ■ **Statique - Manuel** Vous permet de spécifier manuellement une adresse IP spécifique. Si vous sélectionnez cette option, vous devez saisir une adresse IP dans la colonne **Adresse IP**. ■ **DHCP** Récupère une adresse IP depuis un serveur DHCP.
Adresse MAC	Entrez l'adresse MAC de l'interface réseau.

7 Cliquez sur **Enregistrer**.

Modifier les propriétés de personnalisation du système d'exploitation invité d'une machine virtuelle

La personnalisation du système d'exploitation invité sur vCloud Director est facultative pour toutes les plates-formes. Elle est nécessaire pour les machines virtuelles qui doivent joindre un domaine Windows.

Certaines des informations demandées sur ce menu s'appliquent uniquement aux plates-formes Windows. Le panneau Personnalisation du système d'exploitation invité comporte les informations nécessaires pour que la machine virtuelle puisse joindre un domaine Windows. Un **administrateur d'organisation** peut spécifier des valeurs par défaut pour un domaine que les invités Windows dans cette organisation peuvent joindre. Toutes les machines virtuelles Windows ne doivent pas joindre un domaine, mais dans la plupart des installations d'entreprise, une machine virtuelle qui n'est pas un membre du domaine ne peut pas accéder à beaucoup de ressources réseau disponibles.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de vApp** prédéfini ou un ensemble de droits équivalent.
- La personnalisation du système d'exploitation invité exige que la machine virtuelle exécute VMware Tools.
- Avant que vous puissiez personnaliser un système d'exploitation invité Windows, votre **administrateur système** doit installer les fichiers Microsoft Sysprep appropriés sur le groupe vCloud Director Server. Reportez-vous au *Guide d'installation et de mise à niveau de vCloud Director*.
- La personnalisation des systèmes d'exploitation invités Linux exige que Perl soit installé sur le système d'exploitation invité.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Dans la fiche de la machine virtuelle que vous souhaitez modifier, cliquez sur **Détails**.

4 Cliquez sur **Personnalisation et propriétés du système d'exploitation invité** pour développer la liste des paramètres du système d'exploitation invité.

Option	Description
Activer la personnalisation du client	Sélectionnez cette option pour activer la personnalisation de l'invité.
Modifier le SID	Sélectionnez cette option pour modifier l'ID de sécurité (SID) Windows. Cette option est spécifique aux machines virtuelles exécutant un système d'exploitation invité Windows. Le SID est utilisé par certains systèmes d'exploitation Windows pour identifier de manière unique les systèmes et les utilisateurs. Si vous ne cochez pas cette option, la nouvelle machine virtuelle portera le même SID que la machine virtuelle ou le modèle sur lequel elle se base. Les doublons de SID ne posent pas problème quand les ordinateurs font partie d'un domaine et que seuls des comptes d'utilisateurs de domaine sont utilisés. Par contre, si les machines font partie d'un groupe de travail ou si des comptes d'utilisateurs locaux sont utilisés, les doublons de SID peuvent compromettre les contrôles d'accès aux fichiers. Pour plus d'informations, reportez-vous à la documentation de votre système d'exploitation Microsoft Windows.
Autoriser le mot de passe d'administrateur local	Sélectionnez cette option pour permettre la définition d'un mot de passe d'administrateur sur le système d'exploitation invité. a Spécifiez un mot de passe pour l'administrateur local. Si vous laissez la zone de texte **Spécifier le mot de passe** vide, un mot de passe est généré automatiquement. b Spécifiez le nombre de connexions automatiques autorisées. Si vous entrez une valeur égale à zéro, la connexion automatique en tant qu'administrateur est désactivée.
Les administrateurs doivent modifier le mot de passe lors de la première connexion.	Sélectionnez cette option pour contraindre les administrateurs de modifier le mot de passe du système d'exploitation invité lors de la première connexion. Cela est recommandé pour des raisons de sécurité.
Génération automatique de mot de passe	Sélectionnez cette option pour autoriser la génération automatique de mot de passe.

Option	Description
Autoriser cette machine virtuelle à joindre un domaine	Vous pouvez sélectionner cette option pour joindre la machine virtuelle à un domaine Windows. Vous pouvez choisir d'utiliser le domaine de l'organisation ou de remplacer le domaine de l'organisation et d'entrer les propriétés du domaine. a Entrez un nom de domaine. b Entrez le nom d'utilisateur et le mot de passe. c Entrez l'unité d'organisation de compte.
Script	Vous pouvez utiliser un script de personnalisation pour modifier le système d'exploitation invité de la machine virtuelle. Lorsque vous ajoutez un script de personnalisation à une machine virtuelle, le script est appelé uniquement en cas de personnalisation initiale et de repersonnalisation forcée. Si vous définissez le paramètre de ligne de commande `precustomization`, le script est appelé avant le début de la personnalisation du client. Si vous définissez le paramètre de ligne de commande `postcustomization`, le script est appelé une fois la personnalisation du client terminée. ■ Cliquez sur le bouton de téléchargement situé sous la zone de texte du script pour accéder à un script de personnalisation sur votre machine locale. ■ Saisissez le script de personnalisation directement dans la zone de texte **Fichier de script**. Le script de personnalisation que vous saisissez directement dans la zone de texte **Fichier de script** ne peut pas contenir plus de 1 500 caractères. Pour plus d'informations, consultez l'article de la base de connaissances VMware à l'adresse https://kb.vmware.com/kb/1026614.

5 Une fois que vous avez terminé vos modifications, cliquez sur **Enregistrer**.

Description de la personnalisation du client

Lorsque vous personnalisez votre système d'exploitation client, vous devez connaître certains paramètres et options.

Case à cocher Activer la personnalisation du client

Cette case à cocher se situe sous l'onglet **Personnalisation du système d'exploitation client** de la page **Propriétés** de la machine virtuelle. L'objectif de la personnalisation du client est de configurer en fonction des options sélectionnées dans la page **Propriétés**. Si cette case est cochée, la personnalisation et la repersonnalisation d'invité sont effectuées lorsque cela est nécessaire.

Ce processus est requis pour garantir le bon fonctionnement des fonctionnalités de personnalisation d'invité, telles que le nom de l'ordinateur, les paramètres réseau, la définition et l'expiration des mots de passe de l'administrateur/racine, la modification du SID pour les systèmes d'exploitation Windows, etc. Cette option doit être cochée pour que **Mettre sous tension et forcer la re-personnalisation** fonctionne.

Si cette case est cochée et si les paramètres de configuration de la machine virtuelle dans vCloud Director ne sont pas synchronisés avec ceux du système d'exploitation invité, l'onglet **Profil** sur la page **Propriétés** indique que les paramètres ne sont pas synchronisés avec le système d'exploitation invité et que la machine virtuelle a besoin d'une personnalisation d'invité.

Personnalisation d'invité pour les vApp et les machines virtuelles

Les cases sont décochées.

- **Activer la personnalisation du client**
- Dans les SE clients Windows, **Modifier le SID**
- **Réinitialisation de mot de passe**

Si vous souhaitez procéder à une personnalisation (ou si vous avez apporté des modifications aux paramètres réseau qui doivent se refléter dans le système d'exploitation invité), vous pouvez cocher la case **Activer la personnalisation de l'invité** et définir les options dans l'onglet **Personnalisation du système d'exploitation invité** de la page **Propriétés** de la machine virtuelle. Lorsque les machines virtuelles des modèles de vApp sont utilisées pour créer un vApp, puis pour ajouter une machine virtuelle, les modèles de vApp agissent comme des blocs fonctionnels. Lorsque vous ajoutez des machines virtuelles du catalogue dans un nouveau vApp, les machines virtuelles sont activées pour la personnalisation du client par défaut. Lorsque vous enregistrez un modèle de vApp depuis un catalogue en tant que vApp, les machines virtuelles sont activées pour la personnalisation du client uniquement si la case **Activer la personnalisation du client** est cochée.

Voici les valeurs par défaut des paramètres de personnalisation du client :

- La case à cocher **Activer la personnalisation de l'invité** est identique à la machine virtuelle source de votre catalogue.
- Pour les machines virtuelles clientes Windows, l'option **Modifier le SID** est identique à la machine virtuelle source de votre catalogue.
- Le paramètre de réinitialisation du mot de passe est identique à la machine virtuelle source de votre catalogue.

Vous pouvez décocher la case **Activer la personnalisation de l'invité** si nécessaire avant de démarrer le vApp.

Si des machines virtuelles vides sur lesquelles un SE client doit encore être installé sont ajoutées au vApp, la case **Activer la personnalisation du client** est décochée par défaut car ces machines virtuelles ne sont pas encore prêtes pour la personnalisation.

Après avoir installé le SE client et VMware Tools, vous pouvez mettre les machines virtuelles hors tension, arrêter le vApp, cocher la case **Activer la personnalisation du client** et démarrer le vApp et les machines virtuelles pour procéder à la personnalisation du client.

Si le nom de la machine virtuelle et les paramètres réseau sont mis à jour sur une machine virtuelle qui a été personnalisée, la prochaine fois que vous mettez la machine virtuelle sous tension, elle est repersonnalisée, ce qui resynchronise la machine virtuelle invitée avec vCloud Director.

Mettre sous tension et forcer la re-personnalisation d'une machine virtuelle

Vous pouvez mettre une machine virtuelle sous tension et forcer la repersonnalisation d'une machine virtuelle.

Si les paramètres d'une machine virtuelle ne sont pas synchronisés avec vCloud Director ou si une tentative de personnalisation de l'invité a échoué, vous pouvez forcer la repersonnalisation de la machine virtuelle.

Assurez-vous que l'application en cours d'exécution dans la machine virtuelle prend en charge une repersonnalisation. Si vous modifiez un contrôleur de domaine à l'aide de Microsoft Sysprep et que vous modifiez le SID, la machine virtuelle risque d'être endommagée. Afin de réduire le risque d'endommager votre machine virtuelle, créez un snapshot avant la repersonnalisation.

Conditions préalables

- Vous devez être un administrateur d'organisation.
- La machine virtuelle doit être hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Alimentation** de la machine virtuelle que vous souhaitez activer et personnaliser, sélectionnez **Mettre sous tension et forcer la repersonnalisation**.

Résultats

La machine virtuelle est repersonnalisée et mise sous tension.

Changer les propriétés avancées d'une machine virtuelle

Dans les paramètresavancés, utilisez les paramètres d'allocation des ressources (parts, réservation et limite) pour déterminer la quantité de ressources fournie pour une machine virtuelle en termes de CPU, de mémoire et de stockage.

Utilisez les paramètres d'allocation de ressources (parts, réservation et limite) pour déterminer le volume de ressources processeur, mémoire et de stockage fourni pour une machine virtuelle.

Parts d'allocation de ressources

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 d'une ressource qu'une autre machine virtuelle, elle est autorisée à consommer le double de cette ressource lorsque ces deux machines virtuelles sont en compétition pour les ressources. Les parts sont habituellement spécifiées en tant que Élevé, Normal ou Faible et ces valeurs spécifient les valeurs de part avec un ratio 4:2:1, respectivement. Vous pouvez également sélectionner Personnalisé pour attribuer un nombre spécifique de parts (qui exprime un poids proportionnel) à chaque machine virtuelle. Lorsque vous attribuez des parts à une machine virtuelle, vous spécifiez toujours la priorité pour cette machine virtuelle par rapport aux autres machines virtuelles sous tension.

Réservation d'allocation de ressources

Spécifie l'allocation minimale garantie pour une machine virtuelle. vCloud Director permet de mettre sous tension une machine virtuelle uniquement s'il y a suffisamment de ressources non réservées pour répondre à la réservation de la machine virtuelle. Le centre de données virtuel garantit le nombre de ressources, même si ses ressources sont très chargées. La réservation est exprimée en unités concrètes (mégahertz ou mégaoctets).

Supposons par exemple, que vous disposiez de 2 GHz disponibles et que vous spécifiez une réservation d'allocation de ressources de 1 GHz pour la machine virtuelle 1 et de 1 GHz pour la machine virtuelle 2. Chaque machine virtuelle est désormais assurée de recevoir 1 GHz si elle en a besoin. Cependant, si la machine virtuelle 1 n'utilise que 500 MHz, la machine virtuelle 2 peut utiliser 1,5 GHz.

Par défaut, la réservation est à 0. Vous pouvez spécifier une réservation si vous devez garantir que les volumes minimum requis de processeur ou de mémoire sont toujours disponibles pour la machine virtuelle.

Limite d'allocation de ressources

Cette limite spécifie un lien supérieur pour les ressources de CPU et de mémoire qui peuvent être allouées à une machine virtuelle. Un centre de données virtuel peut allouer plus que la réservation à une machine virtuelle, mais il n'alloue jamais plus que la limite, même si des ressources ne sont pas utilisées dans le système. La limite est exprimée en unités concrètes (mégahertz ou mégaoctets).

Par défaut, les limites de ressources mémoire et processeur sont illimitées. Lorsque la limite de mémoire est illimitée, le volume de mémoire configuré pour la machine virtuelle lors de sa création devient sa limite effective dans la plupart des cas.

Dans la plupart des cas, il n'est pas nécessaire de spécifier une limite. Vous risqueriez de perdre des ressources inactives si vous spécifiez une limite. Le système ne permet pas à une machine virtuelle d'utiliser plus de ressources que la limite, même lorsque le système est sous-utilisé et que des ressources inactives sont disponibles. Spécifiez une limite uniquement si vous avez de bonnes raisons de le faire.

Conditions préalables

- Centre de données virtuel de pool de réservation.
- Assurez-vous que le centre de données de données virtuel fournit une certaine quantité de mémoire pour une machine virtuelle
- et qu'une machine virtuelle particulière se voit toujours allouer un pourcentage supérieur de ressources de centre de données virtuel par rapport aux autres machines virtuelles.
- Définir un lien supérieur sur les ressources qui peut être alloué à une machine virtuelle.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans la fiche de la machine virtuelle que vous souhaitez modifier, cliquez sur **Détails**.
4. Cliquez sur **Avancé**.
5. Définissez les parts d'allocation de ressources pour les paramètres de CPU en sélectionnant une option dans le menu déroulant **Priorité**.

Option	Description
Faible	Alloue 500 parts par CPU virtuel.
Normal	Alloue 1 000 parts par CPU virtuel.
Élevé	Alloue 2 000 parts par CPU virtuel.
Personnalisé	Vous permet d'attribuer un nombre spécifique de parts en entrant le nombre de parts (qui exprime un poids proportionnel) pour chaque machine virtuelle. Lorsque vous attribuez des parts à une machine virtuelle, vous spécifiez toujours la priorité pour cette machine virtuelle par rapport aux autres machines virtuelles sous tension.

6. Spécifiez la réservation pour les paramètres de CPU en saisissant la réservation en MHz et, éventuellement, la limite pour les paramètres de CPU en MHz.

Option	Description
Illimité	Option de ressource de CPU par défaut.
Maximum	Spécifiez un lien supérieur pour les ressources de CPU qui peuvent être allouées à une machine virtuelle en MHz.

7 Définissez les parts d'allocation de ressources pour les paramètres de mémoire en sélectionnant une option dans le menu déroulant **Priorité**.

Option	Description
Faible	Alloue 5 parts par mégaoctet de la mémoire configurée de la machine virtuelle.
Normal	Alloue 10 parts par mégaoctet de la mémoire configurée de la machine virtuelle.
Élevé	Alloue 20 parts par mégaoctet de la mémoire configurée de la machine virtuelle.
Personnalisé	Vous permet d'attribuer un nombre spécifique de parts en entrant le nombre de parts.

8 Spécifiez la réservation pour les paramètres de mémoire en Mo et, éventuellement, la limite pour les paramètres de mémoire en Mo.

Option	Description
Illimité	Option de ressource de CPU par défaut.
Maximum	Spécifiez un lien supérieur pour les ressources de CPU qui peuvent être allouées à une machine virtuelle en MHz.

9 Cliquez sur **Ajouter** sous **Métadonnées** pour spécifier les métadonnées.

Par exemple, vous pouvez ajouter des métadonnées sur la date de création ou sur le propriétaire.

10 Une fois que vous avez terminé vos modifications, cliquez sur **Enregistrer**.

Insérer un support

Vous pouvez insérer un support, comme des images de CD/DVD, à partir des catalogues pour les utiliser dans un système d'exploitation invité de machine virtuelle. Vous pouvez utiliser ces fichiers de support pour installer un système d'exploitation dans la machine virtuelle, diverses applications, pilotes et ainsi de suite.

Conditions préalables

Vous avez accès à un catalogue avec des fichiers de support.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Sélectionnez la machine virtuelle sur laquelle vous souhaitez ajouter le support.

4 Dans le menu **Actions**, sélectionnez **Insérer un support**.

5 Dans la fenêtre **Insérer un CD**, sélectionnez le fichier du support à insérer dans la machine virtuelle.

6 Cliquez sur **Insérer**.

Éjecter un support

Lorsque vous avez terminé d'utiliser un CD ou un DVD sur votre machine virtuelle, vous pouvez éjecter le fichier de support.

Conditions préalables

Un fichier de support a été inséré précédemment dans la machine virtuelle.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Sélectionnez la machine virtuelle pour laquelle vous souhaitez éjecter le support.

4 Dans le menu **Actions**, sélectionnez **Éjecter un support**.

Résultats

Le fichier de support est éjecté.

Copier une machine virtuelle vers un autre vApp

Vous pouvez copier une machine virtuelle dans un autre vApp. Lorsque vous copiez une machine virtuelle, la machine virtuelle d'origine reste dans le vApp source.

Lorsque vous copiez une machine virtuelle, les snapshots ne sont pas inclus dans la copie.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de vApp** prédéfini ou un ensemble de droits équivalent.
- Mettez hors tension la machine virtuelle.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle à copier, sélectionnez **Copier vers**.
4. Sélectionnez le vApp de destination vers lequel vous souhaitez copier la machine virtuelle, puis cliquez sur **Suivant**.
5. Configurez les ressources, comme le nom de la machine virtuelle et le nom de l'ordinateur et, le cas échéant, la stratégie de stockage et les cartes réseau, puis cliquez sur **Suivant**.

   Important Le nom de l'ordinateur ne peut contenir que des caractères alphanumériques et des traits d'union. Il ne peut pas être composé de chiffres uniquement et ne peut pas contenir d'espaces.
6. Sur la page **Prêt à terminer**, vérifiez les paramètres et cliquez sur **Terminé**.

Déplacer une machine virtuelle vers un autre vApp

Vous pouvez copier une machine virtuelle dans un autre vApp. Lorsque vous déplacez une machine virtuelle, la machine virtuelle d'origine est supprimée du vApp source.

Lorsque vous déplacez une machine virtuelle vers un vApp différent, les snapshots que vous avez pris sont perdus.

À partir de vCloud Director 9.5, le déplacement des machines virtuelles entre les différents vApp s'appuie sur VMware vSphere® vMotion® et Enhanced vMotion Compatibility (EVC). Vous pouvez déplacer une machine virtuelle vers un autre vApp appartenant au même ou à un autre VDC d'organisation au sein du même VDC fournisseur.

Lorsque vous déplacez une machine virtuelle vers un autre vApp, vous pouvez effectuer des reconfigurations, comme la modification du réseau et du profil de stockage.

Tableau 2-1. Reconfigurations pendant les mouvements de machine virtuelle et les états de machine virtuelle

Reconfiguration	État de la machine virtuelle si le vApp cible se trouve dans le même VDC d'organisation	État de la machine virtuelle si le vApp cible se trouve dans un autre VDC d'organisation au sein du même VDC fournisseur
modifier le réseau	hors tension	S/O
supprimer le réseau	sous tension ou hors tension	S/O
modifier le profil de stockage	sous tension ou hors tension	hors tension

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de vApp** prédéfini ou un ensemble de droits équivalent.
- Vérifiez que les ressources vSphere sous-jacentes prennent en charge vMotion et EVC. Pour plus d'informations sur les conditions requises et limitations de vMotion et EVC, reportez-vous à la section *Gestion de vCenter Server et des hôtes*.
- Si vous souhaitez modifier le réseau de la machine virtuelle ou le profil de stockage, vérifiez si vous devez mettre la machine virtuelle hors tension. Reportez-vous au tableau *Reconfigurations au cours de mouvements de machine virtuelle et d'états de machine virtuelle*.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine que vous souhaitez déplacer, sélectionnez **Déplacer vers**.
4. Sélectionnez le vApp de destination, puis cliquez sur **Suivant**.
5. Configurez les ressources, comme le nom de la machine virtuelle et le nom de l'ordinateur et, le cas échéant, la stratégie de stockage et les cartes réseau, puis cliquez sur **Suivant**.

   Important Le nom de l'ordinateur ne peut contenir que des caractères alphanumériques et des traits d'union. Il ne peut pas être composé de chiffres uniquement et ne peut pas contenir d'espaces.
6. Sur la page **Prêt à terminer**, vérifiez les paramètres et cliquez sur **Terminé**.

Affinité et anti-affinité des machines virtuelles

Les règles d'affinité et d'anti-affinité vous permettent de répartir un groupe de machines virtuelles entre différents hôtes ESXi ou de conserver un groupe de machines virtuelles sur un hôte ESXi particulier.

Une règle d'affinité place un groupe de machines virtuelles sur un hôte spécifique afin de pouvoir effectuer facilement un audit de l'utilisation de ces machines virtuelles. Une règle d'anti-affinité répartit un groupe de machines virtuelles entre différents hôtes, ce qui empêche toutes les machines virtuelles de tomber simultanément en panne en cas d'échec d'un seul hôte.

Si les règles d'affinité ou d'anti-affinité ne peuvent pas être satisfaites, cela empêche la mise sous tension des machines virtuelles ajoutées à la règle.

Afficher des règles d'affinité et des règles d'anti-affinité

Vous pouvez afficher des règles existantes d'affinité et d'anti-affinité et leurs propriétés, par exemple les machines virtuelles concernées par les règles et déterminer si les règles sont activées.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Règles d'affinité** dans le panneau de gauche.
2. (Facultatif) Cliquez sur l'icône **Éditeur de grille** ( ) et sélectionnez les détails sur les règles que vous souhaitez afficher.

Résultats

Vous voyez la liste des règles d'affinité et d'anti-affinité existantes, les machines virtuelles et l'état activé de chaque règle.

Créer une règle d'affinité

Créez une règle d'affinité pour placer un groupe spécifique de machines virtuelles sur un seul hôte afin de pouvoir effectuer un audit de l'utilisation de ces machines.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Règles d'affinité** dans le panneau de gauche.
2. Sous **Règles d'affinité**, cliquez sur **Nouveau**.
3. Entrez un nom pour la règle.
4. Décochez **Activé** pour créer la règle sans l'activer.

   Par défaut, la case est cochée et les règles sont activées après leur création.

5 Laissez la case **Requis** cochée.

Par défaut, chaque règle d'affinité est requise. Cela signifie que si la règle ne peut pas être respectée, les machines virtuelles ajoutées à la règle ne sont pas mises sous tension.

6 Sélectionnez les machines virtuelles à ajouter à la règle d'affinité.

7 Cliquez sur **Enregistrer**.

Résultats

vCloud Director place les machines virtuelles associées à la règle d'affinité sur un hôte spécifique.

Créer une règle d'anti-affinité

Créez une règle d'anti-affinité pour placer un groupe spécifique de machines virtuelles sur plusieurs hôtes afin d'empêcher une panne simultanée de ces machines virtuelles si un hôte spécifique tombe en panne.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Règles d'affinité** dans le panneau de gauche.

2 Sous **Règles d'anti-affinité**, cliquez sur **Nouveau**.

3 Entrez un nom pour la règle.

4 Décochez **Activé** pour créer la règle sans l'activer.

Par défaut, la case est cochée et les règles sont activées après leur création.

5 Laissez la case **Requis** cochée.

Par défaut, chaque règle d'anti-affinité est requise. Cela signifie que si la règle ne peut pas être respectée, les machines virtuelles ajoutées à la règle ne sont pas mises sous tension.

6 Sélectionnez les machines virtuelles à ajouter à la règle d'anti-affinité.

7 Cliquez sur **Enregistrer**.

Résultats

vCloud Director place les machines virtuelles associées à la règle d'anti-affinité sur plusieurs hôtes.

Modifier une règle d'affinité ou d'anti-affinité

Vous pouvez modifier une règle d'anti-affinité pour activer ou désactiver la règle, ajouter ou supprimer des machines virtuelles, modifier le nom ou les préférences de la règle.

Conditions préalables

Cette opération nécessite le droit d'accès `Organization vDC: VM-VM Affinity Edit` . Ce droit d'accès est inclus dans les rôles prédéfinis **Auteur de catalogue**, **Auteur de vApp** et **Administrateur d'organisation**.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Règles d'affinité** dans le panneau de gauche.
2. Sélectionnez la case d'option en regard du nom de la règle à modifier et cliquez sur **Modifier**.
3. Modifiez les propriétés de la règle.
   a. Modifiez le nom de la règle si nécessaire.
   b. Choisissez d'activer ou de désactiver la règle.
   c. Laissez la case **Requis** cochée.
   d. Ajoutez davantage de machines virtuelles ou supprimez des machines virtuelles.
4. Cliquez sur **Enregistrer**.

Supprimer une règle d'affinité ou d'anti-affinité

Si vous souhaitez ne plus utiliser une règle d'affinité ou d'anti-affinité, vous pouvez la supprimer.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Règles d'affinité** dans le panneau de gauche.
2. Sélectionnez la case d'option en regard du nom de la règle à supprimer et cliquez sur **Supprimer**.
3. Pour confirmer la suppression de la règle, cliquez sur **OK**.

Résultats

vCloud Director supprime la règle d'affinité ou d'anti-affinité.

Surveiller les machines virtuelles

Si votre administrateur vCloud Director a activé la fonctionnalité de surveillance des machines virtuelles, vous pouvez afficher le graphique de surveillance dans le portail de locataires.

Cette fonctionnalité permet de comprendre l'état d'une machine virtuelle donnée dans le temps (jours, semaines ou mois).

Conditions préalables

Cette fonctionnalité est uniquement disponible si votre administrateur vCloud Director l'a activée.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Sélectionnez la machine virtuelle que vous souhaitez surveiller et cliquez sur **Détails**.

4 Cliquez sur **Graphique de surveillance** pour développer la vue de surveillance.

Le graphique de surveillance s'affiche.

5

6 Sélectionnez une option de mesure pour la surveillance des machines virtuelles.

La liste figurant dans le menu déroulant **Mesure** varie en fonction des choix de votre **administrateur système**. Vous voyez l'intégralité ou une partie des options disponibles.

Indicateur	Description
Dernier disque provisionné	Spécifié en Ko. Choisissez une vue par jour, par semaine ou par mois.
Moyenne de lecture du disque	Spécifiée sous forme de pourcentage. Choisissez une vue par jour, par semaine ou par mois.
Moyenne d'écriture du disque	Spécifiée sous forme de pourcentage. Choisissez une vue par jour, par semaine ou par mois.
Moyenne d'utilisation du CPU	Spécifiée sous forme de pourcentage. Choisissez une vue par jour, par semaine ou par mois.
Moyenne d'utilisation du CPU en MHz	Indiquée en MHz. Choisissez une vue par jour, par semaine ou par mois.
Utilisation maximale du CPU	Spécifiée sous forme de pourcentage. Choisissez une vue par jour, par semaine ou par mois.
Utilisation moyenne de mémoire	Spécifiée sous forme de pourcentage. Choisissez une vue par jour, par semaine ou par mois.
Disque utilisé en dernier	Spécifié en Ko. Choisissez une vue par jour, par semaine ou par mois.

Un nouveau graphique s'affiche chaque fois que vous sélectionnez une valeur différente dans la liste.

7 (Facultatif) Modifiez la période de la collecte des mesures.

8 Cliquez sur **Actualiser**.

9 Pour enregistrer les modifications, cliquez sur **Enregistrer**.

Utilisation des snapshots

Un snapshot conserve l'état et les données d'une machine virtuelle au moment où vous prenez le sanapshot. Lorsque vous créez un snapshot d'une machine virtuelle, cette machine virtuelle n'est pas affectée et seule une image de cette machine dans un état donné est copiée et stockée. Les snapshots sont utiles lorsque vous devez retourner à plusieurs reprises au même état de la machine virtuelle mais que vous ne souhaitez pas créer plusieurs machines virtuelles.

Les snapshots sont utiles en tant que solution à court terme pour tester un logiciel dont les effets sont inconnus ou potentiellement dangereux. Vous pouvez utiliser un snapshot comme point de restauration pendant un processus linéaire ou itératif, tel que l'installation de packages de mise à niveau, ou pendant un processus d'embranchement, tel que l'installation de différentes versions d'un programme.

Vous pouvez utiliser un snapshot lors de la mise à niveau du système d'exploitation d'une machine virtuelle. Par exemple, avant de mettre à niveau la machine virtuelle, vous prenez un snapshot pour conserver le point dans le temps avant la mise à niveau. S'il n'y a aucun problème lors de la mise à niveau, vous pouvez choisir de supprimer le snapshot, ce qui validera les modifications apportées au cours de la mise à niveau. Cependant, si vous avez rencontré un problème, vous pouvez restaurer le snapshot, ce qui va rétablir l'état de votre machine virtuelle enregistré avant la mise à niveau.

Avec vCloud Director, vous ne pouvez avoir qu'un seul snapshot d'une machine virtuelle. Chaque tentative de prendre un nouveau snapshot d'une machine virtuelle supprime le précédent.

Prendre un snapshot d'une machine virtuelle

Vous pouvez prendre un snapshot d'une machine virtuelle. Une fois que vous avez pris le snapshot, vous pouvez restaurer la machine virtuelle sur le snapshot ou supprimer le snapshot.

Conditions préalables

Vérifiez que la machine virtuelle n'est pas connectée à un disque nommé.

Note Les snapshots ne capturent pas les configurations de carte réseau.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.

3 Dans le menu **Actions** de la machine virtuelle pour laquelle vous souhaitez créer un snapshot, sélectionnez **Créer un snapshot**.

   La création du snapshot d'une machine virtuelle remplace le snapshot existant, le cas échéant.

4 (Facultatif) Indiquez si vous voulez créer un snapshot de la mémoire de la machine virtuelle.

   Lorsque vous capturez l'état de la mémoire de la machine virtuelle, le snapshot conserve l'état actif de la machine virtuelle. Les snapshots de mémoire permettent de créer un snapshot à un instant précis (par exemple, pour mettre à niveau un logiciel qui fonctionne parfaitement). Si vous créez un snapshot de mémoire et que la mise à niveau ne s'exécute pas correctement, ou si le logiciel ne vous convient pas, vous pouvez restaurer l'état précédent de la machine virtuelle.

   Lorsque vous capturez l'état de la mémoire, les fichiers de la machine virtuelle ne nécessitent aucune mise au repos. Si vous ne capturez pas l'état de la mémoire, le snapshot ne sauvegarde pas l'état actif de la machine virtuelle et les disques sont cohérent en cas d'incident à moins que vous ne les mettiez au repos.

5 (Facultatif) Indiquez si vous souhaitez mettre au repos le système de fichiers invité.

   Pour cette opération, VMware Tools doit être installé sur la machine virtuelle. Lorsque vous mettez au repos une machine virtuelle, VMware Tools met au repos le système de fichiers de la machine virtuelle. Une opération de mise au repos garantit qu'un disque de snapshot représente un état cohérent des systèmes de fichiers invités. Les snapshots mis au repos s'utilisent notamment lors des sauvegardes automatisées ou périodiques. Par exemple, si vous méconnaissez l'activité de la machine virtuelle, mais que vous souhaitiez disposer de plusieurs sauvegardes récentes, vous pouvez mettre les fichiers au repos.

   Les machines virtuelles équipées de disques haute capacité ne peuvent pas être mises au repos.

6 Cliquez sur **OK**.

Résultats

Le snapshot vous permet de restaurer votre machine virtuelle au snapshot le plus récent.

Restaurer une machine virtuelle à un snapshot

Vous pouvez restaurer une machine virtuelle à l'état dans lequel elle était lorsque le snapshot a été créé.

Conditions préalables

La machine virtuelle a un snapshot.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle dont vous souhaitez restaurer un snapshot, sélectionnez **Restaurer le snapshot**.
4. Cliquez sur **OK**.

Résultats

La machine virtuelle est restaurée au snapshot enregistré.

Supprimer un snapshot d'une machine virtuelle

Vous pouvez supprimer un snapshot d'une machine virtuelle.

Lorsque vous supprimez un snapshot, vous supprimez l'état de la machine virtuelle que vous avez préservé et ne pouvez ensuite plus revenir à cet état. La suppression d'un snapshot n'affecte pas l'état actuel de la machine virtuelle.

Conditions préalables

Une machine virtuelle avec un snapshot stocké.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle dont vous souhaitez supprimer le snapshot, sélectionnez **Supprimer un snapshot**.
4. Cliquez sur **OK**.

Renouveler le bail d'une machine virtuelle

Vous pouvez renouveler le bail d'une machine virtuelle qui expire sous peu.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle dont le bail arrive à expiration, sélectionnez **Renouveler le bail**.

Résultats

Le bail est renouvelé. La durée du nouveau bail s'affiche dans le champ **Bail**.

Supprimer une machine virtuelle

Vous pouvez supprimer une machine virtuelle de votre organisation.

Conditions préalables

Votre machine virtuelle doit être hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Machines virtuelles** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher la liste dans une vue de carte et, le cas échéant, filtrer la liste des machines virtuelles depuis le menu déroulant **Rechercher dans**.
3. Dans le menu **Actions** de la machine virtuelle à supprimer, sélectionnez **Supprimer**.
4. Confirmez la suppression.

Résultats

La machine virtuelle est supprimée.

Utilisation des vApp

3

Un vApp est constitué d'une ou plusieurs machines virtuelles qui communiquent sur un réseau et utilisent des ressources et des services dans un environnement déployé. Un vApp peut contenir plusieurs machines virtuelles.

À partir de vCloud Director 9.5, les vApp prennent en charge la connectivité IPv6. Vous pouvez attribuer des adresses IPv6 aux machines virtuelles connectées à des réseaux IPv6.

Important Toutes les étapes de l'utilisation des vApp sont documentées dans la vue de carte, en partant du principe que vous avez plusieurs centres de données virtuels. Il est également possible de suivre les mêmes procédures à partir de la vue grille, mais les étapes peuvent varier légèrement.

Ce chapitre contient les rubriques suivantes :

- Afficher les vApp
- Construire un nouveau vApp
- Créer un vApp depuis un module OVF
- Créer un vApp à partir d'un modèle de vApp
- Ouvrir un vApp
- Exécution des opérations d'alimentation sur les vApp
- Modifier les propriétés d'un vApp
- Afficher un diagramme du réseau vApp
- Utilisation des réseaux dans un vApp
- Utilisation des snapshots
- Changer le propriétaire d'un vApp
- Déplacer un vApp vers un autre centre de données virtuel
- Copier un vApp arrêté vers un autre centre de données virtuel
- Copier un vApp activé
- Ajouter une machine virtuelle à un vApp
- Enregistrer un vApp en tant que modèle de vApp dans un catalogue

- Télécharger un vApp comme module OVF
- Renouveler le bail d'un vApp
- Supprimer un vApp

Afficher les vApp

Vous pouvez afficher les vApp dans une vue de grille ou dans une vue de carte.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Pour afficher les vApp dans une vue grille, cliquez sur . Pour les afficher dans une vue carte, cliquez sur .

La liste des vApp s'affiche dans une grille ou comme une liste de cartes.

3 (Facultatif) Configurez la vue de grille pour qu'elle contienne les détails que vous souhaitez afficher.

a Dans la vue de grille, cliquez sur l'icône de **Éditeur de grille** ( ).

b Sélectionnez les détails vApp que vous voulez inclure dans la vue grille en cochant la case à côté de chaque détail que vous voulez voir.

c Cliquez sur **OK** pour enregistrer les modifications.

Les détails sélectionnés apparaissent sous forme de colonnes pour chaque vApp.

4 (Facultatif) Dans la vue grille, cliquez sur à gauche d'un vApp, pour afficher les actions que vous pouvez entreprendre pour le vApp sélectionné.

Par exemple, vous pouvez arrêter un vApp.

Construire un nouveau vApp

Plutôt que de créer un vApp à partir d'un modèle de vApp, vous pouvez décider d'en créer un à l'aide des machines virtuelles à partir des catalogues, de nouvelles machines virtuelles ou d'une combinaison des deux.

Lors de la création d'un vApp, vous devez fournir un nom et éventuellement une description du vApp. Vous pouvez revenir en arrière et ajouter les machines virtuelles au vApp ultérieurement.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle d'**auteur de vApp** prédéfini ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur **Nouveau vApp**.
3. Entrez le nom et la description (facultative) du vApp.
4. (Facultatif) Recherchez dans le catalogue les machines virtuelles à ajouter à ce vApp ou ajoutez une nouvelle machine virtuelle vide en cliquant sur **Ajouter une Machine virtuelle**.

   S'il n'y a aucune machine virtuelle dans le catalogue, créez une machine virtuelle et ajoutez-la au vApp.

   a. Entrez le nom de la machine virtuelle et le nom de l'ordinateur pour celle-ci.

      Important Le nom de l'ordinateur ne peut contenir que des caractères alphanumériques et des traits d'union. Un nom d'ordinateur ne peut pas être composé de chiffres uniquement et ne peut pas contenir d'espaces.

   b. (Facultatif) Entrez une description significative.

c Sélectionnez la manière dont vous souhaitez déployer la machine virtuelle.

Option	Action
Nouveau	Vous déployez une nouvelle machine virtuelle avec des paramètres personnalisables. 1 Sélectionnez une famille de systèmes d'exploitation et le système d'exploitation. 2 (Facultatif) Sélectionnez une image de démarrage. 3 (Facultatif) Sélectionnez une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle. Les menus déroulants de stratégie de positionnement et de dimensionnement de machine virtuelle ne sont visibles que si le fournisseur de services a publié de telles stratégies sur le VDC d'organisation. 4 Sélectionnez la taille de la machine virtuelle ou cliquez sur **Options de dimensionnement personnalisé** pour entrer manuellement les paramètres de calcul, de mémoire et de stockage. Les tailles prédéfinies de la machine virtuelle sont Petit, Moyen et Grand. 5 Spécifiez les options de stockage, comme la stratégie de stockage et la taille de l'espace de stockage en Go. 6 Spécifiez les paramètres réseau de la machine virtuelle, comme le réseau, le mode IP, l'adresse IP et la carte réseau principale.
À partir du modèle	Vous déployez une machine virtuelle à partir d'un modèle que vous sélectionnez dans le catalogue de modèles. 1 Sélectionnez le modèle de machine virtuelle dans le catalogue. 2 (Facultatif) Sélectionnez une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle. Les menus déroulants de stratégie de positionnement et de dimensionnement de machine virtuelle ne sont visibles que si le fournisseur de services a publié de telles stratégies sur le VDC d'organisation. Si des stratégies sont attribuées au modèle sélectionné, vous pouvez être limité aux stratégies de modèle prédéfinies. 3 (Facultatif) Sélectionnez cette option pour utiliser une stratégie de stockage personnalisée et sélectionnez la stratégie dans **Stratégie de stockage personnalisée à utiliser**. 4 Si un contrat de licence d'utilisateur final est disponible, vous devez le consulter et l'accepter.

d Pour ajouter la machine virtuelle au vApp, cliquez sur **OK**.

Vous pouvez voir la machine virtuelle ajoutée dans le catalogue.

5 (Facultatif) Répétez l'Étape 4 pour chaque machine virtuelle supplémentaire que vous souhaitez créer au sein du vApp.

6 Pour terminer la création du vApp, cliquez sur **Créer**.

Résultats

Le vApp est créé et se trouve à l'état hors tension. Lorsque vous mettez le vApp sous tension, les machines virtuelles qu'il contient sont créées et sont également mises sous tension.

Créer un vApp depuis un module OVF

Vous pouvez créer et déployer un vApp directement depuis un module OVF sans créer de modèle vApp ni d'élément de catalogue correspondant.

vCloud Director a ses propres restrictions pour les déploiements d'OVF qui diffèrent des restrictions du système vCenter Server. Par conséquent, un déploiement d'OVF réussi dans le système vCenter Server peut échouer dans vCloud Director.

vCloud Director prend en charge OVF 1.1, mais ne prend pas en charge toutes les sections du schéma OVF 1.1. Par exemple, la section `DeploymentOptions` dans l'OVF n'est pas prise en charge.

Un déploiement d'OVF dans vCloud Director implique de nombreux composants, tels que `TransferService`, la zone de spool sur le montage NFS, la connexion NFC à l'instance de vCenter Server, la validation du total de contrôle, etc. Si l'un de ces composants échoue, cela entraîne l'échec du téléchargement du fichier OVF.

Si vous téléchargez un module OVF avec un fichier manifeste, vCloud Director valide le hachage SHA-1 du fichier descripteur OVF et tous les fichiers VMDK sur les valeurs du fichier `manifest.mf`. Si aucun hachage ne correspond, le téléchargement échoue. Un **administrateur système** peut désactiver cette vérification en définissant la propriété `CONFIG` sur `ovf.manifest.check.disabled`.

Conditions préalables

- Vérifiez que vous disposez d'un module OVF à télécharger et que vous êtes autorisé à télécharger des modules OVF et déployer des vApp.
- Vérifiez que la version de l'OVF dans le fichier descripteur OVF n'est pas 0.9.
- La taille maximale prise en charge par défaut d'un fichier descripteur OVF dans vCloud Director est de 12 Mo. Vous pouvez remplacer cette option en modifiant la propriété `CONFIG ovf.descriptor.size.max`.
- Vérifiez que la taille maximale autorisée par défaut du fichier manifeste (extension .mf) est de 1 Mo.
- Vérifiez que le module OVF est conforme au schéma XSD OVF.
- Si une version de matériel est fournie dans l'élément `VirtualSystemType` du fichier descripteur OVF, vérifiez qu'elle est inférieure à la version de matériel la plus élevée prise en charge dans le VDC sur lequel vous téléchargez le fichier OVF.
- Si le fichier descripteur OVF contient des éléments `ExtraConfig`, vérifiez que votre **administrateur système** inclus ces éléments dans la liste `AllowedList` des éléments `extraConfigs`. Les éléments qui ne sont pas inclus dans la liste `AllowedList` entraînent l'échec du téléchargement du fichier OVF avec une erreur de validation.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur **Ajouter un vApp depuis OVF**.
3. Cliquez sur le bouton **Télécharger** ( ) pour atteindre un emplacement accessible depuis votre ordinateur, puis sélectionnez le fichier du modèle OVF/OVA.

   L'emplacement peut être votre disque dur local, un partage réseau ou un lecteur de CD/DVD. Les extensions de fichier prises en charge incluent `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` et `.strings`. Si vous choisissez de télécharger un fichier OVF qui fait référence à plus de fichiers que ce que vous essayez d'importer (par exemple, un fichier VMDK), vous devez parcourir et sélectionner tous les fichiers.
4. Cliquez sur **Suivant**.
5. Vérifiez les détails du modèle OVF/OVA que vous êtes sur le point de déployer et cliquez sur **Suivant**.
6. Entrez un nom et une description (facultative) pour le vApp, puis cliquez sur **Suivant**.
7. (Facultatif) Modifiez le nom d'ordinateur du vApp afin qu'il contienne uniquement des caractères alphanumériques.

   Cette étape est requise uniquement si le nom du vApp contient des espaces ou des caractères spéciaux. Par défaut, le nom d'ordinateur est prérempli avec le nom de la machine virtuelle. Cependant, les noms d'ordinateur doivent contenir uniquement des caractères alphanumériques.
8. Dans le menu déroulant **Stratégie de stockage**, sélectionnez une stratégie de stockage pour chaque machine virtuelle du vApp, puis cliquez sur **Suivant**.
9. Sélectionnez les réseaux auxquels vous souhaitez que chaque machine virtuelle se connecte.
   - Sélectionnez un réseau pour chaque machine virtuelle dans le menu déroulant **Réseau**.
   - Vous pouvez sélectionner la case **Passer au workflow de mise en réseau avancée** et entrer manuellement les paramètres réseau tels que la carte réseau principale, le type d'adaptateur réseau, le réseau, l'attribution d'adresse IP et les paramètres d'adresse IP pour chaque machine virtuelle du vApp.

   Vous pouvez configurer des propriétés supplémentaires pour les machines virtuelles une fois que vous avez terminé les étapes de l'assistant.
10. Cliquez sur **Suivant**.

11 Personnalisez le matériel des machines virtuelles dans le vApp et cliquez sur **Suivant**.

Option	Description
Nombre de processeurs virtuels	Entrez le nombre de CPU virtuels pour chaque machine virtuelle dans le vApp. Le nombre maximal de processeurs virtuels pouvant être attribués à une machine virtuelle dépend du nombre de processeurs logiques sur l'hôte et du type de système d'exploitation invité installé sur la machine virtuelle.
Cœurs par socket	Entrez le nombre de cœurs par socket pour chaque machine virtuelle dans le vApp. Vous pouvez configurer la façon dont les processeurs virtuels sont attribués en matière de cœurs et de cœurs par socket. Déterminez le nombre de CPU que la machine virtuelle doit avoir, puis sélectionnez le nombre de cœurs de chaque socket, selon que vous désirez un processeur monocœur, double cœur, triple cœur, etc.
Nombre de cœurs	Affichez le nombre de cœurs pour chaque machine virtuelle dans le vApp. Ce nombre est modifié lorsque vous mettez à jour le nombre de processeurs virtuels.
Mémoire totale (Mo)	Entrez la mémoire en Mo pour chaque machine virtuelle dans le vApp. Ce paramètre détermine la quantité de mémoire de l'hôte ESXi allouée à la machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications qui s'exécutent dans la machine virtuelle. Une machine virtuelle ne peut pas bénéficier de plus de ressources mémoire que sa taille de mémoire matérielle virtuelle configurée.

12 Sur la page Prêt à terminer, vérifiez les paramètres et cliquez sur **Terminer**.

Résultats

Le nouveau vApp s'affiche dans la vue Carte.

Créer un vApp à partir d'un modèle de vApp

Vous pouvez créer un nouveau vApp à partir d'un modèle de vApp stocké dans un catalogue auquel vous avez accès.

Si le modèle de vApp repose sur un fichier OVF incluant des propriétés OVF pour personnaliser ses machines virtuelles, ces propriétés sont transmises au vApp. Si certaines de ces propriétés peuvent être configurées par l'utilisateur, vous pouvez spécifier les valeurs.

Conditions préalables

- Seuls les administrateurs d'organisation et les auteurs de vApp ont accès aux modèles de vApp dans les catalogues publics.
- Les utilisateurs de vApp et au-dessus peuvent accéder aux modèles de vApp dans les catalogues d'organisation partagés avec eux.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) sur la gauche du modèle de vApp que vous souhaitez déployer en tant que vApp et sélectionnez **Créer un vApp**.

3 Sur la page **Accepter les licences** de l'assistant, lisez les contrats de licence d'utilisateur final et cliquez sur **Accepter**.

4 Cliquez sur **Suivant**.

5 Entrez le nom et la description (facultative) du vApp.

6 Spécifiez la durée de fonctionnement du vApp avant son arrêt automatique en heures ou en jours.

7 Spécifiez le délai de disponibilité des vApp arrêtés avant leur suppression automatique en heures ou en jours.

8 Cliquez sur **Suivant**.

9 Sélectionnez le centre de données virtuel dans lequel vous souhaitez créer le vApp.

10 Sélectionnez une stratégie de stockage

11 Cliquez sur **Suivant**.

12 Sélectionnez les réseaux auxquels vous souhaitez que chaque machine virtuelle se connecte.

   - Sélectionnez un réseau pour chaque machine virtuelle dans le menu déroulant **Réseau**.
   - Vous pouvez sélectionner la case **Passer au workflow de mise en réseau avancée** et entrer manuellement les paramètres réseau tels que la carte réseau principale, le type d'adaptateur réseau, le réseau, l'attribution d'adresse IP et les paramètres d'adresse IP pour chaque machine virtuelle du vApp.

   Vous pouvez configurer des propriétés supplémentaires pour les machines virtuelles une fois que vous avez terminé les étapes de l'assistant.

13 Cliquez sur **Suivant**.

14 Personnalisez le matériel des machines virtuelles dans le vApp et cliquez sur **Suivant**.

Option	Description
Nombre de processeurs virtuels	Entrez le nombre de CPU virtuels pour chaque machine virtuelle dans le vApp. Le nombre maximal de processeurs virtuels pouvant être attribués à une machine virtuelle dépend du nombre de processeurs logiques sur l'hôte et du type de système d'exploitation invité installé sur la machine virtuelle.
Cœurs par socket	Entrez le nombre de cœurs par socket pour chaque machine virtuelle dans le vApp. Vous pouvez configurer la façon dont les processeurs virtuels sont attribués en matière de cœurs et de cœurs par socket. Déterminez le nombre de CPU que la machine virtuelle doit avoir, puis sélectionnez le nombre de cœurs de chaque socket, selon que vous désirez un processeur monocœur, double cœur, triple cœur, etc.
Nombre de cœurs	Affichez le nombre de cœurs pour chaque machine virtuelle dans le vApp. Ce nombre est modifié lorsque vous mettez à jour le nombre de processeurs virtuels.
Mémoire totale (Mo)	Entrez la mémoire en Mo pour chaque machine virtuelle dans le vApp. Ce paramètre détermine la quantité de mémoire de l'hôte ESXi allouée à la machine virtuelle. La taille de la mémoire du matériel virtuel détermine la quantité de mémoire disponible pour les applications qui s'exécutent dans la machine virtuelle. Une machine virtuelle ne peut pas bénéficier de plus de ressources mémoire que sa taille de mémoire matérielle virtuelle configurée.
Propriétés du disque dur	Entrez la taille du disque dur de la machine virtuelle en Mo.

15 Sur la page Prêt à terminer, vérifiez les paramètres et cliquez sur **Terminer**.

Résultats

Le nouveau vApp s'affiche dans la vue Carte.

Ouvrir un vApp

Vous pouvez ouvrir un vApp pour afficher les machines virtuelles et réseaux qu'il contient. Vous pouvez également afficher un diagramme détaillant la façon dont les machines virtuelles et les réseaux sont connectés.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la vue de carte, vous pouvez voir des informations générales, telles que le nombre de machines virtuelles associées au vApp, des informations sur le bail, le nombre total de CPU, le total du stockage et la mémoire, les réseaux associés et si un snapshot est pris.

4 Pour afficher les paramètres détaillés d'un vApp sélectionné, cliquez sur **Détails** dans la fiche du vApp.

Exécution des opérations d'alimentation sur les vApp

Vous pouvez effectuer des opérations d'alimentation sur les vApp, telles que la mise sous tension ou hors tension d'un vApp, l'interruption ou la réinitialisation d'un vApp.

Mettre sous tension un vApp

La mise sous tension d'un vApp met sous tension toutes les machines virtuelles du vApp qui ne sont pas encore sous tension.

Conditions préalables

Vous êtes au moins auteur de vApp.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous voulez mettre sous tension, sélectionnez **Mettre sous tension**.

Résultats

Le vApp est mis sous tension.

Mettre hors tension un vApp

La mise hors tension d'un vApp met hors tension toutes les machines virtuelles du vApp. Vous devez mettre un vApp hors tension pour pouvoir réaliser certaines actions. Par exemple, l'ajout du vApp à un catalogue, sa copie ou son déplacement vers un autre VDC.

Conditions préalables

Le vApp doit être démarré.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez arrêter, sélectionnez **Mettre hors tension**.

4 Cliquez sur **OK**.

Résultats

Toutes les machines virtuelles du vApp et le vApp lui-même sont mis hors tension.

Arrêter un vApp

L'arrêt d'un vApp met hors tension ou arrête toutes les machines virtuelles dans le vApp. Vous devez arrêter un vApp pour pouvoir réaliser certaines actions. Par exemple, l'ajout du vApp à un catalogue, sa copie ou son déplacement vers un autre VDC.

Conditions préalables

Le vApp doit être démarré.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez arrêter, sélectionnez **Arrêter**.

4 Cliquez sur **OK**.

Résultats

Toutes les machines virtuelles du vApp et le vApp lui-même sont mis hors tension ou arrêtés.

Réinitialiser un vApp

La réinitialisation d'un vApp efface l'état (mémoire, cache, etc.), mais ce vApp continue à s'exécuter.

Conditions préalables

Votre vApp est démarré et les machines virtuelles qu'il contient sont sous tension.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez réinitialiser, sélectionnez **Réinitialiser**.

Résultats

L'état est effacé et ce vApp continue à s'exécuter.

Interrompre un vApp

L'interruption d'un vApp préserve son état actuel en écrivant la mémoire sur le disque.

Conditions préalables

Le vApp s'exécute.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous voulez interrompre, sélectionnez **Interrompre**.

Résultats

Le vApp est interrompu et son état est conservé.

Ignorer l'état interrompu d'un vApp

Si un vApp est à l'état interrompu et que vous n'avez plus besoin de recommencer à utiliser le vApp, vous pouvez ignorer l'état interrompu. Lorsque vous ignorez l'état interrompu, vous supprimez la mémoire enregistrée et ramenez les vApp à un état hors tension.

Conditions préalables

Le vApp doit se trouver dans un état interrompu.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp interrompu, sélectionnez **Ignorer l'état d'interruption**.

Résultats

L'état est ignoré et le vApp est mis hors tension.

Modifier les propriétés d'un vApp

Vous pouvez modifier les propriétés d'un vApp existant, y compris son nom et sa description, les paramètres de bail, l'ordre de démarrage des machines virtuelles dans le vApp, les paramètres de partage et les paramètres réseau.

Modifier les propriétés générales du vApp

Vous pouvez vérifier et modifier le nom, la description et les autres propriétés générales d'un vApp.

Conditions préalables

Vérifiez que le vApp est hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la carte du vApp sélectionné, cliquez sur **Détails** pour afficher et modifier les propriétés du vApp.
4. Vérifiez et modifiez les propriétés si nécessaire, puis cliquez sur **Enregistrer**.

Option	Action
Nom	Entrez un nouveau nom pour le vApp.
Description	Entrez une description facultative du vApp.
Centre de données virtuel	Nom du centre de données auquel le vApp appartient.
Snapshot	S'il existe un snapshot, les détails le concernant s'affichent.
Baux	Cliquez sur **Renouveler** pour renouveler le bail. a Planifiez le bail d'exécution en nombre d'heures ou de jours. Définit la durée de fonctionnement du vApp avant son arrêt automatique. b Planifiez le bail de stockage en nombre d'heures ou de jours. Définit la durée pendant laquelle le vApp reste disponible avant d'être automatiquement supprimé.

Résultats

Les paramètres généraux sont enregistrés.

Modifier les propriétés avancées d'un vApp

Vous pouvez configurer l'ordre de démarrage et d'arrêt des machines virtuelles dans votre vApp. Configurez l'ordre de démarrage et d'arrêt si vous disposez d'applications installées dans les machines virtuelles qui doivent se démarrer et s'arrêter dans un ordre particulier.

Ces paramètres sont utiles si vous devez démarrer et arrêter vos machines virtuelles dans un ordre particulier. Par exemple, une machine virtuelle héberge un serveur de base de données, une autre héberge un serveur d'applications et la dernière héberge un serveur Web. Pour que les fonctions complémentaires fonctionnent correctement, le serveur de base de données doit démarrer en premier, suivi du serveur d'applications et du serveur Web en dernier.

Conditions préalables

Vérifiez que le vApp est hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Sur la fiche du vApp sélectionné, cliquez sur **Détails** et faites défiler vers le bas jusqu'aux propriétés avancées du vApp.
4. Entrez les propriétés de l'ordre de démarrage et d'arrêt pour chaque machine virtuelle, puis cliquez sur **Enregistrer**.

Option	Action
Ordre de démarrage	Entrez l'ordre dans lequel vous souhaitez que la machine virtuelle démarre. Vous devez entrer une valeur pour chaque machine dans la séquence.
Action de démarrage	Sélectionnez une action de démarrage. L'action détermine le comportement d'une machine virtuelle lorsque vous démarrez le vApp qui les contient. Par défaut, cette option est définie sur **Mettre sous tension**.
Délai de démarrage	Entrez le délai d'attente du démarrage. Le délai d'attente de démarrage est la période (en secondes) au terme de laquelle vCloud Director démarre la machine suivante de la séquence.

Option	Action
Action d'arrêt	Sélectionnez l'action d'arrêt. L'action d'arrêt est l'action effectuée par la machine virtuelle lorsque vous arrêtez le vApp qui la contient. Si vous sélectionnez **Mettre hors tension**, la machine virtuelle se met hors tension sans effectuer d'actions d'arrêt garantissant la stabilité (ce qui équivaut à retirer le câble d'alimentation de la prise). Sélectionnez cette action si vous n'avez pas installé VMware Tools. Sinon, sélectionnez **Arrêter**, ce qui garantit la stabilité lors de la mise hors tension.
Délai d'arrêt	Entrez la durée du délai d'arrêt. Le délai d'attente d'arrêt est la période au terme de laquelle vCloud Director arrête la machine virtuelle suivante de la séquence.

Partager un vApp

Vous pouvez partager vos vApp avec d'autres groupes ou utilisateurs au sein de votre organisation. Les contrôles d'accès que vous définissez déterminent les opérations qui peuvent être effectuées sur les vApp partagés.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la carte du vApp sélectionné, cliquez sur **Détails** et faites défiler vers le bas jusqu'aux propriétés de partage du vApp.

4 Sélectionnez les utilisateurs avec lesquels vous souhaitez partager le vApp et cliquez sur **Enregistrer**.

Option	Action
Partager avec tout le monde dans l'organisation	Sélectionnez cette option pour partager le vApp avec tous les utilisateurs de l'organisation et choisir le niveau d'accès. ■ Pour accorder le contrôle total, sélectionnez **Contrôle total**. Tous les utilisateurs de l'organisation peuvent ouvrir, démarrer, enregistrer un vApp comme un modèle de vApp, ajouter le modèle à un catalogue, changer le propriétaire du vApp, copier dans un catalogue et modifier les propriétés. ■ Pour accorder l'accès en lecture seule, sélectionnez **Lecture seule**.
Partager avec certains utilisateurs et groupes	Sélectionnez cette option pour partager uniquement avec les utilisateurs de votre choix. a Sélectionnez les noms dans le panneau **Utilisateurs et groupes sans accès** pour les déplacer vers le panneau **Utilisateurs et groupes avec accès**. b Sélectionnez un niveau d'accès pour les utilisateurs et les groupes spécifiés. ■ Pour accorder le contrôle total, sélectionnez **Contrôle total**. Les utilisateurs disposant du contrôle total peuvent ouvrir, démarrer, enregistrer un vApp comme un modèle de vApp, ajouter le modèle à un catalogue, changer le propriétaire du vApp, copier dans un catalogue et modifier les propriétés. ■ Pour accorder l'accès en lecture seule, sélectionnez **Lecture seule**.

Résultats

Votre vApp est partagé avec les utilisateurs ou groupes spécifiés.

Afficher un diagramme du réseau vApp

Un diagramme du réseau vApp fournit une vue graphique des machines virtuelles et des réseaux d'un vApp.

Conditions préalables

Pour afficher le diagramme du réseau vApp, votre vApp doit contenir moins de 40 machines virtuelles. Si le vApp contient plus de 40 machines virtuelles, le diagramme n'est pas disponible.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la fiche du vApp sélectionné, cliquez sur **Détails**.

4 Cliquez sur l'onglet **Diagramme de réseau**.

Le diagramme illustrant la connexion des machines virtuelles et des réseaux du vApp s'affiche. Une étoile représente une carte réseau principale. Si une carte réseau est connectée, sa couleur est verte. Dans le cas contraire, elle est blanche.

5 (Facultatif) Pour mettre en surbrillance les machines virtuelles et les réseaux connectés, cliquez sur un réseau ou une machine virtuelle.

Les objets connectés et les connexions établies entre eux sont mis en surbrillance.

Étape suivante

Vous pouvez ajouter des machines virtuelles ou des réseaux à partir de cette page.

Utilisation des réseaux dans un vApp

Les machines virtuelles d'un vApp peuvent se connecter aux réseaux vApp (isolés ou acheminés) et aux réseaux de centre de données virtuel d'organisation (directs ou clôturés). Vous pouvez ajouter différents types de réseaux à un vApp afin de répondre aux besoins de plusieurs scénarios de mise en réseau.

Les machines virtuelles dans le vApp peuvent se connecter aux réseaux disponibles dans un vApp. Si vous souhaitez connecter une machine virtuelle à un autre réseau, vous devez d'abord l'ajouter au vApp.

Un vApp peut contenir des réseaux vApp et de centre de données virtuel d'organisation. Un réseau vApp peut être isolé ou routé. Un réseau vApp isolé est inclus dans le vApp. Vous pouvez également router un réseau vApp vers un réseau de centre de données virtuel d'organisation pour fournir une connectivité aux machines virtuelles en dehors du vApp. Pour les réseaux vApp avec acheminement, vous pouvez configurer des services réseau, comme un pare-feu et un routage statique.

Vous pouvez connecter un vApp directement à un réseau de centre de données virtuel d'organisation. Si vous disposez de plusieurs vApp qui contiennent des machines virtuelles identiques connectées au même réseau de centre de données virtuel d'organisation et que vous voulez démarrer les vApp simultanément, vous pouvez le clôturer. L'isolation du vApp vous permet de mettre sous tension les machines virtuelles sans créer de conflit, en isolant leurs adresses MAC et IP.

Les réseaux que vous ajoutez au vApp utilisent le pool de réseaux associé au centre de données virtuel d'organisation dans lequel vous avez créé le vApp.

Afficher les réseaux vApp

Vous pouvez accéder aux réseaux et les afficher dans un vApp.

Conditions préalables

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la fiche du vApp sélectionné, cliquez sur **Détails**.
4. Cliquez sur l'onglet **Réseaux**.

   La liste des réseaux, le cas échéant, s'affiche. Vous pouvez afficher des informations sur chaque réseau, comme le nom, la passerelle, le masque réseau, la connexion et les ressources IP et NAT.
5. (Facultatif) Pour modifier les colonnes à afficher, cliquez sur l'icône **Éditeur de grille** ( ) et sélectionnez ou désélectionnez les cases à cocher des colonnes que vous voulez afficher ou masquer, respectivement.

Clôturer un réseau vApp

La mise sous tension de machines virtuelles identiques incluses dans différents vApp peut entraîner un conflit. Pour permettre la mise sous tension de machines virtuelles identiques dans différents vApp sans conflit, vous devez clôturer le vApp.

La clôture d'un vApp isole les adresses MAC et IP des machines virtuelles, et redéfinit le type de connexion, direct, des réseaux VDC d'organisation sur Clôturé. Sur les réseaux clôturés, le pare-feu est automatiquement activé et configuré de sorte que seul le trafic sortant est autorisé. Lorsque vous clôturez un vApp, vous pouvez également configurer des règles NAT et de pare-feu sur les réseaux clôturés.

Conditions préalables

- Vous ne pouvez clôturer que des réseaux vApp directs. Si le vApp utilise plusieurs réseaux et que les autres réseaux sont, par exemple, acheminés, seul le réseau direct est clôturé.
- Les machines virtuelles du vApp qui utilisent le réseau direct doivent être arrêtées, afin que le réseau vApp direct ne soit pas en cours d'utilisation.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la fiche du vApp sélectionné, cliquez sur **Détails**.
4. Cliquez sur l'onglet **Réseaux**.

5 Si le vApp n'est pas clôturé, cliquez sur le bouton **Modifier**.

6 Activez l'option **Clôturer le vApp** et cliquez sur **OK**.

Résultats

Les adresses IP et MAC des machines virtuelles sont alors isolées. Vous pouvez mettre sous tension, sans conflit, des machines virtuelles identiques dans différents vApp.

Ajouter un réseau à un vApp

Vous pouvez ajouter un réseau à un vApp pour rendre le réseau accessible aux machines virtuelles du vApp. Vous pouvez ajouter un réseau vApp ou un réseau de centre de données virtuel d'organisation à un vApp.

Les connexions peuvent être directes ou clôturées. Le clôturage permet de mettre sous tension sans conflit des machines virtuelles identiques dans différents vApp, en isolant les adresses MAC et IP des machines virtuelles.

Lorsque l'isolation est activée et que le vApp est sous tension, un réseau isolé est créé depuis le pool de réseaux de centre de données virtuel d'organisation. Une passerelle Edge est créée et connectée au réseau isolé et au réseau de centre de données virtuel d'organisation. Le trafic vers et depuis les machines virtuelles communique par la passerelle Edge, qui convertit l'adresse IP à l'aide de NAT et d'AR de proxy. Cela permet à un routeur de transmettre le trafic entre deux réseaux en utilisant le même espace IP.

Conditions préalables

Pour ajouter un réseau de centre de données virtuel d'organisation, votre administrateur doit avoir créé un réseau de ce type.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la fiche du vApp sélectionné, cliquez sur **Actions** et sélectionnez **Ajouter un réseau**.

4 Sélectionnez le type de réseau à ajouter.

Option	Action
Réseau VDC d'organisation	Sélectionnez un réseau de centre de données virtuel d'organisation dans la liste des réseaux disponibles.
Réseau vApp	a Entrez le nom et la description (facultative) du réseau. b Entrez les paramètres CIDR de la passerelle réseau. c (Facultatif) Saisissez le DNS primaire et secondaire et le suffixe DNS. d (Facultatif) Choisissez d'autoriser ou non un VLAN invité. e (Facultatif) Entrez les paramètres du pool d'adresses IP statiques, comme les plages d'adresses IP. f (Facultatif) Pour pouvoir se connecter à un réseau de centre de données virtuel d'organisation, activez l'option **Se connecter à un réseau VDC d'organisation** et sélectionnez un réseau dans la liste.

5 Cliquez sur **Ajouter**.

Résultats

Le réseau est ajouté au vApp.

Étape suivante

Connectez une machine virtuelle du vApp au réseau.

Configuration des services réseau pour un réseau vApp

Vous pouvez configurer des services réseau, tels que DHCP, des pare-feu, NAT (network address translation) et l'acheminement statique pour certains réseaux vApp.

Les services réseau disponibles varient selon le type de réseau vApp.

Tableau 3-1. Services réseau disponibles par type de réseau

Type de réseau vApp	DHCP	Pare-feu	NAT	Acheminement statique
Direct				
Routage	X	X	X	X
Isolé	X			

Afficher et modifier les détails généraux du réseau

Vous pouvez afficher et modifier les informations générales du réseau vApp, par exemple le nom et la description du réseau.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Dans l'onglet **Général**, passez en revue les informations du réseau.

6 Cliquez sur **Modifier**.

7 Modifiez le nom et la description du réseau vApp.

8 Cliquez sur **Enregistrer**.

Modifier les paramètres de pool d'adresses IP statiques d'un réseau vApp

Vous pouvez configurer un réseau de vApp pour fournir des adresses IP statiques aux machines virtuelles dans le vApp en les extrayant à partir d'un pool statique d'adresses IP.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Sous l'onglet **Gestion des adresses IP**, cliquez sur **Pools statiques**.

6 Cliquez sur **Modifier**.

7 Entrez une plage d'adresses IP, puis cliquez sur **Ajouter**.

8 Cliquez sur **Enregistrer**.

Modifier les paramètres DNS d'un réseau vApp

Après avoir créé un réseau de vApp, vous pouvez afficher et modifier les paramètres DNS à tout moment.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Sous l'onglet **Gestion des adresses IP**, cliquez sur **DNS**.

   Les paramètres DNS sont affichés.

6 Cliquez sur **Modifier**.

7 Modifier le DNS principal et secondaire, et le suffixe DNS.

8 Cliquez sur **Enregistrer**.

Configurer DHCP pour un réseau vApp

Vous pouvez configurer certains réseaux vApp afin de fournir des services DHCP à des machines virtuelles du vApp.

Lorsque vous activez le protocole DHCP pour un réseau de vApp, connectez une carte réseau sur une machine virtuelle du vApp à ce réseau, puis sélectionnez DHCP comme mode IP pour cette carte réseau. vCloud Director attribue une adresse IP DHCP à la machine virtuelle lorsque vous la mettez sous tension.

Conditions préalables

Un réseau vApp avec acheminement ou un réseau vApp isolé.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Sous l'onglet **Gestion des adresses IP**, cliquez sur **DHCP**.

   L'état DHCP s'affiche.

6 Cliquez sur **Modifier**.

7 Cliquez sur **Activé**.

8 Dans la zone de texte **Pool d'adresses IP**, entrez une plage d'adresses IP.

   vCloud Director utilise ces adresses pour satisfaire les demandes DHCP. La plage d'adresses IP DHCP ne peut pas recouvrir le pool IP statique pour le réseau vApp.

9 Définissez la durée du bail par défaut et maximale en secondes.

10 Cliquez sur **Enregistrer**.

Afficher les allocations IP pour votre réseau vApp

Vous pouvez passer en revue les allocations IP pour les réseaux de votre vApp.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Sous l'onglet **Gestion des adresses IP**, cliquez sur **Allocations d'adresse IP**.

Les adresses IP allouées sont affichées.

Configurer le routage statique pour un réseau vApp

Vous pouvez configurer certains réseaux vApp pour fournir des services de routage statique afin de permettre aux machines virtuelles sur différents réseaux vApp de communiquer.

Toute route statique que vous créez est automatiquement activée.

Conditions préalables

Un réseau vApp avec acheminement.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.

4 Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.

5 Sous l'onglet **Routage**, cliquez sur **Modifier**.

Vous pouvez activer ou désactiver le routage statique pour le réseau.

Ajouter un routage statique pour un réseau vApp

Vous pouvez ajouter des chemins statiques entre deux réseaux vApp acheminés vers le même réseau de centre de données virtuel d'organisation. Les chemins statiques permettent le trafic entre les réseaux.

Vous ne pouvez pas ajouter des chemins statiques vers un vApp clôturé ou entre des réseaux qui se chevauchent. Après avoir ajouté un chemin statique à un réseau vApp, configurez les règles de pare-feu du réseau pour permettre le trafic sur le chemin statique. Pour les vApp avec des chemins statiques, choisissez d'utiliser les adresses IP allouées jusqu'à ce que ce vApp ou les réseaux associés soient supprimés.

Les chemins statiques fonctionnent uniquement lorsque les vApp contenus dans les chemins sont en cours d'exécution. Si vous modifiez le réseau parent d'un vApp, supprimez un vApp ou un réseau vApp, et que le vApp comporte des chemins statiques, ces chemins ne peuvent pas fonctionner et vous devez les supprimer manuellement.

Conditions préalables

- Deux réseaux vApp sont acheminés vers le même réseau de centre de données virtuel d'organisation.
- Les réseaux vApp figurent dans des vApp démarrés au moins une fois.
- L'acheminement statique est activé sur les deux réseaux vApp.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.
4. Sous l'onglet **Réseaux**, cliquez sur un réseau pour afficher ses détails.
5. Dans l'onglet **Routage**, sous Routage statique, cliquez sur **Ajouter**.

   Les adresses IP allouées sont affichées.
6. Entrez un nom pour le chemin statique.
7. Entrez l'adresse réseau au format CIDR.

   L'adresse réseau désigne le réseau vApp auquel ajouter un chemin statique.
8. Entrez l'adresse IP du prochain saut.

   L'adresse IP du prochain saut représente l'adresse IP externe du routeur de ce réseau vApp.
9. Cliquez sur **Enregistrer**.
10. Répétez la même procédure pour le second réseau vApp.

Exemple : Exemple d'acheminement statique

Réseau vApp 1 et Réseau vApp 2 sont tous deux acheminés vers Réseau org partagé. Vous pouvez créer un chemin statique sur chaque réseau vApp pour permettre le trafic entre les réseaux. Vous pouvez utiliser les informations concernant les réseaux vApp afin de créer des chemins statiques.

Tableau 3-2. Informations du réseau

Nom du réseau	Spécification du réseau	Adresse IP externe du routeur
Réseau vApp 1	192.168.1.0/24	192.168.0.100
Réseau vApp 2	192.168.2.0/24	192.168.0.101
Réseau org partagé	192.168.0.0/24	NA

Sur Réseau vApp 1, créez un chemin statique vers Réseau vApp 2. Sur Réseau vApp 2, créez un chemin statique vers Réseau vApp 1.

Tableau 3-3. Paramètres d'acheminement statique

Réseau vApp	Nom du chemin	Réseau	Adresse IP du prochain saut
Réseau vApp 1	tovapp2	192.168.2.0/24	192.168.0.101
Réseau vApp 2	tovapp1	192.168.1.0/24	192.168.0.100

Supprimer un réseau vApp

Si vous n'avez plus besoin d'un réseau dans votre vApp, vous pouvez le supprimer.

Conditions préalables

Le vApp est arrêté et aucune machine virtuelle du vApp n'est connectée au réseau.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans la carte du dispositif virtuel sélectionné, cliquez sur **Détails**.
4. Dans l'onglet **Réseaux**, sélectionnez le réseau que vous souhaitez supprimer, cliquez sur **Supprimer** et confirmez la suppression.

Utilisation des snapshots

La création d'un snapshot préserve l'état et les données des machines virtuelles au sein d'un vApp à un moment spécifique dans le temps. Un snapshot n'est pas prévu pour être utilisé pendant de longues périodes ou à la place de la sauvegarde du vApp.

Vous pouvez utiliser un snapshot lors de la mise à niveau des machines virtuelles dans un vApp. Par exemple, avant de mettre à niveau les machines virtuelles, vous créez un snapshot pour conserver le point dans le temps avant la mise à niveau. Pour ce faire, vous enregistrez un snapshot avant la mise à niveau, puis vous effectuez la mise à niveau. S'il n'y a aucun problème lors de la mise à niveau, vous pouvez choisir de supprimer le snapshot, ce qui validera les modifications apportées au cours de la mise à niveau. Cependant, si vous avez rencontré un problème, vous pouvez restaurer le snapshot, ce qui va rétablir l'état de votre vApp enregistré avant la mise à niveau.

Prendre un snapshot d'un vApp

En prenant un snapshot d'un vApp, vous prenez des snapshots de toutes les machines virtuelles dans le vApp. Une fois que vous avez pris le snapshot, vous pouvez restaurer toutes les machines virtuelles dans le vApp sur le snapshot ou supprimer ce dernier si vous n'en avez pas besoin.

Les snapshots de vApp présentent certaines limitations.

- Les snapshots de vApp ne capturent pas les configurations de carte réseau.
- Si une machine virtuelle située dans le vApp est connectée à un disque nommé, vous ne pouvez pas prendre de snapshot du vApp.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp pour lequel vous souhaitez créer un snapshot, sélectionnez **Créer un snapshot**.

   La création du snapshot d'un vApp remplace le snapshot existant, le cas échéant.
4. (Facultatif) Indiquez si vous voulez créer un snapshot de la mémoire du vApp.

   Lorsque vous capturez l'état de la mémoire du vApp, le snapshot conserve l'état actif du vApp et des machines virtuelles dans ce dernier. Les snapshots de mémoire permettent de créer un snapshot à un instant précis (par exemple, pour mettre à niveau un logiciel qui fonctionne parfaitement). Si vous créez un snapshot de mémoire et que la mise à niveau ne s'exécute pas correctement, ou si le logiciel ne vous convient pas, vous pouvez restaurer l'état précédent de la machine virtuelle.

Lorsque vous capturez l'état de la mémoire, les fichiers du vApp ne nécessitent aucune mise au repos. Si vous ne capturez pas l'état de la mémoire, le snapshot ne sauvegarde pas l'état actif du vApp et les disques sont cohérents en cas d'incident à moins que vous ne les mettiez au repos.

5 (Facultatif) Indiquez si vous souhaitez mettre au repos le système de fichiers invité.

Pour cette opération, VMware Tools doit être installé sur les machines virtuelles dans le vApp. Lorsque vous mettez au repos une machine virtuelle, VMware Tools met au repos le système de fichiers de la machine virtuelle. Une opération de mise au repos garantit qu'un disque de snapshot représente un état cohérent des systèmes de fichiers invités. Les snapshots mis au repos s'utilisent notamment lors des sauvegardes automatisées ou périodiques. Par exemple, si vous méconnaissez l'activité de la machine virtuelle, mais que vous souhaitiez disposer de plusieurs sauvegardes récentes, vous pouvez mettre les fichiers au repos.

Les vApp équipés de disques haute capacité ne peuvent pas être mis au repos.

6 Cliquez sur **OK**.

Résultats

Un snapshot du vApp est créé.

Étape suivante

Vous pouvez restaurer toutes les machines virtuelles du vApp au snapshot le plus récent.

Restaurer un vApp à un snapshot

Vous pouvez restaurer toutes les machines virtuelles dans un vApp à l'état dans lequel elles étaient lorsque vous avez créé le snapshot vApp.

Conditions préalables

Vérifiez que le vApp dispose d'un snapshot existant.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez restaurer, sélectionnez **Restaurer le snapshot**.

4 Cliquez sur **OK.**

Résultats

Toutes les machines virtuelles dans le vApp reviennent à l'état de snapshot.

Supprimer un snapshot d'un vApp

Vous pouvez supprimer un snapshot d'un vApp.

Lorsque vous supprimez un snapshot du vApp, vous supprimez l'état des machines virtuelles dans le snapshot du vApp et ne pouvez ensuite plus revenir à cet état. La suppression d'un snapshot n'affecte pas l'état actuel du vApp.

Conditions préalables

Vous avez pris un snapshot du vApp.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp dont vous souhaitez supprimer un snapshot, sélectionnez **Supprimer un snapshot**.
4. Cliquez sur **OK**.

Résultats

Le snapshot est supprimé.

Changer le propriétaire d'un vApp

Vous pouvez changer le propriétaire du vApp, par exemple, lorsque le propriétaire d'un vApp quitte l'entreprise ou change de rôle au sein de celle-ci.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp dont vous souhaitez changer le propriétaire, sélectionnez **Changer le propriétaire**.
4. Sélectionnez un utilisateur dans la liste.

5 Cliquez sur **OK**.

Résultats

Le propriétaire du vApp est modifié.

Déplacer un vApp vers un autre centre de données virtuel

Lorsque vous déplacez un vApp vers un autre centre de données virtuel, le vApp est supprimé depuis le centre de données virtuel source.

Conditions préalables

- Vous êtes au moins un **auteur de vApp**.
- Votre vApp est mis hors tension.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez déplacer, sélectionnez **Déplacer vers**.

4 Sélectionnez le centre de données virtuel vers lequel vous souhaitez déplacer le vApp et cliquez sur **OK**.

5 (Facultatif) Sélectionnez la stratégie de stockage.

6 Cliquez sur **OK**.

Résultats

Le vApp est supprimé du centre de données source et déplacé vers le centre de données cible.

Copier un vApp arrêté vers un autre centre de données virtuel

Lorsque vous copiez un vApp vers un autre centre de données virtuel, le vApp d'origne reste dans le centre de données virtuel source.

Conditions préalables

- Vous êtes au moins un **auteur de vApp**.
- Le vApp est mis hors tension.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp à copier, sélectionnez **Copier vers**.
4. Saisissez un nom et une description.
5. Sélectionnez le centre de données virtuel dans lequel vous souhaitez créer la copie du vApp.
6. (Facultatif) Sélectionnez une stratégie de stockage
7. Cliquez sur **OK**.

Résultats

Le vApp est copié vers le centre de données virtuel spécifié avec le nom et la description que vous avez fournis.

Copier un vApp activé

Pour créer un vApp à partir d'un vApp existant, vous pouvez copier un vApp et modifier la copie en fonction de vos besoins. Il n'est pas nécessaire de mettre hors tension les machines virtuelles dans le vApp avant de le copier. L'état de la mémoire des machines virtuelles en cours d'exécution est conservé dans le vApp copié.

Conditions préalables

Vérifiez que les conditions suivantes sont réunies.

- Vous êtes au moins un **utilisateur de vApp**.
- Le centre de données virtuel de l'organisation est sauvegardé par vCenter Server 5.5 ou version ultérieure.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp à copier, sélectionnez **Copier vers**.
4. Saisissez un nom et une description.
5. Sélectionnez le centre de données virtuel dans lequel vous souhaitez créer la copie du vApp.
6. (Facultatif) Sélectionnez une stratégie de stockage

7 Cliquez sur **OK**.

Résultats

Une copie du vApp est créée et celle-ci se trouve à l'état d'interruption. Le vApp copié est activé pour le clôturage de réseau.

Étape suivante

Modifiez les propriétés réseau du nouveau vApp ou activez-le.

Ajouter une machine virtuelle à un vApp

Vous pouvez ajouter une machine virtuelle à un vApp.

Conditions préalables

Vous devez être **administrateur d'organisation** ou **auteur de vApp** pour accéder à des machines virtuelles dans des catalogues publics.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp auquel vous souhaitez ajouter une machine virtuelle, sélectionnez **Ajouter une machine virtuelle**.

La liste des machines virtuelles qui sont associées au vApp s'affiche dans la fenêtre **Ajouter des machines virtuelles**.

4 Pour créer une machine virtuelle et l'associer automatiquement au vApp, cliquez sur **Ajouter une machine virtuelle**.

5 Entrez le nom de la machine virtuelle et le nom de l'ordinateur pour celle-ci.

Important Le nom de l'ordinateur ne peut contenir que des caractères alphanumériques et des traits d'union. Un nom d'ordinateur ne peut pas être composé de chiffres uniquement et ne peut pas contenir d'espaces.

6 (Facultatif) Entrez une description significative.

7 Indiquez si vous souhaitez que la machine virtuelle se mette sous tension après sa création.

8 Sélectionnez la manière dont vous souhaitez déployer la machine virtuelle.

Option	Action
Nouveau	Vous déployez une nouvelle machine virtuelle avec des paramètres personnalisables. a Sélectionnez une famille de systèmes d'exploitation et le système d'exploitation. b (Facultatif) Sélectionnez une image de démarrage. c Sélectionnez la stratégie de calcul. d Sélectionnez la taille de la machine virtuelle ou cliquez sur **Options de dimensionnement personnalisé** pour entrer manuellement les paramètres de calcul, de mémoire et de stockage. Les options de dimensionnement prédéfinies sont Petit, Moyen et Grand. e Spécifiez les paramètres de stockage de la machine virtuelle, comme la stratégie de stockage et la taille de l'espace de stockage en Go. f Spécifiez les paramètres réseau de la machine virtuelle, comme le réseau, le mode IP, l'adresse IP et la carte réseau principale.
À partir du modèle	Vous déployez une machine virtuelle à partir d'un modèle que vous sélectionnez dans le catalogue de modèles. a Sélectionnez le modèle de machine virtuelle dans le catalogue. b (Facultatif) Sélectionnez cette option pour utiliser une stratégie de stockage personnalisée et sélectionnez la stratégie dans **Stratégie de stockage personnalisée à utiliser**. c Si un contrat de licence d'utilisateur final est disponible, vous devez le consulter et l'accepter.

9 Cliquez sur **OK** pour créer la machine virtuelle.

10 Cliquez sur **Ajouter** pour ajouter la machine virtuelle au vApp.

Enregistrer un vApp en tant que modèle de vApp dans un catalogue

En ajoutant un vApp à un catalogue, vous le convertissez en un modèle de vApp.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de vApp** prédéfini ou un ensemble de droits équivalent.
- Votre organisation doit disposer d'un catalogue et d'un centre de données virtuel avec de l'espace disponible.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.

2 Cliquez sur l'icône pour afficher les vApp dans une vue de carte.

3 Dans le menu **Actions** du vApp que vous souhaitez ajouter à un catalogue, sélectionnez **Ajouter au catalogue**.

Note Vous pouvez ajouter des vApp à un catalogue, même si les machines virtuelles qui appartiennent au vApp sont en cours d'exécution. Toutefois, si vous sélectionnez un vApp en cours d'exécution, il est ajouté au catalogue en tant que modèle de vApp et toutes les machines virtuelles sont à l'état interrompu.

4 Sélectionnez le catalogue de destination dans le menu déroulant **Catalogue**.

5 Entrez le nom et la description (facultative) du modèle de vApp.

6 (Facultatif) Sélectionnez **Remplacer un élément de catalogue** si vous voulez que le nouvel élément de catalogue remplace un modèle de vApp existant et sélectionnez l'élément de catalogue à remplacer.

Par exemple, lorsque vous importez la nouvelle version d'un vApp dans le catalogue, vous voudrez peut-être remplacer l'ancienne version.

7 Spécifiez la manière dont le modèle sera utilisé.

Ce paramètre s'applique lorsque vous créez un vApp à partir du modèle de vApp. Il est ignoré lorsque vous créez un vApp à l'aide de machines virtuelles individuelles à partir de ce modèle.

Option	Description
Faire une copie identique	Sélectionnez cette option pour effectuer une copie identique du vApp lorsque vous créez un vApp à partir du modèle de vApp.
Personnaliser les paramètres de la machine virtuelle	Sélectionnez cette option pour permettre la personnalisation des paramètres de la machine virtuelle lorsque vous créez un vApp à partir du modèle de vApp.

8 Cliquez sur **OK** pour terminer la création du modèle de vApp.

Résultats

Le vApp est enregistré en tant que modèle vApp et apparaît dans le catalogue de destination.

Télécharger un vApp comme module OVF

Vous pouvez télécharger un vApp en tant que module OVF ou en tant qu'OVA, qui est une distribution de fichier unique du même module de fichier OVF.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de vApp** prédéfini ou un ensemble de droits équivalent.

- Vérifiez que le vApp est hors tension et non déployé.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Cliquez sur l'icône pour afficher les vApp dans une vue de carte.
3. Dans le menu **Actions** du vApp à télécharger, sélectionnez **Télécharger**.
4. Sélectionnez le format dans lequel télécharger le vApp.
5. (Facultatif) Sélectionnez **Conserver les informations d'identité** pour inclure les adresses UUID et MAC des machines virtuelles qui se trouvent dans le vApp, dans le module OVF téléchargé.

   Cette opération limite la portabilité du module et ne doit être utilisée qu'en cas de besoin.
6. Cliquez sur **OK** pour confirmer la sélection et lancer le téléchargement.

Résultats

Par défaut, le module est téléchargé dans le dossier `Téléchargements` correspondant à votre navigateur.

Renouveler le bail d'un vApp

Si le bail d'un vApp a expiré ou s'il est sur le point d'expirer, vous pouvez le renouveler.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Utilisateur de vApp** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Sélectionnez le vApp que vous souhaitez renouveler.
3. Dans le menu **Actions**, sélectionnez **Renouveler le bail**.

Résultats

Le bail est renouvelé. La durée du nouveau bail s'affiche dans le champ **Bail**.

Supprimer un vApp

Vous pouvez supprimer un vApp, ce qui le supprime de votre organisation.

Conditions préalables

Votre vApp doit être arrêté.

Vous devez au moins être un **auteur de vApp**.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **vApp** dans le panneau de gauche.
2. Sélectionnez le vApp à supprimer.
3. Dans le menu **Actions**, sélectionnez **Supprimer**.
4. Cliquez sur **OK**.

Résultats

Le vApp est supprimé.

Gestion des réseaux de centre de données virtuel d'organisation 4

Les réseaux VDC d'organisation sont créés et attribués à votre VDC d'organisation par un **administrateur système** ou un **administrateur d'organisation**. Un **administrateur d'organisation** peut consulter les informations sur les réseaux, configurer des services réseau, etc.

Vous pouvez utiliser des réseaux de centre de données virtuel d'organisation directs, routés, internes ou inter-VDC reposant sur NSX Data Center for vSphere.

Vous pouvez utiliser des réseaux de centre de données virtuel d'organisation routés, internes et importés reposant sur NSX-T Data Center.

Tableau 4-1. Types de réseaux VDC d'organisation

Réseau de type centre de données	Description
Direct	Un réseau VDC d'organisation disposant d'une connexion directe à l'un des réseaux externes qui sont provisionnés par **l'administrateur système** et qui reposent sur des ressources vSphere. Les réseaux directs sont uniquement pris en charge pour les VDC d'organisation qui reposent sur NSX Data Center for vSphere. Accessible par plusieurs VDC d'organisation. Des machines virtuelles appartenant à différents VDC d'organisation peuvent se connecter à ce réseau et en voir le trafic. Ce réseau fournit une connectivité directe de couche 2 aux machines virtuelles situées à l'extérieur du VDC d'organisation. Les machines virtuelles situées à l'extérieur de ce VDC d'organisation peuvent se connecter directement aux machines virtuelles dans le VDC d'organisation. **Note** Seul votre **administrateur système** peut ajouter un réseau VDC d'organisation direct. Peut être IPv4 ou IPv6.
Isolé (interne)	Accessible uniquement par le même VDC d'organisation. Seules les machines virtuelles situées dans ce VDC d'organisation peuvent se connecter au réseau du VDC d'organisation interne et en voir le trafic. Les réseaux isolés sont pris en charge pour les VDC d'organisation reposant sur NSX-T Data Center et pour l'instance de NSX Data Center for vSphere du VDC d'organisation. Le réseau du VDC d'organisation isolé fournit à un VDC d'organisation un réseau privé isolé auquel plusieurs machines virtuelles et vApp peuvent se connecter. Ce réseau ne fournit aucune connectivité aux machines virtuelles situées à l'extérieur du VDC d'organisation. Les machines situées à l'extérieur du VDC d'organisation ne peuvent pas se connecter aux machines situées à l'intérieur du VDC d'organisation.

Tableau 4-1. Types de réseaux VDC d'organisation (suite)

Réseau de type centre de données	Description
Routage	Accessible uniquement par le même VDC d'organisation. Seules les machines virtuelles situées à l'intérieur de ce VDC d'organisation peuvent se connecter à ce réseau. Ce réseau fournit également un accès contrôlé à un réseau externe. En tant qu'**administrateur système** ou **administrateur d'organisation**, vous pouvez configurer des paramètres de traduction d'adresse réseau (NAT), de pare-feu et VPN pour rendre certaines machines virtuelles accessibles depuis le réseau externe. Peut être IPv4 ou IPv6.
Importé	Ce réseau utilise un commutateur logique NSX-T existant Seul un **administrateur système** peut importer un réseau.
Inter-VDC	Ce réseau fait partie d'un réseau étiré englobant un groupe de centres de données. Un groupe de centres de données peut comprendre entre deux et quatre centres de données virtuels d'organisation dans un déploiement vCloud Director unique ou multisite. Les machines virtuelles connectées à ce réseau sont connectées au réseau étiré sous-jacent. La mise en réseau inter-VDC nécessite NSX Data Center for vSphere. Peut être IPv4 uniquement. Pour plus d'informations sur les réseaux inter-VDC, reportez-vous au Chapitre 5 Gestion de la mise en réseau entre centres de données virtuels.

Toutes les étapes permettant de gérer vos réseaux VDC d'organisation sont documentées en partant du principe que vous disposez de plusieurs centres de données virtuels.

Ce chapitre contient les rubriques suivantes :

- Afficher les réseaux VDC d'organisation disponibles
- Ajouter un réseau de centre de données virtuel d'organisation isolé
- Ajouter un réseau de centre de données virtuel d'organisation acheminé
- Ajouter un réseau de centre de données virtuel d'organisation direct
- Ajouter un réseau VDC d'organisation avec un commutateur logique NSX-T importé
- Modifier les paramètres généraux d'un réseau de centre de données virtuel d'organisation
- Convertir un réseau de centre de données virtuel d'organisation
- Convertir l'interface d'un réseau VDC d'organisation acheminé
- Afficher les adresses IP utilisées pour un réseau de centre de données virtuel d'organisation
- Ajouter des adresses IP à un pool d'adresses IP de réseau de centre de données virtuel d'organisation
- Modifier ou supprimer des plages d'adresses IP utilisées dans un réseau de centre de données virtuel d'organisation
- Modifier les paramètres DNS d'un réseau de centre de données virtuel d'organisation

- Configurer les paramètres DHCP pour un réseau de centre de données virtuel d'organisation isolé
- Modifier ou supprimer un pool DHCP existant pour un réseau
- Réinitialiser un réseau de centre de données virtuel d'organisation
- Supprimer un réseau de centre de données virtuel d'organisation

Afficher les réseaux VDC d'organisation disponibles

Vous pouvez afficher les réseaux de centre de données virtuel d'organisation disponibles.

Conditions préalables

Cette opération nécessite les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.

Procédure

- Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

Résultats

Vous avez accès à une liste des réseaux disponibles que vous pouvez trier par nom.

Étape suivante

Vous pouvez ajouter un nouveau réseau. Vous pouvez également modifier, supprimer ou réinitialiser un réseau existant.

Ajouter un réseau de centre de données virtuel d'organisation isolé

Vous pouvez ajouter un réseau VDC d'organisation isolé, qui est accessible uniquement par cette organisation. Il ne fournit aucune connectivité aux machines virtuelles situées à l'extérieur de cette organisation. Les machines virtuelles situées à l'extérieur de cette organisation ne peuvent pas se connecter aux machines virtuelles à l'intérieur de cette organisation.

Vous pouvez ajouter un mélange de réseaux VDC d'organisation isolés ou acheminés pour répondre aux besoins de votre organisation. Par exemple, vous pouvez isoler un réseau qui contient des informations sensibles et disposer d'un réseau distinct associé à une passerelle Edge et connecté à Internet.

Vous pouvez créer un réseau VDC isolé qui dépend d'un pool de réseaux. Votre fournisseur de services peut également créer un réseau VDC isolé qui est sauvegardé par un commutateur logique NSX-T.

Vous pouvez créer uniquement un réseau VDC d'organisation isolé IPv4.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur **Ajouter**.
3. Sur la page **Sélectionner un type de réseau**, sélectionnez **Isolé** et cliquez sur **Suivant**.
4. Entrez un nom significatif pour votre réseau VDC d'organisation.
5. Entrez les paramètres CIDR (Classless Inter-Domain Routing, notation de routage interdomaine sans classe) du réseau isolé.

   Utilisez le format *adresse_IP_de_passerelle_réseau/longueur_préfixe_de_sous-réseau*, par exemple, **`192.167.1.1/24`**.
6. (Facultatif) Entrez la description du réseau VDC d'organisation.
7. (Facultatif) Pour rendre le réseau VDC d'organisation disponible pour d'autres VDC d'organisation au sein d'une même organisation, activez l'option **Partagé**.

   Cela peut s'avérer utile lorsqu'il existe une application au sein d'un VDC d'organisation qui dispose d'un pool de réservation ou d'allocation défini comme modèle d'allocation. Dans ce cas, l'espace peut s'avérer insuffisant pour exécuter plus de machines virtuelles. Pour résoudre ce problème, vous pouvez créer un VDC d'organisation secondaire avec paiement à l'utilisation et exécuter plus de machines virtuelles sur ce réseau de manière temporaire.

   Note Les VDC d'organisation doivent être pris en charge par le même VDC fournisseur.
8. Cliquez sur **Suivant**.
9. (Facultatif) Pour réserver une ou plusieurs adresses IP à des fins d'attribution aux machines virtuelles requérant des adresses IP statiques, configurez les **pools d'adresses IP statiques** pour le réseau.
   a. Entrez l'adresse IP ou une plage d'adresses IP, puis cliquez sur **Ajouter**.
   b. Pour ajouter plusieurs adresses IP ou plages d'adresses statiques, répétez cette étape.
   c. (Facultatif) Pour modifier ou supprimer des adresses IP et des plages d'adresses IP, cliquez sur **Modifier** ou **Supprimer**.
10. Cliquez sur **Suivant**.

11 (Facultatif) Configurez les paramètres DNS.

Option	Action
DNS primaire	Entrez l'adresse IP de votre serveur DNS primaire.
DNS secondaire	Entrez l'adresse IP de votre serveur DNS secondaire.
Suffixe DNS	Entrez votre suffixe DNS. Le suffixe DNS est le nom DNS, à l'exclusion du nom d'hôte.

12 Cliquez sur **Suivant**.

13 Sur la page **Prêt à terminer**, vérifiez les paramètres du réseau VDC d'organisation que vous avez fournis, puis cliquez sur **Terminer**.

Ajouter un réseau de centre de données virtuel d'organisation acheminé

Pour contrôler l'accès à un réseau externe, vous pouvez ajouter un réseau VDC d'organisation acheminé. Les **administrateurs système** et **d'organisation** peuvent configurer des paramètres de traduction d'adresse réseau (NAT), de pare-feu et VPN pour rendre certaines machines virtuelles accessibles depuis le réseau externe.

Vous pouvez ajouter un mélange de réseaux VDC d'organisation isolés ou acheminés pour répondre aux besoins de votre organisation. Par exemple, vous pouvez ajouter un réseau associé à une passerelle Edge et connecté à Internet, tout en ayant un réseau isolé contenant des informations sensibles.

Vous pouvez ajouter un réseau VDC d'organisation acheminé IPv4 ou IPv6.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur **Ajouter**.

3 Sur la page **Sélectionner un type de réseau**, sélectionnez **Acheminé**, puis cliquez sur **Suivant**.

4 Entrez un nom significatif pour votre réseau VDC d'organisation.

5 Entrez les paramètres CIDR (Classless Inter-Domain Routing, notation de routage interdomaine sans classe) du réseau VDC d'organisation acheminé.

   Utilisez le format *adresse_IP_de_passerelle_réseau/longueur_préfixe_de_sous-réseau*, par exemple, **`192.167.1.1/24`**.

6 (Facultatif) Saisissez la description du réseau VDC d'organisation.

7 (Facultatif) Pour rendre le réseau VDC d'organisation disponible pour d'autres VDC d'organisation au sein d'une même organisation, activez l'option **Partagé**.

Cela peut s'avérer utile lorsqu'une application au sein d'un VDC d'organisation possède un pool de réservation ou d'allocation défini comme modèle d'allocation. Dans ce cas, l'espace peut s'avérer insuffisant pour exécuter plus de machines virtuelles. Pour résoudre ce problème, vous pouvez créer un VDC d'organisation secondaire avec paiement à l'utilisation et exécuter plus de machines virtuelles sur ce réseau de manière temporaire.

Note Les VDC d'organisation doivent partager le même pool de réseaux.

8 Cliquez sur **Suivant**.

9 Sur la page **Connexion Edge**, sélectionnez une passerelle Edge à laquelle associer le réseau VDC d'organisation.

Si le VDC d'organisation inclut plusieurs passerelles Edge, vous devez sélectionner celle à laquelle ce réseau sera connecté. Pour prendre en charge un autre réseau acheminé, la passerelle Edge doit afficher une valeur d'au moins 1 dans la colonne Nbre de réseaux disponibles.

10 Dans le menu déroulant **Type d'interface**, sélectionnez le type d'interface.

Option	Description
Interne	Connexion à l'une des interfaces internes de la passerelle Edge. Le nombre maximal de réseaux autorisés est de 9.
Distribué	Crée le réseau sur un routeur logique distribué connecté à cette passerelle Edge. Le nombre maximal de réseaux autorisés est de 400.
Sous-interface	Étend un réseau VDC d'organisation. vCloud Director identifie le réseau à étendre via le VPN L2. vCloud Director, à l'aide de la virtualisation de réseau NSX, crée un type d'interface de jonction pour ce réseau. Le nombre maximal de réseaux autorisés est de 200.

11 (Facultatif) Pour activer le marquage des VLAN invités sur ce réseau, activez l'option **VLAN invité autorisé**.

12 Cliquez sur **Suivant**.

13 (Facultatif) Pour réserver une ou plusieurs adresses IP à des fins d'attribution aux machines virtuelles requérant des adresses IP statiques, configurez les **pools d'adresses IP statiques** pour le réseau.

   a Entrez l'adresse IP ou une plage d'adresses IP, puis cliquez sur **Ajouter**.

   b Pour ajouter plusieurs adresses IP ou plages d'adresses statiques, répétez cette étape.

   c (Facultatif) Pour modifier ou supprimer des adresses IP et des plages d'adresses IP, cliquez sur **Modifier** ou **Supprimer**.

14 Cliquez sur **Suivant**.

15 (Facultatif) Configurez les paramètres DNS.

Option	Action
DNS primaire	Entrez l'adresse IP de votre serveur DNS primaire.
DNS secondaire	Entrez l'adresse IP de votre serveur DNS secondaire.
Suffixe DNS	Entrez votre suffixe DNS. Le suffixe DNS est le nom DNS, à l'exclusion du nom d'hôte.

16 Cliquez sur **Suivant**.

17 Sur la page **Prêt à terminer**, vérifiez les paramètres du réseau VDC d'organisation que vous avez fournis, puis cliquez sur **Terminer**.

Ajouter un réseau de centre de données virtuel d'organisation direct

Pour se connecter à un réseau externe par une route directe, les **administrateurs système** peuvent configurer une connexion directe.

Si vous vous connectez au portail de locataires vCloud Director en tant qu'**administrateur d'organisation** et que vous tentez de créer un réseau de centre de données virtuel d'organisation direct, vous recevez un message d'avertissement indiquant que vous ne disposez pas des droits suffisants.

Conditions préalables

Cette opération est limitée aux administrateurs système.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur **Ajouter**.

3 Sur la page **Sélectionner un type de réseau**, sélectionnez **Direct** et cliquez sur **Suivant**.

4 Entrez un nom significatif pour votre réseau VDC d'organisation.

5 (Facultatif) Saisissez la description du réseau VDC d'organisation.

6 (Facultatif) Pour rendre le réseau VDC d'organisation disponible pour d'autres VDC d'organisation au sein d'une même organisation, activez l'option **Partagé**.

7 Sur la page **Connexion au réseau externe**, sélectionnez le réseau externe auquel vous souhaitez que le nouveau réseau de centre de données virtuel d'organisation se connecte directement, puis cliquez sur **Suivant**.

8 Sur la page **Prêt à terminer**, vérifiez les paramètres du réseau VDC d'organisation que vous avez fournis, puis cliquez sur **Terminer**.

Ajouter un réseau VDC d'organisation avec un commutateur logique NSX-T importé

Les **administrateurs système** peuvent créer un réseau VDC d'organisation en important un commutateur logique à partir d'une instance associée de NSX-T Manager.

Note Un commutateur logique NSX-T vous permet uniquement de créer un réseau d'organisation isolé IPv4. Vous ne pouvez pas créer de réseau d'organisation direct basé sur un commutateur logique NSX-T.

Conditions préalables

- Cette opération est limitée aux **administrateurs système**.
- Le centre de données virtuel fournisseur qui soutient le centre de données virtuel d'organisation cible doit être associé à une instance de NSX-T Manager.
- L'**administrateur système** doit créer au moins un commutateur logique NSX-T qui n'est pas en cours d'utilisation par d'autres réseaux de centre de données virtuel d'organisation.

Pour plus d'informations sur la création et la configuration des commutateurs logiques NSX-T, consultez le *Guide d'administration de NSX-T*.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur **Ajouter**.

3 Sur la page **Sélectionner un type de réseau**, sélectionnez **Importer** et cliquez sur **Suivant**.

4 Entrez un nom pour le nouveau réseau VDC d'organisation et, éventuellement, une description, puis cliquez sur **Suivant**.

5 Dans la liste des commutateurs logiques NSX-T disponibles, sélectionnez le commutateur cible en cliquant sur le bouton radio en regard de son nom, puis cliquez sur **Suivant**.

6 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`**.

   Si le commutateur est configuré avec un sous-réseau, cette information est préremplie.

7 (Facultatif) Configurez les paramètres DNS et le pool d'adresses IP statiques.

   Vous pouvez ajouter plusieurs adresses IP et plages d'adresses IP.

8 Cliquez sur **Suivant**.

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

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

Vous pouvez modifier les propriétés des réseaux VDC d'organisation.

Conditions préalables

Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur le nom du réseau VDC d'organisation que vous souhaitez afficher ou modifier.

3 Dans l'onglet **Général**, cliquez sur **Modifier**.

   a Modifiez le nom et la description du réseau.

   b Activez ou désactivez l'option **Partagé** pour partager ou ne pas partager le réseau VDC d'organisation avec d'autres centres de données virtuels au sein d'une même organisation.

4 Cliquez sur **Enregistrer**.

Convertir un réseau de centre de données virtuel d'organisation

Après avoir créé un réseau VDC d'organisation, vous pouvez convertir un réseau isolé en un réseau acheminé, et inversement.

Conditions préalables

Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le nom du réseau VDC d'organisation que vous souhaitez convertir.
3. Dans l'onglet **Général**, cliquez sur **Modifier**.
4. Cliquez sur **Connexion**.
5. Pour vous connecter à une passerelle Edge ou pour isoler le réseau de tous les autres réseaux, activez l'option **Se connecter à une passerelle Edge** ou désactivez cette option.

Option	Action
Convertissez un réseau isolé en un réseau acheminé.	1 Activez l'option **Se connecter à une passerelle Edge**. 2 Sélectionnez la passerelle Edge à laquelle se connecter dans la liste des passerelles Edge disponibles. 3 Sélectionnez le type d'interface. 4 Pour autoriser un VLAN invité, activez l'option **VLAN invité autorisé**.
Convertissez un réseau acheminé en un réseau isolé.	Désactivez l'option **Se connecter à une passerelle Edge**.

6. Cliquez sur **Enregistrer**.

Résultats

Vous avez converti le réseau VDC d'organisation.

Convertir l'interface d'un réseau VDC d'organisation acheminé

Vous pouvez modifier l'interface d'un réseau pour qu'elle passe du routage interne au routage de sous-interface ou distribué, par exemple, en modifiant les propriétés du réseau.

Note Les réseaux inter-VDC ne peuvent pas être convertis.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le nom du réseau que vous souhaitez convertir.
3. Cliquez sur le nom du réseau VDC d'organisation que vous souhaitez modifier.

4 Dans l'onglet **Général**, cliquez sur **Modifier**.

5 Cliquez sur **Connexion**.

6 Dans le menu déroulant **Type d'interface**, sélectionnez le type d'interface.

Option	Description
Interne	Connexion à l'une des interfaces internes de la passerelle Edge. Le nombre maximal de réseaux autorisés est de 9.
Distribué	Crée le réseau sur un routeur logique distribué connecté à cette passerelle Edge. Le nombre maximal de réseaux autorisés est de 400.
Sous-interface	Étend un réseau VDC d'organisation. vCloud Director identifie le réseau à étendre via le VPN L2. vCloud Director, à l'aide de la virtualisation de réseau NSX, crée un type d'interface de jonction pour ce réseau. Le nombre maximal de réseaux autorisés est de 200.

7 Cliquez sur **Enregistrer**.

Afficher les adresses IP utilisées pour un réseau de centre de données virtuel d'organisation

Vous pouvez afficher la liste des adresses IP utilisées d'un pool d'adresses IP d'un réseau de centre de données virtuel d'organisation.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé ou acheminé.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur le nom du réseau pour lequel vous souhaitez afficher les adresses IP utilisées.

3 Cliquez sur l'onglet **Gestion des adresses IP**.

4 Cliquez sur **Allocations IP** pour voir quelles adresses IP sont en cours d'utilisation.

Ajouter des adresses IP à un pool d'adresses IP de réseau de centre de données virtuel d'organisation

Si un réseau de centre de données virtuel d'organisation manque d'adresses IP, vous pouvez en ajouter à son pool d'adresses IP.

Vous ne pouvez pas ajouter des adresses IP à des réseaux de centre de données virtuel d'organisation externe ayant une connexion directe.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé ou acheminé.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le nom du réseau que vous souhaitez modifier.
3. Cliquez sur l'onglet **Gestion des adresses IP**.

   L'option **Pools d'adresses IP statiques** est sélectionnée par défaut.
4. Cliquez sur le bouton **Modifier** à droite.

   Dans la fenêtre **Modifier le réseau**, vous voyez les paramètres CIDR de la passerelle et les plages d'adresses IP, le cas échéant.
5. Dans la zone de texte **Pool d'adresses IP statiques**, entrez l'adresse IP ou la plage d'adresses IP, et cliquez sur **Ajouter**.

   Note Pour les réseaux entre VDC, les adresses IP ne doivent pas chevaucher les adresses IP attribuées aux autres réseaux VDC d'organisation à partir du même réseau étiré.
6. Cliquez sur **Enregistrer**.

Résultats

L'adresse IP ou la plage d'adresses IP est ajoutée au pool d'adresses IP du réseau.

Modifier ou supprimer des plages d'adresses IP utilisées dans un réseau de centre de données virtuel d'organisation

Si un réseau de centre de données virtuel d'organisation contient des adresses IP dont vous n'avez plus besoin, vous pouvez modifier les adresses ou les supprimer du pool d'adresses IP.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé ou acheminé.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le nom du réseau que vous souhaitez modifier.
3. Cliquez sur l'onglet **Gestion des adresses IP**.

   L'option **Pools d'adresses IP statiques** est sélectionnée par défaut.
4. Cliquez sur le bouton **Modifier** à droite.
   - Pour modifier une plage d'adresses IP, sélectionnez la plage, effectuez les modifications nécessaires et cliquez sur **Modifier**.
   - Pour supprimer une plage d'adresses IP, sélectionnez la plage et cliquez sur **Supprimer**.
5. Cliquez sur **Enregistrer**.

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

Vous pouvez modifier les paramètres DNS d'un réseau de centre de données virtuel d'organisation.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé ou acheminé.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le nom du réseau que vous souhaitez modifier.
3. Cliquez sur l'onglet **Gestion des adresses IP**.
4. Sélectionnez **DNS** et cliquez sur le bouton **Modifier** à droite.

5 Modifiez les informations relatives au DNS principal, au DNS secondaire et au suffixe DNS, si nécessaire.

6 Cliquez sur **Enregistrer**.

Configurer les paramètres DHCP pour un réseau de centre de données virtuel d'organisation isolé

Vous pouvez modifier les paramètres DHCP d'un réseau VDC d'organisation isolé. Le service DHCP d'un réseau VDC d'organisation fournit les adresses IP à partir de son pool d'adresses à des cartes réseau de VM qui sont configurés pour demander une adresse à partir de DHCP. Le service fournit l'adresse lorsque la machine virtuelle est mise sous tension.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur le nom du réseau que vous souhaitez modifier.

3 Cliquez sur l'onglet **Gestion des adresses IP**.

4 Sélectionnez **DHCP**.

Les paramètres du DHCP apparaissent sur la droite.

5 Pour activer le DHCP, cliquez sur **Modifier** à droite de **Service de pools DHCP**.

6 Activez le **service de pools DHCP** et cliquez sur **Enregistrer**.

Les adresses demandées par les clients DHCP sont extraites d'un pool DHCP.

7 Créez un pool DHCP pour le réseau.

a Cliquez sur **Ajouter**.

b Entrez une plage d'adresses IP pour le pool.

La plage d'adresses IP que vous spécifiez ne peut pas chevaucher le pool d'adresses IP statiques pour le centre de données virtuel d'organisation.

c Indiquez la durée de bail par défaut pour les adresses DHCP en secondes.

La valeur par défaut est 3 600 secondes.

d Indiquez la durée de bail maximale pour les adresses DHCP en secondes.

Il s'agit de la durée maximale pendant laquelle les adresses IP attribuées par DHCP sont allouées aux machines virtuelles. La valeur par défaut est 7 200 secondes.

8 Cliquez sur **Enregistrer**.

Modifier ou supprimer un pool DHCP existant pour un réseau

Si vous n'avez plus besoin d'un pool DHCP au sein de votre réseau de centre de données virtuel d'organisation isolé, vous pouvez le supprimer ou le modifier.

Conditions préalables

- Ces opérations nécessitent les rôles d'**administrateur d'organisation** ou d'**administrateur système** prédéfinis, ou un rôle qui inclut un ensemble de droits équivalent.
- Vérifiez que votre réseau est un réseau de centre de données virtuel d'organisation isolé.

Procédure

1 Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.

2 Cliquez sur le nom du réseau que vous souhaitez modifier.

3 Cliquez sur l'onglet **Gestion des adresses IP**.

4 Sélectionnez **DHCP**.

Les paramètres du DHCP apparaissent sur la droite.

5 Modifiez ou supprimez un pool DHCP existant.

Option	Action
Modifiez un pool DHCP.	1 Sélectionnez le pool DHCP à modifier. 2 Cliquez sur le bouton **Modifier**. 3 Mettez à jour la plage d'adresses IP du pool. 4 Modifiez la durée de bail par défaut pour les adresses DHCP en secondes. 5 Modifiez la durée de bail maximale pour les adresses DHCP en secondes. 6 Cliquez sur **Enregistrer**.
Supprimez un pool DHCP.	1 Sélectionnez le pool DHCP à supprimer. 2 Cliquez sur le bouton **Supprimer**.

Réinitialiser un réseau de centre de données virtuel d'organisation

Si les services réseau, tels que les paramètres DHCP ou les paramètres de pare-feu associés à un réseau de centre de données virtuel d'organisation, ne fonctionnent pas comme prévu, vous pouvez réinitialiser le réseau.

Lorsque vous réinitialisez le réseau de centre de données virtuel d'organisation, vous forcez le redéploiement de la passerelle du service DHCP du réseau. Cette opération entraîne une interruption temporaire des services DHCP, et aucun service réseau n'est disponible pendant la réinitialisation du réseau.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Le réseau n'est pas connecté à des machines virtuelles, des vApp ou d'autres réseaux.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Sélectionnez un réseau VDC d'organisation.
3. Cliquez sur **Réinitialiser** et confirmez l'opération de réinitialisation.

Supprimer un réseau de centre de données virtuel d'organisation

Si vous n'utilisez plus un réseau de centre de données virtuel d'organisation, vous pouvez le supprimer.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Le réseau n'est pas connecté à des machines virtuelles, des vApp ou d'autres réseaux.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Réseaux** dans le panneau de gauche.
2. Cliquez sur le bouton radio en regard du nom du réseau cible, puis cliquez sur **Supprimer**.
3. Pour confirmer, cliquez sur **OK**.

Gestion de la mise en réseau entre centres de données virtuels 5

Pour créer un réseau sur plusieurs centres de données virtuel d'organisation, vous commencez par regrouper les centres de données virtuel, puis vous créez un réseau étiré dans le groupe de centre de données. Un groupe de centre de données peut avoir une configuration de points de sortie communs ou une configuration de points de sortie pour chaque domaine d'erreur de réseau.

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

Groupe de centres de données

Groupe comprenant jusqu'à quatre centres de données virtuels configurés pour partager plusieurs points de sortie. Un groupe de centres de données peut avoir l'une des configurations de points de sortie suivantes :

Type de configuration de points de sortie	Description
Configuration de points de sortie communs	Le groupe de centres de données peut être configuré avec un point de sortie actif et un point de sortie de veille. Les deux points de sortie sont communs à tous les centres de données virtuels appartenant au groupe dans tous les domaines d'erreur du réseau du groupe de centres de données.
Configuration de points de sortie par domaine d'erreur	Le groupe de centres de données peut être configuré avec un point de sortie actif pour chaque domaine d'erreur de réseau dans le groupe de centres de données. Aucune sortie de veille ne peut être créée.

Une organisation peut avoir plusieurs groupes de centres de données. Un centre de données virtuel d'organisation peut appartenir à plusieurs groupes de centres de données.

Les centres de données virtuels d'organisation figurant dans le groupe peuvent appartenir à différents sites vCloud Director. Reportez-vous à Configurer et gérer les déploiements multisite.

Domaine d'erreur du réseau

Étendue du fournisseur réseau, représentant généralement l'instance de vCenter Server sous-jacente avec l'instance de NSX Manager associée.

Point de sortie

Passerelle Edge qui connecte un groupe de centres de données ou un domaine d'erreur de réseau à Internet. La passerelle Edge doit appartenir à un centre de données virtuel du groupe de centres de données. Les routes BGP sont configurées sur la passerelle Edge représentant le point de sortie et le routeur universel du groupe de centres de données virtuels ou du domaine d'erreur de réseau. Les chemins existants sur la passerelle Edge ne sont pas affectés.

Réseau étiré

Réseau de couche 2 étiré sur tous les centres de données virtuels d'un groupe de centres de données. Peut être IPv4 uniquement.

Ce chapitre contient les rubriques suivantes :

- Gestion des groupes de centres de données
- Gestion des réseaux étirés

Gestion des groupes de centres de données

Après avoir créé un groupe de centres de données, vous pouvez modifier la topologie réseau de ce groupe. Vous pouvez ajouter des centres de données virtuels au groupe et en supprimer. Vous pouvez échanger, remplacer et supprimer des points de sortie. Vous pouvez corriger les échecs de configuration en effectuant différentes tâches de synchronisation.

Vous ne pouvez pas convertir une configuration de sortie commune en une configuration de sortie par domaine d'erreur, ou inversement.

Créer et configurer un groupe de centres de données avec une configuration de sortie commune

Vous pouvez créer et configurer un groupe de centres de données virtuels avec une configuration de sortie commune. Pour cela, vous définissez une paire de passerelles Edge qui sont utilisées en tant que points de sortie actif et de secours pour tous les centres de données virtuels appartenant au groupe.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- L'**administrateur système** doit activer les centres de données virtuels cibles pour la mise en réseau entre centres de données virtuels.

Procédure

1 Créer un groupe de centres de données avec une configuration de sortie commune

Vous pouvez regrouper entre deux et quatre centres de données virtuels dans un groupe de centres de données avec une configuration de sortie commune.

2 Ajouter un point de sortie actif

Pour connecter votre groupe de centres de données à Internet, vous devez ajouter un point de sortie actif à sa topologie réseau.

3 Ajouter un point de sortie de secours

Dans les groupes de centres de données virtuels avec des configurations de sortie courantes, vous pouvez ajouter un point de sortie secondaire servant de point de sortie de secours pour les scénarios de tolérance de panne.

Créer un groupe de centres de données avec une configuration de sortie commune

Vous pouvez regrouper entre deux et quatre centres de données virtuels dans un groupe de centres de données avec une configuration de sortie commune.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Cliquez sur **Nouveau groupe de centres de données**.

3 Entrez un nom pour le nouveau groupe de centres de données et, éventuellement, une description.

4 Sélectionnez **Points de sortie communs** et cliquez sur **Suivant**.

5 Sur la page **Centres de données**, sélectionnez entre deux et quatre centres de données pour le nouveau groupe de centres de données, puis cliquez sur **Suivant**.

La page **Centres de données** contient une liste des centres de données virtuels activés pour la mise en réseau entre centres de données virtuels par l'**administrateur système**.

6 Vérifiez les détails du groupe de centres de données, puis cliquez sur **Terminer**.

Résultats

Le groupe de centres de données virtuels récemment créé est répertorié dans la vue **Groupes de centres de données**.

Ajouter un point de sortie actif

Pour connecter votre groupe de centres de données à Internet, vous devez ajouter un point de sortie actif à sa topologie réseau.

Conditions préalables

L'**administrateur système** a créé au moins une passerelle Edge sur l'un des centres de données virtuels qui participent au groupe de centres de données.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Cliquez sur **Ajouter un point de sortie**.

   La page **Ajouter un point de sortie actif** qui s'ouvre fournit une liste des passerelles Edge qui appartiennent aux centres de données virtuels participants.

4 Sélectionnez la passerelle Edge que vous souhaitez voir servir de point de sortie actif pour ce groupe de centres de données et cliquez sur **Ajouter**.

Résultats

Les chemins BGP sont configurés sur la passerelle Edge représentant le point de sortie et le routeur universel du groupe de centres de données virtuel. Les chemins existants sur la passerelle Edge ne sont pas affectés.

Le diagramme de la topologie réseau est mis à jour avec le point de sortie récemment ajouté. Le trafic allant des centres de données virtuels participants vers Internet est représenté par une ligne bleue continue.

Ajouter un point de sortie de secours

Dans les groupes de centres de données virtuels avec des configurations de sortie courantes, vous pouvez ajouter un point de sortie secondaire servant de point de sortie de secours pour les scénarios de tolérance de panne.

Conditions préalables

Outre la passerelle Edge qui sert de point de sortie actif, vous devez disposer d'au moins une passerelle Edge supplémentaire dans tout centre de données virtuel faisant partie du groupe.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Cliquez sur **Ajouter un point sortie de secours**.

   La page **Ajouter un point de sortie de secours** s'ouvre et affiche une liste des passerelles Edge inutilisées qui appartiennent aux centres de données virtuels participants. La passerelle Edge utilisée par le point de sortie actif dans ce groupe de centres de données virtuels n'est pas affichée.

4 Sélectionnez la passerelle Edge que vous souhaitez voir servir de point de sortie de secours pour ce groupe de centres de données et cliquez sur **Ajouter**.

Résultats

Les chemins BGP sont configurés sur la passerelle Edge représentant le point de sortie et le routeur universel du groupe de centres de données virtuel. Les chemins existants sur la passerelle Edge ne sont pas affectés.

Le diagramme de la topologie réseau est mis à jour avec le point de sortie récemment ajouté. Dans les scénarios de tolérance de panne, le trafic allant des centres de données virtuels participants vers Internet est représenté par une ligne bleue en pointillés.

Créer et configurer un groupe de centres de données avec une configuration de sortie de domaine d'erreur

Vous pouvez créer et configurer un groupe de centres de données virtuels avec une configuration de sortie de domaine d'erreur. Pour cela, vous configurez une passerelle Edge qui est utilisée en tant que point de sortie actif pour chaque domaine d'erreur du réseau dans le groupe. Vous ne pouvez pas créer de sortie de veille dans un groupe de centres de données avec une configuration de sortie de domaine d'erreur.

Conditions préalables

Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.

Procédure

1 Créer un groupe de centres de données avec une configuration de sortie de domaine d'erreur

   Vous pouvez regrouper entre deux et quatre centres de données virtuels dans un groupe de centres de données avec une configuration de sortie de domaine d'erreur.

2 Ajouter un point de sortie pour un domaine d'erreur

Pour établir une connexion entre les centres de données virtuels d'un domaine d'erreur du réseau dans un groupe de centres de données et Internet, vous devez ajouter un point de sortie à ce domaine d'erreur du réseau. Vous pouvez ajouter un point de sortie à chaque domaine d'erreur du réseau dans le groupe de centres de données. Les points de sortie de secours ne sont pas pris en charge dans un groupe de centres de données ayant une configuration de sortie de domaine d'erreur.

Créer un groupe de centres de données avec une configuration de sortie de domaine d'erreur

Vous pouvez regrouper entre deux et quatre centres de données virtuels dans un groupe de centres de données avec une configuration de sortie de domaine d'erreur.

Conditions préalables

L'**administrateur système** doit avoir activé les centres de données virtuels cibles pour la mise en réseau intercentre de données virtuel.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Cliquez sur **Nouveau groupe de centres de données**.

3 Entrez un nom pour le nouveau groupe de centres de données et, éventuellement, une description.

4 Sélectionnez **Points de sortie par domaine d'erreur**, puis cliquez sur **Suivant**.

5 Sur la page **Centres de données**, sélectionnez entre deux et quatre centres de données pour le nouveau groupe de centres de données, puis cliquez sur **Suivant**.

La page **Centres de données** contient une liste des centres de données virtuels activés pour la mise en réseau entre centres de données virtuels par l'**administrateur système**.

6 Vérifiez les détails du groupe de centres de données, puis cliquez sur **Terminer**.

Résultats

Le groupe de centres de données virtuels récemment créé est répertorié dans la vue **Groupes de centres de données**.

Ajouter un point de sortie pour un domaine d'erreur

Pour établir une connexion entre les centres de données virtuels d'un domaine d'erreur du réseau dans un groupe de centres de données et Internet, vous devez ajouter un point de sortie à ce domaine d'erreur du réseau. Vous pouvez ajouter un point de sortie à chaque domaine d'erreur du réseau dans le groupe de centres de données. Les points de sortie de secours ne sont pas

pris en charge dans un groupe de centres de données ayant une configuration de sortie de domaine d'erreur.

Conditions préalables

Outre les passerelles Edge utilisées en tant que points de sortie dans ce groupe de centres de données, vous devez disposer d'au moins une passerelle Edge inutilisée dans un centre de données virtuel participant.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3. Dans le diagramme de la topologie réseau, cliquez sur le domaine d'erreur du réseau cible.

   Les domaines d'erreur du réseau sont représentés par des lignes continues et leurs noms apparaissent en bas du diagramme.

   Le domaine d'erreur sélectionné est représenté en bleu.

4. Cliquez sur **Ajouter un point de sortie**.

   La page **Ajouter un point de sortie actif** s'ouvre et affiche une liste des passerelles Edge qui appartiennent aux centres de données virtuels participants.

5. Sélectionnez la passerelle Edge que vous souhaitez voir servir de point de sortie pour ce domaine d'erreur et cliquez sur **Ajouter**.

Résultats

Les chemins BGP sont configurés sur la passerelle Edge représentant le point de sortie et le routeur universel du domaine d'erreur du réseau. Les chemins existants sur la passerelle Edge ne sont pas affectés.

Le diagramme de la topologie réseau est mis à jour avec le point de sortie récemment ajouté. Le trafic allant des centres de données virtuels dans le domaine d'erreur du réseau vers Internet est représenté par une ligne bleue continue.

Afficher un groupe de centres de données

Vous pouvez afficher les groupes de centres de données de votre organisation et les détails relatifs à leur configuration actuelle.

Conditions préalables

Cette opération nécessite le rôle **Administrateur système** ou un rôle doté du droit **Groupe de VDC : Afficher le groupe de VDC** publié dans l'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

Ajouter un centre de données virtuel à un groupe de centres de données

Vous pouvez ajouter un centre de données virtuel à un groupe de centres de données, étirant ainsi les réseaux existants vers le nouveau centre de données virtuel.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- Le groupe de centres de données contient moins de quatre centres de données virtuels.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3. Cliquez sur **Ajouter un centre de données**.

4 Sur la page de **Centres de données**, sélectionnez le centre de données que vous souhaitez ajouter au groupe de centres de données et cliquez sur **Terminer**.

La page **Centres de données** contient une liste des centres de données virtuels qui sont activés par l'administrateur système pour la mise en réseau entre centres de données virtuels.

Note Un groupe de centres de données doit contenir jusqu'à quatre centres de données virtuels.

Supprimer un centre de données virtuel d'un groupe de centres de données

Vous pouvez supprimer un centre de données virtuel d'un groupe de centres de données, annulant ainsi l'extension des réseaux existants à partir de ce centre de données virtuelles.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- Le groupe de centres de données doit contenir au moins trois centres de données virtuels.
- Le centre de données virtuel que vous souhaitez supprimer ne doit pas fournir de point de sortie au groupe de centres de données.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Dans le coin supérieur droit de la fiche du centre de données virtuel cible, cliquez sur les trois points, puis sur **Supprimer**.

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

Résultats

Le centre de données virtuel est supprimé du diagramme de topologie réseau du groupe de centres de données.

Synchroniser un groupe de centres de données

Pour réappliquer les configurations réseau du groupe de centres de données et vous assurer que tous les centres de données virtuels participants sont actifs, vous pouvez synchroniser le groupe de centres de données.

Note Pendant le processus de synchronisation du groupe de centres de données, ce dernier devient non disponible pendant quelques secondes, car le routeur universel se synchronise dans NSX.

Conditions préalables

Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.
2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.
3. Cliquez sur **Synchroniser le groupe de centres de données**.
4. Pour confirmer, cliquez sur **OK**.

Échanger les points de sortie dans un groupe de centres de données avec une configuration commune de sortie

Après que vous avez configuré des points de sortie actifs et en veille dans un groupe de centres de données avec une configuration commune de sortie, vous pouvez échanger les rôles des points de sortie. Le point de sortie actif peut devenir un point de sortie en veille et inversement.

Conditions préalables

Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Cliquez sur **Échanger les points de sortie**.

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

Résultats

Le diagramme de la topologie réseau est mis à jour avec les nouvelles routes de trafic. Le trafic Internet est maintenant redirigé vers le nouveau point de sortie actif.

Remplacer la passerelle Edge d'un point de sortie

Vous pouvez remplacer la passerelle Edge qui représente un point de sortie actif ou en veille dans un groupe de centres de données.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- La nouvelle passerelle Edge ne doit pas être utilisée par d'autres points de sortie dans le groupe de centres de données.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Si vous remplacez un point de sortie d'une configuration de domaine d'erreur de réseau, sur le diagramme de topologie réseau, sélectionnez le domaine d'erreur de réseau du point de sortie cible.

   Les domaines de pannes de réseau sont représentés par des lignes continues et des noms de domaine en bas du diagramme.

   Le domaine d'erreur de réseau sélectionné est marqué en bleu.

4 Dans le coin supérieur droit de la fiche du point sortie cible, cliquez sur les trois points, puis sur **Remplacer**.

   La page **Remplacer le point de sortie** s'ouvre fournissant une liste des passerelles Edge qui appartiennent aux centres de données virtuels participants.

5 Sélectionnez la nouvelle passerelle Edge et cliquez sur **Remplacer**.

Résultats

Les routes BGP sont supprimées de l'ancienne passerelle Edge et configurées sur la nouvelle passerelle Edge représentant le point de sortie et le routeur universel du groupe de centres de données virtuel.

Le diagramme de topologie réseau est mis à jour avec le nom de la nouvelle passerelle Edge.

Supprimer un point de sortie

Pour déconnecter d'Internet un groupe de centres de données ou un domaine d'erreur réseau, vous pouvez supprimer son point de sortie.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- Si vous souhaitez supprimer un point de sortie actif couplé à un point de sortie en veille, vous devez échanger les points de sortie ou supprimer le point de sortie en veille.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Si vous supprimez un point de sortie d'une configuration de domaine d'erreur de réseau, sur le diagramme de topologie réseau, sélectionnez le domaine d'erreur de réseau du point de sortie cible.

   Les domaines de pannes de réseau sont représentés par des lignes continues et des noms de domaine en bas du diagramme.

   Le domaine d'erreur de réseau sélectionné est marqué en bleu.

4 Dans le coin supérieur droit de la fiche du point de sortie cible, cliquez sur les trois points, puis sur **Supprimer**.

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

Résultats

Les routes BGP sont supprimées de la passerelle Edge représentant le point de sortie s'il n'est pas en cours d'utilisation par d'autres routeurs universels.

Le point de sortie est supprimé du diagramme de topologie réseau.

Synchroniser les routes et les points de sortie

Vous pouvez réappliquer la configuration de routage dynamique à un groupe de centres de données ou à un domaine d'erreur de réseau, et à ses points de sortie associés en synchronisant les routes. Vous pouvez vous assurer qu'un point de sortie est correctement connecté au groupe de centres de données en synchronisant le point de sortie.

Conditions préalables

- Cette opération nécessite le rôle **Administrateur système** ou un rôle disposant du droit **Groupe de VDC : Configurer le groupe de VDC** publié dans l'organisation.
- Vous avez configuré un point de sortie pour le groupe de centres de données ou le domaine d'erreur du réseau cible.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Si vous synchronisez un domaine d'erreur de réseau dans un groupe de centres de données, sur le diagramme de topologie réseau, sélectionnez le domaine d'erreur de réseau cible.

Les domaines de pannes de réseau sont représentés par des lignes continues et des noms de domaine en bas du diagramme.

Le domaine d'erreur de réseau sélectionné est marqué en bleu.

4 Pour réappliquer la configuration du routage dynamique au groupe ou au domaine d'erreur de réseau, et à ses points de sortie associés, cliquez sur **Synchroniser les routes**, puis cliquez sur **OK**.

5 Pour synchroniser un point de sortie avec son groupe de centres de données, dans le coin supérieur droit de la fiche du point de sortie cible, cliquez sur les trois points, sur **Synchroniser**, puis sur **OK**.

Gestion des réseaux étirés

Après avoir créé et configuré un groupe de centres de données, vous pouvez créer et gérer des réseaux étirés de couche 2 s'étendant sur les centres de données virtuels appartenant au groupe.

Au niveau du centre de données virtuel, les réseaux étirés apparaissent sous la forme de réseaux de centre de données virtuel d'organisation de type routage inter-VDC.

Ajouter un réseau étiré

Vous pouvez créer un réseau étiré entre tous les centres de données virtuels qui participent à un groupe de centres de données.

Vous pouvez ajouter uniquement un réseau étiré IPv4.

Conditions préalables

Cette opération nécessite le rôle prédéfini **Administrateur d'organisation** ou un rôle disposant du droit **Réseau de VDC d'organisation : Modifier les propriétés**.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.
2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.
3. Dans le panneau de gauche, cliquez sur **Réseaux étirés**.

   La liste des réseaux étirés s'affiche dans une vue de grille.
4. Cliquez sur **Ajouter**.
5. Entrez un nom et une description (facultative) pour le nouveau réseau étiré.
6. Entrez les paramètres CIDR (Classless Inter-Domain Routing) du réseau, puis cliquez sur **Créer**.

   Utilisez le format *adresse_IP_de_passerelle_réseau/longueur_préfixe_de_sous-réseau*, par exemple, **`192.167.1.1/24`**.

Résultats

Vous pouvez voir le réseau nouvellement créé dans la liste de réseaux étirés du groupe de centres de données.

Un réseau de centre de données virtuel d'organisation avec un routage de type « entre VDC » est créé pour chaque centre de données virtuel participant. Vous pouvez afficher les réseaux nouvellement créés dans la vue **Centres de données** des centres de données virtuels participants en cliquant sur **Réseaux**. Si une machine virtuelle ou un vApp se connecte à un réseau de centre de données virtuel d'organisation de ce type, cette machine virtuelle ou ce vApp se connecte au réseau étiré.

Étape suivante

Vous pouvez attribuer des adresses IP statiques et des pools d'adresses IP à chaque réseau de centre de données virtuel d'organisation entre VDC. Reportez-vous à Ajouter des adresses IP à un pool d'adresses IP de réseau de centre de données virtuel d'organisation.

Pour les configurations DNS et DHCP pour les machines virtuelles attachées à un réseau étiré, vous pouvez utiliser l'OpenAPI vCloud. Pour examiner la documentation sur l'OpenAPI vCloud, accédez à `https://vCloud_Director_IP_address_or_host_name/docs`. Pour afficher des exemples de code et tester les appels de l'OpenAPI vCloud, accédez à `https://vCloud_Director_IP_address_or_host_name/api-explorer?scope=organization_name`.

Afficher ou modifier un réseau étiré

Vous pouvez afficher le nom, la description et les paramètres CIDR d'un réseau étiré. Vous pouvez uniquement modifier le nom et la description d'un réseau étiré.

Pour plus d'informations sur la modification de l'allocation de pool d'adresses IP statiques pour un réseau étiré au niveau du centre de données virtuel, reportez-vous à la section Ajouter des adresses IP à un pool d'adresses IP de réseau de centre de données virtuel d'organisation.

Conditions préalables

- Pour afficher des réseaux étirés, vous devez disposer du rôle prédéfini **Administrateur d'organisation** ou d'un rôle doté du droit **Réseau VDC d'organisation : Afficher les propriétés**.
- Pour modifier des réseaux étirés, il faut disposer du rôle prédéfini **Administrateur d'organisation** ou d'un rôle doté du droit **Réseau VDC d'organisation : Modifier les propriétés**.

Procédure

1. Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2. Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Dans le panneau de gauche, cliquez sur **Réseaux étirés**.

   La liste des réseaux étirés s'affiche dans une vue de grille.

4 Cliquez sur le bouton radio en regard du nom du réseau cible, puis cliquez sur **Modifier**.

5 Modifiez les détails du réseau, puis cliquez sur **Enregistrer**.

Supprimer un réseau étiré

Vous pouvez supprimer un réseau étiré qui n'est plus utilisé.

Conditions préalables

- Cette opération nécessite le rôle prédéfini **Administrateur d'organisation** ou un rôle disposant du droit **Réseau de VDC d'organisation : Modifier les propriétés**.
- Les réseaux de centre de données virtuel d'organisation correspondants ne doivent pas être connectés à aucune machine virtuelle ou vApp.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Dans le panneau de gauche, cliquez sur **Réseaux étirés**.

   La liste des réseaux étirés s'affiche dans une vue de grille.

4 Cliquez sur le bouton radio en regard du nom du réseau cible, puis cliquez sur **Supprimer**.

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

Résultats

Les réseaux de centre de données virtuel d'organisation correspondants sont supprimés de tous les centres de données virtuels concernés.

Synchroniser un réseau étiré

Pour vous assurer que tous les centres de données virtuels participants peuvent accéder à leur réseau étiré, vous pouvez synchroniser le réseau étiré.

Conditions préalables

Cette opération nécessite le rôle prédéfini **Administrateur d'organisation** ou un rôle disposant du droit **Réseau de VDC d'organisation : Modifier les propriétés**.

Procédure

1 Dans le menu principal (☰), sélectionnez **Groupes de centres de données**.

   La liste des groupes de centres de données s'affiche dans une vue de carte.

2 Dans la carte du groupe de centres de données cible, cliquez sur **Détails**.

   Vous êtes redirigé vers la vue **Topologie réseau** pour ce groupe de centres de données. Vous pouvez afficher un diagramme de la topologie réseau actuelle, qui décrit les centres de données virtuels appartenant au groupe avec leurs domaines d'erreur de réseau, les points de sortie configurés, le cas échéant, et les routes de trafic.

3 Dans le panneau de gauche, cliquez sur **Réseaux étirés**.

   La liste des réseaux étirés s'affiche dans une vue de grille.

4 Cliquez sur la case d'option en regard du nom du réseau cible, puis sur **Synchroniser**.

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

Capacités de mise en réseau avancées pour les locataires vCloud Director

6

vCloud Director fournit des capacités de mise en réseau avancées grâce au logiciel de virtualisation du réseau NSX, qui offrent des contrôles de sécurité améliorés et des capacités de routage et d'évolution du réseau dans un environnement de cloud.

À l'aide de ces fonctionnalités de mise en réseau, vous pouvez obtenir une sécurité et une isolation jamais atteintes dans votre centre de données virtuel d'organisation. Ces capacités offrent les avantages suivants :

- Routage dynamique. Les capacités de NSX dans votre environnement vCloud Director prennent en charge des protocoles de routage tels que les protocoles BGP (Border Gateway Protocol) et OSPF (Open Shortest Path First) pour simplifier l'intégration réseau entre les systèmes, afin de garantir la redondance et la continuité dans le déploiement d'applications hébergées dans le cloud.
- Isolation et sécurité accrues du réseau. Les capacités de NSX dans votre environnement vCloud Director prennent en charge l'utilisation de définitions de règle basées sur un objet pour fournir une isolation du trafic réseau avec état sans recourir à plusieurs réseaux virtuels. Ce modèle de sécurité sans approbation préalable empêche les intrus d'obtenir d'un accès réseau complet si une application ou une machine virtuelle est compromise. La configuration du réseau est simplifiée en utilisant les mêmes stratégies de sécurité réseau afin de protéger les applications lorsqu'elles sont physiquement situées dans l'environnement vCloud Director et d'étendre votre modèle de sécurité sans approbation préalable vers une sécurité portable, quel que soit l'emplacement depuis lequel l'application est déployée.
- Les capacités supplémentaires offertes par NSX sont une prise en charge étendue du VPN pour la connectivité point à site (VPN IPsec) et utilisateur (VPN-Plus SSL), un équilibrage de charge amélioré pour HTTPS et une évolutivité du réseau étendue.

Vous pouvez configurer deux types de pare-feu : le pare-feu de passerelle Edge et le pare-feu distribué. Pour plus d'informations sur les différences entre ces pare-feu, reportez-vous à la rubrique Configuration du pare-feu à l'aide du portail de locataires.

Vous pouvez accéder à ces fonctionnalités de mise en réseau avancées à l'aide du portail de locataires vCloud Director ou de vCloud Director Service Provider Admin Portal. La passerelle Edge doit d'abord être convertie en passerelle Edge avancée. Reportez-vous à la section Convertir une passerelle Edge en passerelle Edge avancée.

Important Les passerelles Edge IPv6 prennent en charge des services limités. Les passerelles Edge IPv6 prennent en charge des pare-feu Edge, des pare-feu distribués et le routage statique.

Ce chapitre contient les rubriques suivantes :

- Démarrage de la mise en réseau avancée de vCloud Director
- Configuration du pare-feu à l'aide du portail de locataires
- Gestion du protocole DHCP de la passerelle Edge
- Gestion de la traduction d'adresses réseau à l'aide du portail de locataires
- Configuration de routage avancée
- Équilibrage de charge
- Sécuriser l'accès à l'aide de réseaux privés virtuels
- Gestion des certificats SSL
- Personnaliser le regroupement d'objets
- Statistiques et journaux pour une passerelle Edge
- Activer l'accès de ligne de commande SSH à une passerelle Edge
- Utilisation des balises de sécurité
- Utilisation des groupes de sécurité

Démarrage de la mise en réseau avancée de vCloud Director

La mise en réseau avancée de vCloud Director permet d'effectuer des tâches de gestion pour une organisation dans un système vCloud Director. Vous pouvez gérer les pare-feu distribués et les autres capacités de réseau avancées fournies par les composants logiciels NSX® VMware mis à disposition d'une organisation par un administrateur système vCloud Director.

La mise en réseau avancée est généralement utilisée par les utilisateurs suivants :

- Les **administrateurs système** vCloud Director, qui peuvent utiliser le portail de locataires pour configurer le pare-feu distribué et d'autres capacités de mise en réseau avancées pour une organisation.
- Les **administrateurs d'organisation**, qui utilisent le portail de locataires pour gérer le pare-feu distribué et d'autres capacités de mise en réseau avancées que l'**administrateur système** a rendues disponibles pour l'organisation.

Configuration du pare-feu à l'aide du portail de locataires

Le portail de locataires vous permet de configurer les fonctionnalités de pare-feu fournies par le logiciel NSX dans votre centre de données virtuel d'organisation vCloud Director. Vous pouvez créer des règles de pare-feu pour des pare-feux distribués afin de mettre en œuvre une sécurité entre machines virtuelles dans un centre de données virtuel d'organisation et des règles de pare-feu à appliquer à un pare-feu de passerelle Edge pour protéger les machines virtuelles dans un centre de données virtuel d'organisation depuis le trafic réseau externe.

Note Le portail de locataires permet de configurer des pare-feux de passerelle Edge et des pare-feux distribués.

La technologie de pare-feu logique NSX est formée de deux composants pour traiter différents cas d'utilisation de déploiement. Le pare-feu de passerelle Edge met l'accent sur l'application du trafic vertical, alors que le pare-feu distribué se concentre sur les contrôles d'accès horizontaux.

Différences clés entre des pare-feux de passerelle Edge et des pare-feux distribués

Un pare-feu de passerelle Edge surveille le trafic vertical afin de mettre en œuvre la fonctionnalité de sécurité de périmètre incluant le pare-feu, la traduction d'adresse réseau (NAT) ainsi que la fonctionnalité IPSec et SSL VPN site à site.

Un pare-feu distribué permet d'isoler et de sécuriser chaque machine virtuelle et chaque application jusqu'au niveau de couche 2 (L2). La configuration des pare-feux distribués met en quarantaine n'importe quel risque de sécurité réseau externe ou interne, isolant le trafic horizontal entre les machines virtuelles sur le même segment réseau. Les stratégies de sécurité sont gérées centralement et peuvent être héritées et imbriquées, afin que les administrateurs réseau et de sécurité puissent les gérer à grande échelle. En outre, une fois déployées, les stratégies de sécurité définies suivent les machines virtuelles ou les applications lorsqu'elles se déplacent entre différents centres de données virtuels.

À propos des règles de pare-feu

Comme décrit dans la documentation du produit NSX, dans NSX, les règles de pare-feu définies au niveau central sont appelées règles préalables. Vous pouvez également ajouter des règles à un niveau de passerelle Edge individuel, ces règles sont alors appelées règles locales.

Chaque session de trafic est comparée à la règle du tableau de pare-feu supérieure avant d'être comparée aux règles suivantes dans le tableau. La première règle du tableau correspondant aux paramètres du trafic est appliquée. Les règles sont affichées dans l'ordre suivant :

1. Les règles préalables définies par l'utilisateur ont la priorité la plus élevée et sont appliquées dans un ordre de haut en bas avec une préséance par niveau de carte réseau virtuelle.
2. Règles à vérification automatique (règles permettant le passage du trafic de contrôle des services de passerelle Edge).
3. Règles locales définies au niveau de la passerelle Edge.

4 Règle de pare-feu distribué par défaut.

Pour plus d'informations sur la façon dont le logiciel NSX applique les règles de pare-feu, reportez-vous à la section *Modifier l'ordre d'une règle de pare-feu* dans la documentation d'*administration de NSX*.

Pare-feu de passerelle Edge

Le pare-feu pour la passerelle Edge vous aide à répondre aux exigences de sécurité de périmètre clés, telles que la création de zones démilitarisées basée sur des structures IP/VLAN, une isolation locataire à locataire dans des centres de données virtuels à plusieurs locataires, la traduction d'adresse réseau (NAT), des VPN de partenaires (extranet) et des SSL VPN basés sur des utilisateurs.

La fonctionnalité de pare-feu de passerelle Edge dans l'environnement vCloud Director est fournie par le logiciel NSX. Dans NSX, cette fonctionnalité de pare-feu est également appelée pare-feu Edge. Le pare-feu de passerelle Edge surveille le trafic vertical pour mettre en œuvre une fonctionnalité de sécurité de périmètre incluant un pare-feu, la traduction d'adresse réseau (NAT) ainsi que la fonctionnalité IPSec et SSL VPN site à site.

Pour obtenir des informations détaillées sur les fonctionnalités offertes par le pare-feu de passerelle Edge du logiciel NSX, consultez la documentation d'*administration de NSX*.

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 des règles de pare-feu distribué à l'aide du portail de locataires.

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.

Convertir une passerelle Edge en passerelle Edge avancée

Pour utiliser une passerelle Edge dans le portail de locataires, vous devez la convertir en passerelle Edge avancée. Après la conversion en passerelle Edge avancée, vous pouvez utiliser le portail de locataires pour configurer les fonctionnalités de routage statique et dynamique qui sont fournies par le logiciel NSX pour ces passerelles Edge avancées.

Conditions préalables

Vous avez une passerelle Edge existante.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et sélectionnez **Dispositifs Edge** dans le panneau de gauche.
2. Sélectionnez la passerelle Edge à modifier.
3. Cliquez sur **Convertir en passerelle avancée**.

Résultats

Votre passerelle Edge est convertie en passerelle Edge avancée.

Étape suivante

Après la conversion en passerelle Edge avancée, vous pouvez configurer ses paramètres en sélectionnant la passerelle et en cliquant sur **Services**.

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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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**.

Pare-feu distribué

Le pare-feu distribué vous permet de segmenter des entités de centre de données virtuel d'organisation, tels que des machines virtuelles, en fonction de noms de machine virtuelle et d'attributs.

vCloud Director prend en charge les services Distributed Firewall sur les centres de données virtuels d'organisation reposant sur NSX Data Center for vSphere. Comme décrit dans la documentation d'*administration de NSX*, ce pare-feu distribué est un pare-feu hyperviseur intégré dans le noyau qui fournit une visibilité et un contrôle pour les charges de travail et les réseaux virtualisés. Vous pouvez créer des stratégies de contrôle d'accès basées sur des objets comme des noms de machine virtuelle et des structures réseau comme des adresses IP ou des adresses IP définies. Les règles de pare-feu sont appliquées au niveau de la vNIC de chaque

machine virtuelle pour mettre en œuvre un contrôle d'accès cohérent, même lorsque la machine virtuelle est déplacée vers un nouvel hôte ESXi par vSphere vMotion. Ce pare-feu distribué prend en charge un modèle de sécurité grâce à une microsegmentation dans laquelle le trafic horizontal peut être inspecté à une vitesse de traitement proche de la vitesse de ligne.

Comme décrit dans la documentation d'*administration de NSX*, pour les paquets de couche 2 (L2), le pare-feu distribué crée un cache afin d'accélérer les performances. Les paquets de la couche 3 (L3) sont traités dans l'ordre suivant :

1 Tous les paquets sont vérifiés pour un état existant.

2 Lorsqu'une correspondance d'état est trouvée, les paquets sont traités.

3 Lorsqu'une correspondance d'état est introuvable, les paquets sont traités en suivant les règles jusqu'à ce qu'une correspondance soit trouvée.

- Pour les paquets TCP, un état est défini uniquement pour les paquets comportant un indicateur SYN. Cependant, les règles qui ne spécifient pas de protocole (service ANY), peuvent faire correspondre les paquets TCP à n'importe quelle combinaison d'indicateurs.
- Pour les paquets UDP, des détails quintuples sont extraits du paquet. Lorsqu'un état n'existe pas dans la table des états, un nouvel état est créé à l'aide des détails quintuples extraits. Les paquets reçus par la suite sont comparés à l'état qui vient d'être créé.
- Pour les paquets ICMP, le type ICMP, le code et la direction du paquet sont utilisés pour créer un état.

Le pare-feu distribué permet de créer également des règles basées sur l'identité. Les administrateurs peuvent appliquer le contrôle d'accès basé sur l'appartenance au groupe de l'utilisateur telle que définie dans l'annuaire Active Directory (AD) de l'entreprise. Cas d'utilisation pour lesquels vous pouvez utiliser des règles de pare-feu basées sur l'identité :

- Utilisateurs accédant aux applications virtuelles à l'aide d'un ordinateur portable ou d'un appareil mobile où AD est utilisé pour l'authentification des utilisateurs
- Utilisateurs accédant à des applications virtuelles à l'aide d'une infrastructure VDI dans laquelle les machines virtuelles sont basées sur Microsoft Windows

Pour obtenir des informations détaillées sur les fonctionnalités offertes par le pare-feu distribué du logiciel NSX, consultez la documentation d'*administration de NSX* .

Activer le pare-feu distribué sur le centre de données virtuel d'une organisation à l'aide du portail de locataires

Avant que vous puissiez utiliser le portail de locataires pour exploiter les capacités de pare-feu distribué sur un centre de données virtuel d'organisation, le pare-feu distribué doit être activé pour ce centre de données virtuel d'organisation. Un administrateur système vCloud Director ou un utilisateur disposant du droit ORG_VDC_DISTRIBUTED_FIREWALL_ENABLE peut activer le pare-feu distribué sur un centre de données virtuel d'organisation.

L'écran de pare-feu distribué du portail de locataires permet d'activer le pare-feu distribué d'un centre de données virtuel d'organisation.

Conditions préalables

Vérifiez que l'organisation à laquelle appartient le centre de données virtuel d'organisation dispose des droits suivants :

- Pare-feu distribué vDC d'organisation : Activer/Désactiver
- Pare-feu distribué vDC d'organisation : Configurer les règles
- Pare-feu distribué vDC d'organisation : Afficher les règles

L'administrateur système vCloud Director attribue des droits à une organisation. Le droit Pare-feu distribué vDC d'organisation : Activer/Désactiver est requis pour activer le pare-feu distribué à l'aide de l'interface utilisateur du portail de locataires. Le droit Pare-feu distribué vDC d'organisation : Afficher les règles est requis pour afficher les règles de pare-feu dans le portail de locataires ; le droit Pare-feu distribué vDC d'organisation : Configurer les règles, quant à lui, est requis pour configurer les règles de pare-feu à l'aide du portail de locataires.

Assurez-vous que vous disposez d'un rôle qui vous accorde le droit appelé Pare-feu distribué vDC d'organisation : Activer/Désactiver. Parmi les rôles prédéfinis dans un système vCloud Director, seul le rôle d'administrateur système dispose de ce droit par défaut.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez le centre de données virtuel d'organisation pour lequel vous souhaitez configurer des règles de pare-feu distribué.
3. Cliquez sur **Configurer des services**.
4. Activez le pare-feu distribué dans l'onglet **Distributed Firewall**.

Étape suivante

Pour une description de la règle de pare-feu distribué par défaut, reportez-vous à la section Gestion des règles de pare-feu distribué à l'aide du portail de locataires.

Gestion des règles de pare-feu distribué à l'aide du portail de locataires

Comme décrit dans le *Guide d'administration de NSX*, les paramètres de pare-feu par défaut s'appliquent au trafic qui ne correspond pas aux règles de pare-feu définies par l'utilisateur. Dans le vCloud Director Tenant Portal, la règle de pare-feu distribué par défaut est étiquetée Règle d'autorisation par défaut.

La fonctionnalité de pare-feu distribué doit être activée sur un centre de données virtuel d'organisation avant que vous puissiez gérer les paramètres de pare-feu distribué à l'aide du vCloud Director Tenant Portal.

La règle de pare-feu distribué par défaut est configurée pour autoriser tout le trafic de couche 3 et de couche 2 à passer par le centre de données virtuel d'organisation. Ce paramètre est indiqué par l'option Autoriser définie dans la colonne Action de l'interface utilisateur. La règle par défaut se situe toujours en bas du tableau de règles.

Important Vous ne pouvez pas supprimer ou modifier les règles de pare-feu distribué 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 sur le centre de données virtuel d'une organisation à l'aide du portail de locataires
- 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez le réseau VDC de services de sécurité pour lequel vous souhaitez modifier les règles de pare-feu, puis cliquez sur **Configurer des services**.

   L'écran Services de sécurité s'affiche.
3. 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**.

4 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.

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

6 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**

7 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**

8 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**.

9 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.

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

11 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**.

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

   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.

   Important Les groupes d'adresses IP (ensembles d'adresses IP), les groupes d'adresses MAC (ensembles d'adresses Mac) et les groupes de sécurité contenant des ensembles d'adresses IP ou des ensembles d'adresses MAC ne sont pas des paramètres d'entrée valides.

13 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.

2 Sélectionnez le réseau VDC de services de sécurité pour lequel vous souhaitez modifier les règles de pare-feu, puis cliquez sur **Configurer des services**.

   L'écran Services de sécurité s'affiche.

3 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.

4 Cliquez sur **Enregistrer les modifications**.

Gestion du protocole DHCP de la passerelle Edge

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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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.
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.

Option	Description
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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

b Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

Option	Description
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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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**.

Gestion de la traduction d'adresses réseau à l'aide du portail de locataires

Le logiciel NSX dans votre environnement vCloud Director permet aux passerelles Edge de fournir un service de traduction d'adresses réseau (NAT). Cette capacité permet de limiter le nombre d'adresses IP publiques qu'une organisation doit utiliser pour des raisons économiques et de sécurité.

Le service NAT d'une passerelle Edge permet d'attribuer une adresse publique à une machine virtuelle ou à un groupe de machines virtuelles dans un réseau privé. Pour permettre à vos passerelles Edge de fournir l'accès aux services exécutés sur des machines virtuelles à adressage privé dans votre centre de données virtuel d'organisation, vous devez configurer des règles NAT sur les passerelles Edge. Dans la plupart des cas, vous associez un service NAT à une interface de liaison montante sur une passerelle Edge dans votre environnement vCloud Director afin que les adresses sur les réseaux de centre de données virtuel d'organisation ne soient pas exposées sur le réseau externe.

La configuration du service NAT est séparée dans les règles de NAT source (SNAT) et de 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 centre de données virtuel d'organisation. Plus précisément, cela signifie que vous configurez les règles de la manière suivante :

- SNAT : le trafic se déplace d'une machine virtuelle sur un réseau interne dans votre centre de données virtuel d'organisation (la source) via Internet vers le réseau externe (la destination). Une règle SNAT traduit l'adresse IP source des paquets sortants d'un réseau de centre de données virtuel d'organisation qui sont envoyés à un réseau externe ou à un autre réseau de centre de données virtuel d'organisation.

- DNAT : le trafic se déplace d'Internet (la source) vers une machine virtuelle à l'intérieur de votre centre de données virtuel d'organisation (la destination). 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.

Vous pouvez configurer les règles NAT pour créer un espace d'adressage IP privé à l'intérieur de votre centre de données virtuel d'organisation. Cette configuration offre la possibilité de porter un espace d'adressage IP privé d'un centre de données virtuel d'organisation vers un autre. La configuration des règles NAT vous permet d'utiliser les mêmes adresses IP privées pour vos machines virtuelles dans un centre de données virtuel d'organisation que celles qui ont été utilisées dans un autre.

La fonctionnalité de règle NAT dans votre environnement vCloud Director prend en charge les opérations suivantes :

- Création de sous-réseaux au sein de l'espace d'adressage IP privé
- Création de plusieurs espaces d'adressage IP privés pour une passerelle Edge
- Configuration de plusieurs règles NAT sur plusieurs interfaces de passerelle Edge

Important Vous devez configurer des règles de pare-feu et NAT sur une passerelle Edge pour que les machines virtuelles sur un réseau de passerelle Edge soient accessibles. Par défaut, les passerelles Edge sont déployées avec des règles de pare-feu configurées pour refuser tout le trafic réseau vers et depuis les machines virtuelles sur les réseaux de passerelle Edge. En outre, la fonctionnalité NAT est désactivée par défaut sur les passerelles Edge afin que celles-ci ne parviennent pas à traduire les adresses IP du trafic entrant et sortant, sauf si vous configurez cette fonctionnalité sur les passerelles Edge. Toute tentative d'exécution d'une commande ping vers une machine virtuelle sur un réseau après la configuration d'une règle NAT échoue, sauf si vous ajoutez une règle de pare-feu pour autoriser le trafic correspondant.

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

Option	Description
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 et une réduction des temps de réponse, et il permet d'éviter la surcharge.

À propos de l'équilibrage de charge

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 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 déjà 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

b Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

b Sélectionnez la passerelle Edge à modifier, puis cliquez 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 6-1. 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 6-2. 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 6-3. 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

b Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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. 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 SSL VPN-Plus d'une passerelle Edge dans un environnement vCloud Director permettent aux utilisateurs distants de se connecter en toute sécurité aux réseaux privés et applications des centres de données virtuels d'organisation soutenus par 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, 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 SSL VPN-Plus sur une passerelle Edge

   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 SSL VPN-Plus sur une passerelle Edge

   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 SSL VPN-Plus sur une passerelle Edge

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 pour le service VPN SSL de la passerelle Edge.

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 SSL VPN-Plus généraux pour une passerelle Edge

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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

b Sélectionnez la passerelle Edge à modifier, puis cliquez 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 SSL VPN-Plus généraux pour une passerelle Edge.

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, 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 SSL VPN-Plus sur une passerelle Edge.

Créer un pool d'adresses IP utilisable avec SSL VPN-Plus sur une passerelle Edge

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 SSL VPN-Plus sur une passerelle Edge.

Ajouter un réseau privé pour une utilisation avec SSL VPN-Plus sur une passerelle Edge

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 SSL VPN-Plus sur une passerelle Edge.

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.

Option	Action
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 SSL VPN-Plus sur une passerelle Edge.

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 SSL VPN-Plus sur une passerelle Edge

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 SSL VPN-Plus 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 SSL VPN-Plus sur une passerelle Edge.
- 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 pour le service VPN SSL de la passerelle Edge.

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 SSL VPN-Plus sur une passerelle Edge.

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 SSL VPN-Plus à la passerelle Edge. 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 SSL VPN-Plus généraux pour une passerelle Edge

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

   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

   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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

Configurer les connexions de site VPN IPSec pour la passerelle Edge

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. Ouvrez les services de passerelle Edge.
   a. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Services**.
2. Sous l'onglet **VPN IPsec**, cliquez sur **Sites VPN IPsec**.
3. Cliquez sur le bouton **Ajouter** ( ).
4. 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.

5 Cliquez sur **Conserver**.

6 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.

Activer le service VPN IPsec sur une passerelle Edge

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.

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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 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.

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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Services**.

2 Accédez à **VPN > VPN L2**.

Étape suivante

Configurez le serveur VPN L2. Reportez-vous à Configurer la passerelle Edge en tant que serveur VPN L2.

Configurer la passerelle Edge 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.
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.

Configurer la passerelle Edge 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.
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.

Activer le service VPN L2 sur une passerelle Edge

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 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 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

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

Option	Description
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.
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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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** du portail de locataires vCloud Director. La page **Regroupement d'objets** est disponible à la fois dans les écrans Services et Passerelle Edge.

Procédure

1 Ouvrez la page Regroupement des objets.

Option	Action
Ouverture via les services de passerelle Edge	a Accédez à **Mise en réseau > Dispositifs Edge**. b Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des objets**.
Ouverture via les services de sécurité	a Accédez à **Mise en réseau > Sécurité**. b Sélectionnez le service de sécurité à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des 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 (Facultatif) Si vous spécifiez l'ensemble d'adresses IP depuis la page **Regroupement d'objets** de l'écran Services, utilisez le bouton bascule **Héritage** afin d'activer l'héritage et autoriser la visibilité des étendues sous-jacentes.

L'héritage est activé par défaut.

6 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.

Créez un ensemble d'adresses MAC à l'aide de la page **Regroupement d'objets** du portail de locataires vCloud Director. La page Regroupement d'objets est disponible à la fois dans les écrans **Services** et **Passerelle Edge**.

Procédure

1 Ouvrez la page Regroupement des objets.

Option	Action
Ouverture via les services de passerelle Edge	a Accédez à **Mise en réseau > Dispositifs Edge**. b Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des objets**.
Ouverture via les services de sécurité	a Accédez à **Mise en réseau > Sécurité**. b Sélectionnez le service de sécurité à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des 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 (Facultatif) Si vous spécifiez l'ensemble d'adresses MAC depuis la page **Regroupement d'objets** de l'écran **Services**, utilisez le bouton bascule **Héritage** afin d'activer l'héritage et d'autoriser la visibilité des étendues sous-jacentes.

L'héritage est activé par défaut.

6 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 du portail de locataires vCloud Director. La page Regroupement d'objets est disponible à la fois dans les écrans Services et Passerelle Edge.

Vous ne pouvez pas ajouter de nouveaux services à la liste à l'aide du portail de locataires. L'ensemble des services à votre disposition est géré par votre administrateur système vCloud Director.

Procédure

1 Ouvrez la page Regroupement des objets.

Option	Action
Ouverture via les services de passerelle Edge	a Accédez à **Mise en réseau > Dispositifs Edge**. b Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des objets**.
Ouverture via les services de sécurité	a Accédez à **Mise en réseau > Sécurité**. b Sélectionnez le service de sécurité à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des 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 du portail de locataires vCloud Director. La page Regroupement d'objets est disponible à la fois dans les écrans Services et Passerelle Edge.

Vous ne pouvez pas créer de groupes de services à l'aide du portail de locataires. L'ensemble des groupes de services à votre disposition est géré par votre administrateur système vCloud Director.

Procédure

1 Ouvrez la page Regroupement des objets.

Option	Action
Ouverture via les services de passerelle Edge	a Accédez à **Mise en réseau > Dispositifs Edge**. b Sélectionnez la passerelle Edge à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des objets**.
Ouverture via les services de sécurité	a Accédez à **Mise en réseau > Sécurité**. b Sélectionnez le service de sécurité à modifier, puis cliquez sur **Configurer les services**. c Cliquez sur **Regroupement des 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.

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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

   b Sélectionnez la passerelle Edge à modifier, puis cliquez 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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
   b. Sélectionnez la passerelle Edge à modifier, puis cliquez 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.

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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez un service de sécurité, puis cliquez sur **Configurer les services**.
3. Cliquez sur l'onglet **Balises de sécurité**.
4. Cliquez sur le bouton **Créer** ( ) et entrez un nom pour la balise de sécurité.
5. (Facultatif) Entrez une description pour la balise de sécurité.
6. (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.
7. 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez un service de sécurité, puis cliquez sur **Configurer les services**.
3. Cliquez sur l'onglet **Balises de sécurité**.
4. Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez modifier, puis cliquez sur le bouton **Modifier** ( ).
5. 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.
6. 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.
7. 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez un service de sécurité, puis cliquez sur **Configurer les services**.
3. 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**.
4. 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.
2. Sélectionnez un service de sécurité, puis cliquez sur **Configurer les services**.
3. Cliquez sur l'onglet **Balises de sécurité**.
4. Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez modifier.
5. Cliquez sur le bouton **Modifier** ( ).
6. Modifiez le nom et la description de la balise de sécurité.
7. Attribuez la balise aux machines virtuelles que vous sélectionnez ou supprimez l'attribution.
8. 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 l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Mise en réseau**, sélectionnez **Sécurité**.

2 Sélectionnez un service de sécurité, puis cliquez sur **Configurer les services**.

3 Cliquez sur l'onglet **Balises de sécurité**.

4 Dans la liste des balises de sécurité, sélectionnez la balise de sécurité que vous souhaitez supprimer.

5 Cliquez sur le bouton **Supprimer** ( ).

6 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.

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 Ouvrez les services de sécurité.

   a Accédez à **Mise en réseau > Sécurité**.

   b Sélectionnez le VDC d'organisation auquel vous souhaitez appliquer les paramètres de sécurité, puis cliquez sur **Configurer des services**.

   Le portail de locataires ouvre les services de sécurité.

2 Accédez à **Regroupement des objets > Groupes de sécurité**.

   La page **Groupes de sécurité** s'ouvre.

3 Cliquez sur le bouton **Créer** ( ).

4 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.

5 (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**.

6 (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.

7 (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.

8 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 Ouvrez les services de sécurité.

a Accédez à **Mise en réseau > Sécurité**.

b Sélectionnez le VDC d'organisation auquel vous souhaitez appliquer les paramètres de sécurité, puis cliquez sur **Configurer des services**.

Le portail de locataires ouvre les services de sécurité.

2 Accédez à **Regroupement des objets > Groupes de sécurité**.

La page **Groupes de sécurité** s'ouvre.

3 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.

4 (Facultatif) Modifiez le nom et la description du groupe de sécurité.

5 (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**.

6 (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**.

7 (Facultatif) Supprimez un ensemble de membres dynamiques en cliquant sur l'icône **Supprimer** (✖) en regard de l'ensemble de membres que vous souhaitez supprimer.

8 (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.

9 (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.

10 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. Ouvrez les services de sécurité.
   a. Accédez à **Mise en réseau > Sécurité**.
   b. Sélectionnez le VDC d'organisation auquel vous souhaitez appliquer les paramètres de sécurité, puis cliquez sur **Configurer des services**.

      Le portail de locataires ouvre les services de sécurité.
2. Accédez à **Regroupement des objets > Groupes de sécurité**.

   La page **Groupes de sécurité** s'ouvre.
3. Sélectionnez le groupe de sécurité que vous souhaitez supprimer.
4. Cliquez sur le bouton **Supprimer** ( ).
5. Pour confirmer la suppression, cliquez sur **OK**.

Résultats

Le groupe de sécurité est supprimé.

Gestion de passerelles Edge NSX-T Data Center 7

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 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
- Créer des profils de port d'application personnalisés

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
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 à partir de 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 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.
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 Accédez à **Mise en réseau** > **Dispositifs Edge**.

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.

Option	Description
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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
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**.

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. Accédez à **Mise en réseau** > **Dispositifs Edge**.
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.

Utilisation de disques nommés et vérification des stratégies de stockage

8

Vous pouvez créer et gérer des disques nommés et passer en revue les stratégies de stockage de centre de données virtuel d'organisation à l'aide du portail de locataires vCloud Director.

Ce chapitre contient les rubriques suivantes :

- Création et utilisation des disques nommés
- Vérifier les propriétés de la stratégie de stockage

Création et utilisation des disques nommés

Les disques nommés sont des disques virtuels autonomes que vous créez dans les VDC d'organisation. Les **administrateurs d'organisation** et les utilisateurs qui disposent des droits concernés peuvent créer, supprimer et mettre à jour des disques nommés, et les connecter à des machines virtuelles.

Lorsque vous créez un disque nommé, il est associé à un VDC d'organisation, mais pas à une machine virtuelle. Après avoir créé le disque dans un VDC, le propriétaire du disque ou un administrateur peut l'attacher à toute machine virtuelle déployée dans le VDC. Le propriétaire du disque peut également modifier les propriétés du disque, le détacher d'une machine virtuelle et le supprimer du VDC. Les **administrateurs système** et les **administrateurs d'organisation** disposent des mêmes droits pour utiliser et modifier le disque que le propriétaire du disque.

Créer un disque nommé

Vous pouvez créer un disque nommé et l'attacher à une machine virtuelle ultérieurement.

Pour créer un disque nommé, vous devez spécifier son nom et la taille. Vous pouvez éventuellement inclure une description et sélectionner un profil de stockage à utiliser par le disque.

Conditions préalables

Vous devez disposer des droits du rôle **Administrateur d'organisation** ou des droits du propriétaire du disque.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Stockage**, sélectionnez **Disques nommés** dans le panneau de gauche.
2. Cliquez sur **Nouveau**.
3. Entrez le nom et la description (facultative) du disque.
4. Sélectionnez la stratégie de stockage dans le menu déroulant **Stratégie de stockage**.
5. Entrez la taille du disque nommé en octets.
6. Sélectionnez le type de bus et le sous-type de bus, dans les menus déroulants **Type de bus** et **Sous-type de bus** respectivement, puis cliquez sur **Enregistrer**.

Étape suivante

Utilisez l'API vCloud pour attacher le disque indépendant à une machine virtuelle. Consultez *Guide de programmation de vCloud API pour fournisseurs de services* sur VMware {code}.

Modifier un disque nommé

Une fois que vous avez créé le disque, vous pouvez modifier son nom, sa description, sa stratégie de stockage et sa taille.

Conditions préalables

Vous devez disposer des droits du rôle **Administrateur d'organisation** ou des droits du propriétaire du disque.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Stockage**, sélectionnez **Disques nommés** dans le panneau de gauche.
2. Sélectionnez le disque que vous souhaitez modifier, puis cliquez sur **Modifier**.
3. Modifiez les paramètres tels que le nom, la description, la stratégie de stockage et la taille en octets.
4. Cliquez sur **Enregistrer**.

Associer un disque nommé à une machine virtuelle

Après avoir créé un disque nommé dans un VDC, vous pouvez l'associer à n'importe quelle machine virtuelle déployée dans le VDC.

Conditions préalables

Vous devez disposer des droits du rôle **Administrateur d'organisation** ou des droits du propriétaire du disque.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Stockage**, sélectionnez **Disques nommés** dans le panneau de gauche.
2. Cliquez sur la case d'option en regard du nom du disque nommé que vous souhaitez associer à une machine virtuelle, puis cliquez sur **Associer**.
3. Dans le menu déroulant, sélectionnez une machine virtuelle à laquelle associer le disque nommé et cliquez sur **Appliquer**.

Résultats

Le disque nommé est associé à la machine virtuelle.

Étape suivante

Vous pouvez associer d'autres disques nommés à la machine virtuelle ou les dissocier si nécessaire.

Supprimer un disque nommé

Si vous n'avez pas besoin d'un disque nommé, vous pouvez le supprimer.

Conditions préalables

Vous devez disposer des droits du rôle **Administrateur d'organisation** ou des droits du propriétaire du disque.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer et, sous **Stockage**, sélectionnez **Disques nommés** dans le panneau de gauche.
2. Sélectionnez le disque que vous souhaitez supprimer, puis cliquez sur **Supprimer**.
3. Cliquez sur **OK**.

Vérifier les propriétés de la stratégie de stockage

Vous pouvez vérifier les stratégies de stockage et leurs détails.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer.

2 Sous **Stockage**, cliquez sur **Stratégies de stockage**.

   La liste des stratégies de stockage disponibles s'affiche.

3 Pour afficher les détails d'une stratégie de stockage, cliquez sur le nom correspondant.

4 Vérifiez les détails dans les onglets **Général** et **Métadonnées**, puis cliquez sur **OK**.

Vérification des propriétés du centre de données virtuel

9

En tant qu'**administrateur d'organisation**, vous pouvez vérifier les propriétés du centre de données virtuel.

Ce chapitre contient les rubriques suivantes :

- Vérifier les propriétés du centre de données virtuel
- Vérifier les métadonnées du centre de données virtuel

Vérifier les propriétés du centre de données virtuel

Vous pouvez vérifier les propriétés des centres de données virtuels attribués à votre organisation.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer.
2. Sous **Paramètres**, cliquez sur **Général**.

Résultats

Vous pouvez vérifier les propriétés du centre de données virtuel telles que son nom, sa description et son état. Les informations de mesures sur le centre de données incluent l'utilisation du modèle d'allocation, du vCPU, du CPU et de la mémoire.

Vérifier les métadonnées du centre de données virtuel

vCloud Director fournit un outil à usage général pour associer des métadonnées définies par l'utilisateur à un objet. Si votre administrateur système a créé les métadonnées du centre de données virtuel de l'organisation, vous pouvez les vérifier.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans l'écran du tableau de bord **Centres de données virtuels**, cliquez sur la carte du centre de données virtuel que vous souhaitez explorer.
2. Sous **Paramètres**, cliquez sur **Métadonnées**.

   La liste des métadonnées disponibles affiche.

Utilisation d'instances de vCenter Server dédiées et de proxys

10

À partir de vCloud Director 9.7, vous pouvez accéder à un environnement vCenter Server dédié depuis vCloud Director. vCloud Director peut agir comme serveur proxy HTTP et fournir un accès aux composants depuis l'environnement vSphere sous-jacent.

Dans vCloud Director, un SDDC (Software-Defined Data Center) encapsule l'intégralité d'un environnement vCenter Server dédié. Une instance de vCenter Server dédiée peut inclure un ou plusieurs proxys qui fournissent un accès à différents composants de l'environnement sous-jacent.

L'**administrateur système** peut publier une ou plusieurs instances de vCenter Serverdédiées vers votre organisation. Vous pouvez utiliser les proxys conteneurs pour accéder à l'interface utilisateur ou à l'API des composants proxy.

Ce chapitre contient les rubriques suivantes :

- Configurer votre navigateur avec vos paramètres de proxy
- Se connecter à l'interface utilisateur d'un composant proxy

Configurer votre navigateur avec vos paramètres de proxy

Avant de pouvoir accéder à l'interface utilisateur d'un composant vSphere proxy, vous devez configurer les proxys qui sont publiés dans votre organisation.

Pour configurer votre navigateur afin qu'il utilise vos serveurs proxy publiés, copiez l'URL du fichier de configuration automatique de serveur proxy (PAC) dans votre navigateur.

Note Lorsque l'**administrateur système** publie un centre de données vSphere dédié pour votre organisation, ou ajoute un serveur proxy à l'un de vos centres de données vSphere dédiés, le navigateur mettra quelques minutes à récupérer la configuration PAC depuis l'URL fournie. Pour forcer l'actualisation du navigateur, vous pouvez répéter cette procédure.

Conditions préalables

- Vérifiez que l'**administrateur système** a publié au moins une instance dédiée et activée de vCenter Server dans votre organisation.
- Vérifier que l'**administrateur système** a publié les droits **SDDC_VIEW** et **Jeton: Gérer** dans votre organisation et que vos rôles incluent ces droits.

- Vérifiez que l'**administrateur système** a publié et activé le plug-in **Extension CPOM** dans votre organisation. Ce plug-in fournit la fonction permettant d'afficher et d'utiliser des centres de données vSphere dédiés dans vCloud Director Tenant Portal.

Procédure

1. Dans le menu principal (☰), sélectionnez **Centres de données**.
2. Dans le volet **Centres de données vSphere dédiés**, cliquez sur **Cliquez ici pour afficher le Guide de configuration du proxy**.
3. Copiez l'URL du fichier PAC, puis cliquez sur **Suivant**.
4. Suivez les instructions pour configurer votre navigateur afin qu'il pointe vers l'URL du fichier PAC.
5. Si un composant proxy utilise des certificats auto-signés, importez-les dans votre navigateur.
   a. Sur la fiche du centre de données vSphere cible, cliquez sur **Actions**, puis sur **Importer le certificat**.
   b. Téléchargez le certificat et la liste de révocation des certificats (CRL).
   c. Importez le certificat téléchargé dans votre navigateur.

      Consultez les instructions de l'utilisateur de votre navigateur.

Se connecter à l'interface utilisateur d'un composant proxy

Vous pouvez accéder à l'interface utilisateur d'un composant proxy avec votre compte vCloud Director.

Conditions préalables

Avant de vous connecter à l'interface utilisateur d'un composant proxy, vous devez configurer votre accès au proxy. Reportez-vous à la section Configurer votre navigateur avec vos paramètres de proxy.

Procédure

1. Dans le menu principal (☰), sélectionnez **Centres de données**.
2. Cliquez sur l'onglet **Centres de données vSphere dédiés**.
3. Ouvrez le proxy de l'instance de vCenter Server dédiée.
   - Pour ouvrir le proxy par défaut, cliquez sur **Ouvrir vSphere**.
   - Pour ouvrir un proxy non défini par défaut, procédez comme suit :
     - Cliquez sur **Actions**, puis sur **Afficher les serveurs proxy**.
     - Cliquez sur l'URL du serveur proxy.

   Une nouvelle carte avec vos informations d'identification sur le proxy s'ouvre.

4 Copiez le nom d'utilisateur et le mot de passe.

5 Pour activer le proxy, cliquez sur **Ouvrir**.

   Une nouvelle carte s'ouvre et vous invite à vous authentifier par rapport au proxy.

6 Dans la zone de texte **Nom d'utilisateur**, collez le nom d'utilisateur copié.

7 Dans la zone de texte **Mot de passe**, collez le mot de passe copié et cliquez sur **OK**.

Résultats

L'interface utilisateur du composant proxy s'ouvre.

Utilisation des modèles de vApp 11

Un modèle de vApp est une image de machine virtuelle qui est chargée avec un système d'exploitation, des applications et des données. Ces modèles veillent à ce que les machines virtuelles soient configurées de manière homogène dans toute l'organisation. Les modèles de vApp sont ajoutés à des catalogues.

Ce chapitre contient les rubriques suivantes :

- Afficher un modèle de vApp
- Créer un modèle de vApp à partir d'un fichier OVF
- Attribuer une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle à un modèle de vApp
- Télécharger un modèle de vApp
- Supprimer un modèle de vApp

Afficher un modèle de vApp

Vous pouvez voir la liste des modèles de vApp qui sont disponibles dans les catalogues auxquels vous avez accès. Vous pouvez afficher un modèle de vApp et explorer les machines virtuelles qu'il contient.

Vous pouvez accéder uniquement aux modèles de vApp qui sont inclus dans les éléments de catalogues qui ont été partagés avec vous. Pour plus d'informations sur le partage de catalogues, reportez-vous à la section Partager un catalogue.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle d'**auteur de vApp** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 (Facultatif) Configurez la vue de grille pour qu'elle contienne les éléments que vous souhaitez afficher.

   a Dans la vue de grille, cliquez sur l'icône de l'éditeur de grille ( ) sous la liste des modèles de vApp.

   b Sélectionnez les éléments que vous souhaitez inclure dans la vue de grille tels que la version, l'état, le catalogue, le propriétaire, etc.

   c Cliquez sur **OK**.

   La grille affiche les éléments que vous avez sélectionnés pour chaque modèle de vApp dans la liste.

3 Cliquez sur le nom d'un modèle de vApp pour afficher les machines virtuelles qui y sont incluses.

   Les machines virtuelles incluses dans le modèle de vApp s'affichent dans une grille.

4 (Facultatif) Cliquez sur l'icône de l'éditeur de grille ( ) sous la liste des machines virtuelles pour sélectionner les éléments que vous souhaitez voir dans la vue de grille.

   a Sélectionnez les éléments que vous souhaitez inclure dans la vue de grille.

   b Cliquez sur **OK**.

Créer un modèle de vApp à partir d'un fichier OVF

Vous pouvez télécharger un module OVF pour créer un modèle de vApp dans un catalogue.

vCloud Director prend en charge les spécifications de format OVF (Open Virtualization Format) et de dispositif OVA (Open Virtualization Appliance). Si vous téléchargez un fichier OVF qui inclut des propriétés OVF pour la personnalisation de ses machines virtuelles, ces propriétés sont préservées dans le modèle de vApp. Pour obtenir des informations sur la création de modules OVF, consultez le *Guide de l'utilisateur d'OVF Tool* et le *Guide de l'utilisateur VMware vCenter Converter*.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle d'**auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal ( ), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 Cliquez sur **Ajouter**.

3 Saisissez l'adresse URL du fichier OVF ou cliquez sur l'icône **Télécharger** (↑) pour naviguer jusqu'à un emplacement accessible dans votre ordinateur, puis sélectionnez le fichier du modèle OVF/OVA.

   L'emplacement peut être votre disque dur local, un partage réseau ou un lecteur de CD/DVD. Les extensions de fichier prises en charge incluent `.ova`, `.ovf`, `.vmdk`, `.mf`, `.cert` et `.strings`. Si vous choisissez de télécharger un fichier OVF qui fait référence à plus de fichiers que ce que vous essayez d'importer (par exemple, un fichier VMDK), vous devez parcourir et sélectionner tous les fichiers.

4 Vérifiez les détails du modèle OVF/OVA que vous êtes sur le point de déployer et cliquez sur **Suivant**.

5 Entrez un nom et une description (facultative) pour le modèle de vApp, puis cliquez sur **Suivant**.

6 Dans le menu déroulant du **Catalogue**, sélectionnez le catalogue auquel vous souhaitez ajouter le modèle.

7 Vérifiez les paramètres du modèle de vApp et cliquez sur **Terminer**.

Résultats

Le nouveau modèle de vApp s'affiche dans la vue Grille des modèles.

Attribuer une stratégie de positionnement de machine virtuelle et une stratégie de dimensionnement de machine virtuelle à un modèle de vApp

Pour associer les machines virtuelles d'un modèle de vApp à des stratégies de positionnement et de dimensionnement de machines virtuelles spécifiques, vous pouvez baliser des machines virtuelles individuelles d'un modèle de vApp avec les stratégies que vous souhaitez attribuer.

À partir de vCloud Director 10.0, vous pouvez autoriser les utilisateurs à modifier les stratégies de placement ou de dimensionnement de VM prédéfinies lors de la modification d'une machine virtuelle.

Note Après la mise à niveau vers vCloud Director 10.0, tous les balisages de modèles pré-existants deviennent modifiables. Si vous souhaitez interdire les modifications des stratégies de placement ou de dimensionnement de VM prédéfinies, vous devez décocher la case **Modifiable** des stratégies que vous souhaitez rendre non modifiables.

Conditions préalables

- Cette opération nécessite le droit de modifier un modèle de vApp.
- Vérifiez que vous disposez d'au moins un modèle de vApp dans votre environnement vCloud Director.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 Sélectionnez la case d'option en regard du modèle de vApp que vous souhaitez étiqueter, puis cliquez sur **Étiqueter avec des stratégies de calcul**.

3 Si vous souhaitez attribuer une stratégie de positionnement de machine virtuelle à une machine virtuelle dans le modèle de vApp, sélectionnez une stratégie dans le menu déroulant **Stratégie de positionnement de VM** sur la ligne correspondant à la machine virtuelle.

4 Si vous souhaitez attribuer une stratégie de dimensionnement de machine virtuelle à une machine virtuelle dans le modèle de vApp, sélectionnez une stratégie dans le menu déroulant **Stratégie de dimensionnement de VM** sur la ligne correspondant à la machine virtuelle.

5 (Facultatif) Pour permettre aux utilisateurs de modifier les stratégies de positionnement ou de dimensionnement de machine virtuelle prédéfinies lors de la modification d'une machine virtuelle, cochez la case **Modifiable** dans le menu déroulant de la stratégie.

6 Cliquez sur **Balise**.

Télécharger un modèle de vApp

Vous pouvez, à partir d'un catalogue, télécharger un modèle de vApp sur votre machine locale en tant que fichier OVA.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle d'**auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) à gauche du modèle de vApp que vous souhaitez télécharger, puis sélectionnez **Télécharger**.

   Note Vous pouvez télécharger des modèles de vApp à partir des catalogues de votre organisation. Si vous êtes un administrateur d'organisation, vous pouvez télécharger des modèles de vApp à partir d'un catalogue public. Dans le cas contraire, le bouton **Télécharger** est grisé.

3 (Facultatif) Pour conserver les UUID et les adresses MAC des machines virtuelles dans le module OVA téléchargé, cochez la case **Conserver les informations d'identité**.

4 Cliquez sur **OK** et attendez que le téléchargement soit terminé.

Le fichier OVA est enregistré à l'emplacement de téléchargement par défaut de votre navigateur Web.

Supprimer un modèle de vApp

Vous pouvez supprimer un modèle de vApp d'un catalogue d'organisation. Si le catalogue est publié, le modèle de vApp est également supprimé des catalogues publics.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle d'**auteur de vApp** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de vApp** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) à gauche du modèle de vApp que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

3 Confirmez la suppression.

Le modèle de vApp supprimé est retiré de la vue Grille.

Utilisation des fichiers de support 12

Le catalogue vous permet de télécharger, de copier, de déplacer et de modifier les propriétés des fichiers de support.

Ce chapitre contient les rubriques suivantes :

- Télécharger des fichiers de support
- Supprimer un fichier de support
- Télécharger un fichier de support

Télécharger des fichiers de support

Vous pouvez télécharger les nouveaux fichiers de support ou de nouvelles versions des fichiers de support existants dans un catalogue. Les utilisateurs ayant accès au catalogue peuvent ouvrir les fichiers de support avec leurs machines virtuelles.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Support et autre** dans le panneau de gauche.

   La liste des fichiers de support s'affiche dans une vue de grille.
2. Cliquez sur **Ajouter**.
3. Dans le menu déroulant **Catalogue**, sélectionnez un catalogue vers lequel vous souhaitez télécharger le fichier de support.
4. Entrez un nom pour le fichier de support.

   Si vous n'entrez pas de nom, la zone de texte de nom est renseignée automatiquement en fonction du nom du fichier de support.
5. Cliquez sur l'icône de téléchargement (⤒) pour rechercher et sélectionner le fichier image de disque, par exemple un fichier `.iso`.

6 Cliquez sur **OK**.

Après le début du téléchargement, le fichier de support figure dans la grille.

Étape suivante

En fonction de la taille du fichier, le téléchargement peut prendre un certain temps. Vous pouvez surveiller l'état du téléchargement dans la vue **Tâches récentes**. Pour plus d'informations, reportez-vous à la section Afficher les tâches.

Supprimer un fichier de support

Vous pouvez supprimer de votre catalogue des fichiers de support que vous ne souhaitez plus utiliser.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Support et autre** dans le panneau de gauche.

La liste des fichiers de support s'affiche dans une vue de grille.

2 Cliquez sur la barre de liste (⋮) à gauche du fichier de support que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

3 Confirmez la suppression.

Le fichier de support supprimé est retiré de la vue de grille.

Télécharger un fichier de support

Vous pouvez télécharger un fichier de support à partir d'un catalogue.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Support et autre** dans le panneau de gauche.

La liste des fichiers de support s'affiche dans une vue de grille.

2 Cliquez sur la barre de liste (⋮) à gauche du fichier de support que vous souhaitez télécharger, puis sélectionnez **Télécharger**.

   La tâche de téléchargement démarre et le fichier est enregistré à l'emplacement de téléchargement par défaut de votre navigateur Web.

Étape suivante

En fonction de la taille du fichier, le téléchargement peut prendre un certain temps. Vous pouvez surveiller l'état du téléchargement dans le panneau **Tâches récentes**. Pour plus d'informations, reportez-vous à la section Afficher les tâches.

Utilisation des catalogues

13

Un catalogue est un conteneur pour des modèles de vApp et des fichiers de support dans une organisation. Les administrateurs d'organisation et les auteurs de catalogue peuvent créer des catalogues dans une organisation. Les catalogues de contenu peuvent être partagés avec d'autres utilisateurs ou organisations dans l'installation vCloud Director ou publiés en externe pour permettre aux organisations en dehors de l'installation vCloud Director d'y accéder.

vCloud Director contient des catalogues privés, des catalogues partagés et des catalogues accessibles de l'extérieur. Les catalogues privés incluent des modèles de vApp et des fichiers de support que vous pouvez partager avec les autres utilisateurs de l'organisation. Si un administrateur système active le partage de catalogue pour votre organisation, vous pouvez partager un catalogue d'organisation pour créer un catalogue accessible aux autres organisations de l'installation vCloud Director. Si l'administrateur système active la publication de catalogue externe pour votre organisation, vous pouvez publier un catalogue d'organisation pour permettre aux organisations en dehors de l'installation vCloud Director d'y accéder. Une organisation externe à l'installation vCloud Director doit s'abonner à un catalogue publié en externe pour accéder à son contenu.

Vous pouvez télécharger un module OVF directement vers un catalogue, enregistrer un vApp comme modèle de vApp ou importer un modèle de vApp depuis vSphere. Reportez-vous à Créer un modèle de vApp à partir d'un fichier OVF et Enregistrer un vApp en tant que modèle de vApp dans un catalogue.

Les membres d'une organisation peuvent accéder aux modèles de vApp et aux fichiers de support dont ils sont propriétaires ou qui sont partagés avec eux. Les administrateurs d'organisation et les administrateurs système peuvent partager un catalogue avec quiconque dans une organisation ou avec des utilisateurs ou des groupes spécifiques d'une organisation. Reportez-vous à Partager un catalogue.

Ce chapitre contient les rubriques suivantes :

- Afficher les catalogues
- Créer un catalogue
- Partager un catalogue
- Supprimer un catalogue
- Gérer les métadonnées pour un catalogue

- Publier un catalogue
- S'abonner à un catalogue externe
- Mettre à jour l'URL d'emplacement et le mot de passe d'un catalogue abonné
- Synchroniser un catalogue abonné

Afficher les catalogues

Vous pouvez accéder aux catalogues partagés avec vous au sein de votre organisation. Vous pouvez accéder aux catalogues publics si un administrateur d'organisation les a rendus accessibles au sein de votre organisation.

L'accès au catalogue est contrôlé par le partage de catalogue, plutôt que par les droits dans votre rôle. Vous pouvez accéder uniquement aux catalogues ou aux éléments de catalogue qui sont partagés avec vous. Pour plus d'informations, reportez-vous à la section Partager un catalogue.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 (Facultatif) Configurez la vue de grille pour qu'elle contienne les éléments que vous souhaitez afficher.

a Dans la vue de grille, cliquez sur l'icône de l'éditeur de grille ( ) située au-dessous de la liste des catalogues.

b Sélectionnez les éléments que vous souhaitez inclure dans la vue de grille, tels que la version, la description, l'état, etc.

c Cliquez sur **OK**.

La grille affiche les éléments que vous avez sélectionnés pour chaque catalogue.

3 (Facultatif) À partir de la vue de grille, utilisez la barre de liste (⋮) pour afficher les actions que vous pouvez effectuer pour chaque catalogue.

Par exemple, vous pouvez partager ou supprimer un catalogue.

Créer un catalogue

Vous pouvez créer des catalogues et les associer à une stratégie de stockage.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

   La liste des catalogues s'affiche dans une vue de grille.
2. Cliquez sur **Nouveau** pour créer un catalogue.
3. Entrez le nom et éventuellement la description du catalogue.
4. (Facultatif) Indiquez si vous souhaitez attribuer une stratégie de stockage au catalogue, puis sélectionnez une stratégie de stockage.
5. Cliquez sur **OK**.

Résultats

Le nouveau catalogue s'affiche dans la vue grille dans l'onglet **Catalogues**.

Partager un catalogue

Vous pouvez partager un catalogue avec tous les membres de votre organisation ou avec des membres spécifiques.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.
- Vous devez être le propriétaire du catalogue.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

   La liste des catalogues s'affiche dans une vue de grille.
2. Cliquez sur la barre de liste (⋮) à gauche du catalogue que vous souhaitez partager, puis sélectionnez **Partager**.

   La liste des utilisateurs qui peuvent accéder au catalogue s'affiche dans la vue de grille de la fenêtre **Partager le catalogue**.

3 Cliquez sur **Ajouter** pour partager le catalogue avec d'autres utilisateurs.

Option	Description
Partager avec tout le monde dans cette organisation	Accordez l'accès à l'ensemble des utilisateurs et des groupes de l'organisation.
Partager avec des groupes et utilisateurs spécifiques	Sélectionnez les utilisateurs ou les groupes auxquels vous souhaitez accorder l'accès au catalogue, puis cliquez sur **Ajouter**.

4 Sélectionnez le niveau d'accès.

Option	Description
Lecture seule	Les utilisateurs ayant accès au catalogue ont accès en lecture aux modèles de vApp et aux fichiers ISO du catalogue.
Lecture/écriture	Les utilisateurs ayant accès au catalogue ont accès en lecture aux modèles de vApp et aux fichiers ISO du catalogue. Ils peuvent également ajouter des modèles de vApp et des fichiers ISO au catalogue.
Contrôle total	Les utilisateurs ayant accès au catalogue ont le contrôle total du contenu et des paramètres du catalogue.

5 Cliquez sur **OK**.

Les utilisateurs ou les groupes qui ont désormais accès au catalogue s'affichent dans la vue de grille de la boîte de dialogue **Partage du catalogue**.

6 (Facultatif) Choisissez de partager l'accès en lecture seule avec les administrateurs de toutes les autres organisations.

7 Cliquez sur **Enregistrer**.

Résultats

Dans l'onglet **Catalogues**, l'état Partagé de ce catalogue dans la vue de grille change.

Supprimer un catalogue

Vous pouvez supprimer un catalogue de votre organisation.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Auteur de catalogue** prédéfini ou un ensemble de droits équivalent.

Note Le catalogue ne doit pas contenir de modèles de vApp ou de fichiers de support. Vous pouvez déplacer ces éléments vers un autre catalogue ou les supprimer.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) à gauche du catalogue que vous souhaitez supprimer, puis sélectionnez **Supprimer**.

3 Confirmez la suppression.

   L'élément de catalogue supprimé est retiré de la vue Grille.

Gérer les métadonnées pour un catalogue

En tant qu'**administrateur d'organisation** ou **propriétaire de catalogues**, vous pouvez créer ou mettre à jour les métadonnées des catalogues que vous possédez.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) sur la gauche d'un catalogue et sélectionnez **Métadonnées**.

   Les métadonnées du catalogue sélectionné s'affichent dans une vue de grille.

3 (Facultatif) Pour ajouter des métadonnées, cliquez sur **Ajouter**.

   a Entrez le nom de métadonnées.

      Le nom doit être unique au sein des noms de métadonnées associés à cet objet.

   b Sélectionnez le type de métadonnées, tel que **Texte**, **Nombre**, **Date et heure** ou **Oui ou non**.

   c Entrez la valeur des métadonnées.

   d Cliquez sur **Enregistrer**.

4 (Facultatif) Mettez à jour des métadonnées existantes.

   Vous ne pouvez pas mettre à jour le nom des métadonnées.

   a Mettez à jour le type de métadonnées.

   b Entrez la nouvelle valeur des métadonnées.

   c Cliquez sur **Enregistrer**.

5 (Facultatif) Supprimez les métadonnées existantes.

   a Cliquez sur l'icône Supprimer.

   b Cliquez sur **Enregistrer**.

Publier un catalogue

Si l'**administrateur système** vous a accordé l'accès aux catalogues, vous pouvez publier un catalogue en externe pour rendre ses modèles de vApp et ses fichiers de support accessibles par abonnement aux organisations en dehors de l'installation vCloud Director.

Conditions préalables

Vérifiez que l'**administrateur système** a activé la publication de catalogues externes pour l'organisation et vous a autorisé à accéder aux catalogues.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) à gauche du catalogue que vous souhaitez publier, puis sélectionnez **Publier les paramètres**.

3 Sélectionnez **Activer la publication** et entrez éventuellement un mot de passe pour accéder au catalogue.

   Seuls les caractères ASCII sont pris en charge.

4 Cliquez sur **Enregistrer**.

S'abonner à un catalogue externe

Vous pouvez vous abonner à un catalogue externe et ainsi en créer une copie en lecture seule. Vous ne pouvez pas modifier un catalogue abonné.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- L'**administrateur système** doit accorder à votre organisation l'autorisation de vous abonner aux catalogues externes.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 Cliquez sur **Nouveau** pour créer un catalogue.

3 Entrez le nom et éventuellement la description du catalogue.

4 Choisissez de vous abonner à un catalogue externe et fournissez l'URL d'abonnement.

5 Entrez le mot de passe facultatif pour accéder au catalogue.

6 Indiquez si vous souhaitez télécharger automatiquement le contenu du catalogue externe.

7 Cliquez sur **OK**.

Mettre à jour l'URL d'emplacement et le mot de passe d'un catalogue abonné

Après avoir créé un catalogue abonné, vous pouvez mettre à jour son URL d'emplacement et son mot de passe.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Vous devez avoir créé un catalogue abonné.
- L'**administrateur système** doit accorder à votre organisation l'autorisation de vous abonner aux catalogues externes.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2 Cliquez sur la barre de liste (⋮) à gauche d'un catalogue abonné, puis sélectionnez **Paramètres d'abonnement**.

   Si le catalogue n'est pas abonné, cette option est grisée.

3 Mettez à jour l'URL d'emplacement et le mot de passe de ce catalogue abonné.

4 Indiquez si vous souhaitez télécharger automatiquement le contenu du catalogue externe.

5 Cliquez sur **Enregistrer**.

Synchroniser un catalogue abonné

Après avoir créé un catalogue abonné, vous pouvez le synchroniser avec le catalogue d'origine pour voir si des modifications ont été apportées. Par exemple, si les métadonnées du catalogue d'origine ont été modifiées, les métadonnées du catalogue abonné sont mises à jour lors de la synchronisation.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Vous devez avoir créé un catalogue abonné.
- L'**administrateur système** doit accorder à votre organisation l'autorisation de vous abonner aux catalogues externes.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Catalogues** dans le panneau de gauche.

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

2. Cliquez sur la barre de liste (⋮) à gauche d'un catalogue abonné, puis sélectionnez **Synchroniser**.

   Si le catalogue n'est pas abonné, cette option est grisée.

   Le catalogue abonné est synchronisé avec celui d'origine.

Utilisation des modèles de centre de données virtuel d'organisation

14

En tant qu'administrateur d'organisation ou si vous bénéficiez d'un rôle autorisé à afficher et à instancier des modèles de centre de données virtuel d'organisation, vous pouvez créer des centres de données virtuels d'organisation supplémentaires.

Un modèle de centre de données virtuel d'organisation spécifie une configuration pour un centre de données virtuel d'organisation et, en option, une passerelle Edge et un réseau de centres de données virtuels d'organisation. Les administrateurs système peuvent autoriser les administrateurs d'organisation à créer ces ressources dans leurs organisations en créant des modèles de centre de données d'organisation et en les partageant avec ces organisations.

En créant et en partageant des modèles de centre de données virtuel d'organisation, les administrateurs système permettent le provisionnement autonome de centres de données virtuels d'organisation tout en gardant le contrôle administratif sur l'allocation des ressources du système, telles que les centres de données virtuels fournisseurs et les réseaux externes.

Les administrateurs système créent des modèles de centre de données virtuel d'organisation et fournissent à différentes organisations l'accès aux modèles.

Si votre organisation a obtenu l'accès à des modèles de centre de données virtuel, vous pouvez utiliser le vCloud Director Tenant Portal pour créer des centres de données virtuels à partir des modèles disponibles.

Ce chapitre contient les rubriques suivantes :

- Afficher les modèles de centre de données virtuel disponibles
- Créer un centre de données virtuel à partir d'un modèle

Afficher les modèles de centre de données virtuel disponibles

Vous pouvez afficher les modèles de centre de données virtuel d'organisation qu'un administrateur système a créés pour vous.

Affichez les modèles de centre de données virtuel avant de créer un centre de données virtuel d'organisation à partir du modèle de centre de données virtuel.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Administrateur d'organisation** prédéfini ou un rôle qui est autorisé à afficher et instancier des modèles de centre de données virtuel d'organisation.

Procédure

- Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de VDC** dans le panneau de gauche.

  La liste des modèles de centre de données virtuel s'affiche dans une vue de grille.

Étape suivante

Passez en revue les descriptions des modèles de centre de données virtuel d'organisation et sélectionnez le modèle à partir duquel vous souhaitez créer un centre de données virtuel d'organisation.

Créer un centre de données virtuel à partir d'un modèle

Vous pouvez créer un centre de données virtuel d'organisation à partir d'un modèle de centre de données virtuel que votre administrateur système a créé.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle **Administrateur d'organisation** prédéfini ou un rôle qui est autorisé à afficher et instancier des modèles de centre de données virtuel d'organisation.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis **Modèles de VDC** dans le panneau de gauche.

   La liste des modèles de centre de données virtuel s'affiche dans une vue de grille.
2. Sélectionnez un modèle, puis cliquez sur **Nouveau VDC**.
3. Entrez un nom pour le centre de données virtuel et, éventuellement, une description.
4. Cliquez sur **Créer**.

Résultats

La création du nouveau centre de données virtuel d'organisation est instanciée et peut prendre quelques minutes. Vous pouvez consultez la progression de la tâche dans le panneau **Tâches récentes**.

Étape suivante

Vous pouvez gérer le centre de données virtuel d'organisation nouvellement créé en effectuant différentes tâches : création de machines virtuelles, création de vApp, gestion des paramètres réseau et de sécurité, etc.

Gestion des utilisateurs, groupes et rôles

15

Vous pouvez ajouter des administrateurs de l'organisation à vCloud Director individuellement, ou comme partie 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.

Important Vous devez être **administrateur d'organisation** pour gérer les utilisateurs, les groupes et les rôles au sein de votre organisation. Votre **administrateur système** peut publier un ou plusieurs rôles de locataire globaux sur votre locataire et, en tant qu'**administrateur d'organisation**, vous pouvez les voir dans la liste des rôles. Ces rôles sont, par exemple, **Auteur de catalogue**, **Auteur de vApp**, **Utilisateur de vApp**, **Administrateur d'organisation**, etc. Vous ne pouvez pas modifier les rôles de locataire globaux prédéfinis, mais vous pouvez créer et mettre à jour les rôles de locataire personnalisés semblables, et les attribuer aux utilisateurs dans votre locataire.

Ce chapitre contient les rubriques suivantes :

- Gestion des utilisateurs
- Gestion des groupes
- Rôles et droits

Gestion des utilisateurs

À partir du portail de locataire vous pouvez créer, modifier, importer et supprimer des utilisateurs. En outre, vous pouvez également déverrouiller les comptes d'utilisateurs dans le cas où un utilisateur a tenté de se connecter avec un mot de passe incorrect et par conséquent a verrouillé son compte d'utilisateur.

Créer un utilisateur

Vous pouvez créer un utilisateur au sein de votre organisation vCloud Director.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

La liste des utilisateurs s'affiche.

3 Cliquez sur **Créer**.

4 (Facultatif) Entrez un nom d'utilisateur et le mot de passe de l'utilisateur.

La longueur minimale du mot de passe est de six caractères.

5 Choisissez d'activer ou non l'utilisateur lors de la création.

6 Choisissez le rôle que vous souhaitez attribuer à l'utilisateur.

Le menu **Rôles disponibles** est composé d'une liste de rôles prédéfinis et de tous les rôles personnalisés que vous ou l'administrateur système pouvez avoir créés.

Rôle prédéfini	Description
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.
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.
Utilisateur de vApp	Les droits associés au rôle prédéfini **Utilisateur de vApp** permettent à un utilisateur d'utiliser des vApp existants.
Administrateur d'organisation	Un utilisateur disposant du rôle **Administrateur de l'organisation** prédéfini peut utiliser le portail de locataires de vCloud Director ou vCloud API pour gérer les utilisateurs et les groupes de son organisation et leur attribuer des rôles, y compris le rôle **Administrateur de l'organisation** prédéfini. Un **administrateur d'organisation** peut utiliser vCloud API pour créer ou mettre à jour les objets de rôle qui sont locaux pour l'organisation. Les rôles créés ou modifiés par un **administrateur d'organisation** ne sont pas visibles par les autres organisations.
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, le nom du rôle indiqué par le fournisseur d'identité doit correspondre exactement, casse comprise, à un nom ou un rôle défini dans votre organisation.
Auteur du catalogue	Les droits associés au rôle prédéfini **Auteur de catalogue** permettent à un utilisateur de créer et de publier des catalogues.

7 (Facultatif) Entrez les informations de contact, comme le nom, l'adresse e-mail, le numéro de téléphone et l'ID de messagerie instantanée.

8 (Facultatif) Entrez le quota de machines virtuelles pour l'utilisateur.

Le quota détermine le nombre de machines virtuelles et de machines virtuelles en cours d'exécution que l'utilisateur peut gérer. Sélectionnez **Illimité** si vous souhaitez permettre à l'utilisateur d'utiliser un nombre illimité de machines virtuelles.

9 Cliquez sur **Enregistrer**.

Importer des utilisateurs

Vous pouvez ajouter des utilisateurs à vos organisations, en important un utilisateur LDAP ou un utilisateur SAML et en leur attribuant un rôle donné.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Vérifiez que vous disposez d'une connexion valide à un serveur LDAP ou que vous Chapitre 16 Permettre à votre organisation d'utiliser un fournisseur d'identité SAML.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

La liste des utilisateurs s'affiche.

3 Cliquez sur **Importer des utilisateurs**.

4 Sélectionnez une source à partir de laquelle vous souhaitez importer les utilisateurs.

Vous n'afficherez que le serveur LDAP source ou le serveur SAML que vous avez configuré comme fournisseur d'identité.

Source	Action
LDAP	Importez des utilisateurs depuis un serveur LDAP. a Entrez un nom partiel ou complet dans la zone de texte et cliquez sur **Rechercher**. b Sélectionnez les utilisateurs que vous souhaitez importer et cliquez sur **Ajouter**.
SAML	Importez des utilisateurs depuis un serveur SAML. Saisir les noms des utilisateurs que vous souhaitez importer. Les noms d'utilisateur doivent être au format d'identifiant de nom pris en charge par le fournisseur d'identité SAML configuré pour cette organisation. **Note** Si vous utilisez vCenter Single Sign-On comme fournisseur d'identité SAML, les noms d'utilisateur que vous importez à partir d'un domaine vCenter Single Sign-On doivent être au format UPN (User Principal Name), par exemple jdoe@mondomaine.com. Utilisez une nouvelle ligne pour chaque nom d'utilisateur.

5 Sélectionnez le rôle que vous voulez attribuer aux utilisateurs à importer.

6 Cliquez sur **Enregistrer**.

Modifier un utilisateur

En tant qu'administrateur d'organisation, vous pouvez modifier le mot de passe, le contact et les paramètres de quota de machines virtuelles d'un utilisateur existant. En outre, vous pouvez également modifier le rôle de l'utilisateur.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

La liste des utilisateurs s'affiche.

3 Sélectionnez la case d'option en regard du nom de l'utilisateur à modifier et cliquez sur **Modifier**.

4 Mettez à jour les paramètres à modifier.

a Modifiez le mot de passe si nécessaire.

b Choisissez d'activer ou de désactiver l'utilisateur.

c Mettez à jour le rôle d'utilisateur.

d Mettez à jour les informations de contact, comme le nom, l'adresse e-mail, le numéro de téléphone et l'ID de messagerie instantanée.

e Modifiez le quota de machines virtuelles pour l'utilisateur.

5 Cliquez sur **Enregistrer**.

Désactiver ou activer un compte d'utilisateur

Vous pouvez désactiver un compte d'utilisateur pour empêcher cet utilisateur de se connecter à vCloud Director. Pour supprimer un utilisateur, vous devez d'abord désactiver son compte.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

   La liste des utilisateurs s'affiche.

3 Pour désactiver un compte d'utilisateur, sélectionnez la case d'option en regard du nom d'utilisateur, cliquez sur **Désactiver** et confirmez que vous souhaitez désactiver le compte.

4 Pour activer un compte d'utilisateur que vous avez déjà désactivé, sélectionnez la case d'option en regard du nom d'utilisateur et cliquez sur **Activer**.

Supprimer un utilisateur

Vous pouvez supprimer un utilisateur de l'organisation vCloud Director en supprimant le compte d'utilisateur.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Désactivez le compte que vous souhaitez supprimer.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

   La liste des utilisateurs s'affiche.

3 Sélectionnez la case d'option en regard du nom de l'utilisateur à supprimer et cliquez sur **Supprimer**.

4 Pour confirmer la suppression du compte d'utilisateur, cliquez sur **OK**.

Déverrouiller un compte utilisateur verrouillé

Dans le cas où vous avez activé une stratégie de verrouillage de votre organisation vCloud Director, un compte d'utilisateur est verrouillé après un certain nombre de tentatives de connexion non valides. Vous pouvez déverrouiller le compte utilisateur verrouillé. La recommandation consiste à modifier le mot de passe de l'utilisateur et déverrouiller le compte.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Utilisateurs**.

   La liste des utilisateurs s'affiche.

3 Cliquez sur le bouton radio en regard du nom d'utilisateur, cliquez sur **Déverrouiller**.

Gestion des groupes

Si vous disposez d'une connexion valide à un serveur LDAP ou si vous avez activé votre organisation pour utiliser un fournisseur d'identité SAML, vous pouvez importer un groupe LDAP ou un groupe SAML. Vous pouvez également modifier ou supprimer un groupe importé.

Importer un groupe

Pour ajouter un groupe d'utilisateurs, vous pouvez importer un groupe LDAP ou un groupe SAML.

Conditions préalables

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Vérifiez que vous disposez d'une connexion valide à un serveur LDAP ou que vous Chapitre 16 Permettre à votre organisation d'utiliser un fournisseur d'identité SAML.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Groupes**.

La liste des groupes d'utilisateurs s'affiche.

3 Cliquez sur **Importer un groupe**.

4 Sélectionnez une source à partir de laquelle vous souhaitez importer le groupe d'utilisateurs.

Vous n'afficherez que le serveur LDAP source ou le serveur SAML que vous avez configuré comme fournisseur d'identité.

Source	Action
LDAP	Importez un groupe d'utilisateurs depuis un serveur LDAP. a Entrez un nom partiel ou complet dans la zone de texte et cliquez sur **Rechercher**. b Sélectionnez les groupes d'utilisateurs que vous souhaitez importer et cliquez sur **Ajouter**.
SAML	Importez des groupes d'utilisateurs à partir d'un serveur SAML. Sélectionnez les noms de groupes que vous souhaitez importer. Utilisez une nouvelle ligne pour chaque nom de groupe.

5 Sélectionnez le rôle que vous voulez attribuer au groupe d'utilisateurs à importer.

6 Cliquez sur **Enregistrer**.

Supprimer un groupe

Vous pouvez supprimer un groupe de votre organisation vCloud Director en supprimant son groupe LDAP.

Lorsque vous supprimez un groupe LDAP, les utilisateurs disposant d'un compte vCloud Director basé uniquement sur leur appartenance à ce groupe sont bloqués et dans l'impossibilité de se connecter.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Groupes**.

   La liste des groupes d'utilisateurs s'affiche.
3. Cliquez sur le bouton radio en regard du nom du groupe à supprimer, puis sur **Supprimer**.
4. Pour confirmer la suppression du groupe, cliquez sur **OK**.

Modifier un groupe

Vous pouvez modifier un groupe à partir du portail de locataires de vCloud Director.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Groupes**.

   La liste des groupes d'utilisateurs s'affiche.
3. Sélectionnez le bouton radio en regard du nom du groupe à supprimer, puis cliquez sur **Modifier**.
4. Modifiez le groupe si nécessaire.
   a. Modifiez la description.
   b. Modifiez le rôle des membres du groupe si nécessaire.
5. Cliquez sur **Enregistrer**.

Rôles et droits

vCloud Director utilise des rôles et droits pour déterminer quelles actions un utilisateur peut effectuer dans une organisation. vCloud Director inclut plusieurs rôles prédéfinis avec des droits spécifiques.

Les **administrateurs système** et les **administrateurs d'organisation** doivent attribuer un rôle à chaque utilisateur ou groupe. Un même utilisateur peut posséder un rôle différent dans plusieurs organisations. Les **administrateurs système** peuvent créer des rôles et modifier des rôles existants pour l'ensemble du système, tandis que les **administrateurs d'organisation** peuvent créer et modifier des rôles uniquement pour l'organisation qu'ils administrent.

Le portail de locataires vCloud Director permet aux **administrateurs d'organisation** de gérer les rôles dans leur organisation. Si un **administrateur système** publie un ou plusieurs rôles prédéfinis de locataire dans votre organisation, en tant qu'**administrateur d'organisation** vous pouvez voir ces rôles, mais vous ne pouvez pas les modifier. Cependant, vous pouvez créer des rôles de locataire personnalisés avec des droits similaires et les attribuer aux utilisateurs de votre organisation.

Pour plus d'informations sur les rôles prédéfinis et leurs droits, reportez-vous à Rôles prédéfinis et leurs droits.

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 *Guide du portail d'administration des fournisseurs de services vCloud Director*. 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

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 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	✓	✓			

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	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	✓	✓			
	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	✓				

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 : 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	✓				
	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	✓				

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 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	✓				
	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	✓				

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 : 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	✓				
	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	✓				

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 : 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	✓				
	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	✓	✓	✓	✓	

Nouveautés dans cette version	Nom du droit	Administrateur d'organisation	Auteur de catalogue	Auteur de vApp	Utilisateur de vApp	Accès via la console uniquement
	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	✓	✓	✓		
	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	✓	✓	✓		

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 : 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	✓				

Créer un rôle de locataire personnalisé

Les administrateurs d'organisations peuvent utiliser le portail de locataires pour créer des objets de rôles de locataires personnalisés dans les organisations qu'ils administrent.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Rôles**.

   La liste des rôles s'affiche.
3. Cliquez sur **Ajouter**.
4. Entrez le nom et la description (facultative) du rôle.
5. Développez les droits du rôle et sélectionnez les droits pour le rôle.

   Les droits sont regroupés en catégories et sous-catégories qui permettent l'affichage ou la gestion des objets.

Option	Description
Contrôle d'accès	Droits de contrôle de l'accès pour afficher et gérer certains objets.
Administration	Droits de contrôle de l'accès administratif.

Option	Description
Calculer	Droits de contrôle de l'accès et de la gestion des centres de données virtuels fournisseur et d'organisation, des vApp, des modèles de centres de données virtuels d'organisation, des groupes de machines virtuelles et de la surveillance de machines virtuelles.
Extensions	Droits de contrôle de l'accès à n'importe quel plug-in et extension de vCloud Director supplémentaire.
Infrastructure	Droits de contrôle de l'accès et de la gestion des objets de l'infrastructure, tels que les banques de données, les disques, les hôtes, etc.
Bibliothèques	Droits de contrôle de l'accès et de la gestion de n'importe quel catalogue et élément du catalogue.
Mise en réseau	Droits de contrôle de l'accès et de la gestion des paramètres réseau.

6 Cliquez sur **Enregistrer**.

Modifier un rôle de locataire personnalisé

Les administrateurs d'organisation peuvent utiliser le portail de locataires pour modifier des objets de rôle de locataire personnalisé dans les organisations qu'ils administrent. En tant qu'administrateur d'organisation, vous pouvez uniquement afficher les rôles de locataire globaux qu'un administrateur système a publié dans votre organisation. Vous ne pouvez pas modifier les rôles de locataire globaux.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Rôles**.

La liste des rôles s'affiche.

3 Sélectionnez la case d'option en regard du rôle à modifier et cliquez sur **Modifier**.

4 Modifiez les paramètres de rôle selon vos besoins.

a Modifiez le nom et la description (facultative) du rôle.

b Modifiez les droits pour le rôle.

5 Cliquez sur **Enregistrer**.

Supprimer un rôle

Les administrateurs d'organisation peuvent utiliser le portail de locataires pour supprimer les objets de rôle dans les organisations qu'ils administrent.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Dans le panneau de gauche, sous **Contrôle d'accès**, cliquez sur **Rôles**.

   La liste des rôles s'affiche.
3. Sélectionnez la case d'option en regard du rôle à supprimer et cliquez sur **Supprimer**.
4. Pour confirmer la suppression du rôle, cliquez sur **OK**.

Permettre à votre organisation d'utiliser un fournisseur d'identité SAML

16

Permettez à votre organisation d'utiliser un fournisseur d'identité SAML (Security Assertion Markup Language), également appelé Single Sign-On, pour importer des utilisateurs et des groupes à partir d'un fournisseur d'identité SAML et autoriser les utilisateurs importés à se connecter à l'organisation avec les informations d'identification établies dans le fournisseur d'identité SAML.

Lorsque vous importez des utilisateurs et des groupes, le système extrait une liste des attributs à partir du jeton SAML, le cas échéant, et les utilise pour interpréter les éléments d'informations correspondants sur l'utilisateur tentant de se connecter.

- `email address = "EmailAddress"`
- `user name = "UserName"`
- `full name = "FullName"`
- `user's groups = "Groups"`
- `user's roles = "Roles"`

  L'attribut Role est configurable.

Les informations sur le groupe sont nécessaires si l'utilisateur n'est pas importé directement, mais doit être en mesure de se connecter en raison de son appartenance aux groupes importés. Un utilisateur peut appartenir à plusieurs groupes, et donc avoir plusieurs rôles pendant une session.

Si le rôle **Différer vers le fournisseur d'identité** est attribué à un utilisateur ou groupe importé, les rôles sont attribués 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

- Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.
- Vérifiez que vous avez accès à un fournisseur d'identité compatible SAML 2.0.

- Vérifiez que vous recevez les métadonnées requises de votre fournisseur d'identité SAML. Vous devez importer les métadonnées dans vCloud Director manuellement ou dans un fichier XML. Les métadonnées doivent inclure les informations suivantes :
  - 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 de métadonnées depuis un fournisseur SAML, consultez la documentation de votre fournisseur SAML.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Sous **Fournisseurs d'identité**, cliquez sur **SAML**.
3. Cliquez sur **Modifier**.
4. Sous l'onglet **Fournisseur de services**, entrez l'ID d'entité.

   L'ID d'entité est l'identifiant unique de votre organisation auprès de votre fournisseur d'identité. Vous pouvez utiliser le nom de votre organisation ou toute autre chaîne qui répond aux exigences de votre fournisseur d'identité SAML.

   Important Une fois que vous spécifiez un ID d'entité, vous ne pouvez pas le supprimer. Pour modifier l'ID d'entité, vous devez effectuer une reconfiguration SAML complète pour votre organisation. Pour plus d'informations sur les ID d'entité, reportez-vous à la section Assertions et protocoles pour SAML (Security Assertion Markup Language) 2.0 développé par OASIS.
5. Cliquez sur le lien de **Métadonnées** pour télécharger les métadonnées SAML pour votre organisation.

   Les métadonnées téléchargées doivent être fournies en l'état à votre fournisseur d'identité.
6. Vérifiez la date d'expiration du certificat et, éventuellement, cliquez sur Régénérer afin de générer à nouveau le certificat utilisé pour signer des messages de fédération.

   Le certificat est inclus dans les métadonnées SAML, et est utilisé pour le chiffrement et la signature. Le chiffrement et/ou la signature peuvent être nécessaire selon la manière dont l'approbation est établie entre votre organisation et votre fournisseur d'identité SAML.
7. Sous l'onglet **Fournisseur d'identité**, activez le bouton bascule **Utiliser le fournisseur d'identité SAML**.
8. Copiez et collez les métadonnées SAML que vous avez reçues de votre fournisseur d'identité dans la zone de texte, ou cliquez sur **Télécharger** pour accéder aux métadonnées et les télécharger dans un fichier XML.
9. Cliquez sur **Enregistrer**.

Étape suivante

- Configurez votre fournisseur SAML avec les métadonnées de vCloud Director. Consultez la documentation de votre fournisseur d'identité SAML et le *Guide d'installation et de mise à niveau de vCloud Director*.
- Importez des utilisateurs et des groupes depuis votre fournisseur d'identité SAML. Consultez Chapitre 15 Gestion des utilisateurs, groupes et rôles

Gestion de votre organisation 17

En tant qu'**administrateur d'organisation**, vous pouvez modifier un certain nombre de paramètres au sein de votre organisation, tels que le nom de l'organisation, les paramètres de messagerie, les paramètres de domaine, les métadonnées, les stratégies, etc.

Ce chapitre contient les rubriques suivantes :

- Modifier le nom et la description de l'organisation
- Modifier vos paramètres d'e-mail
- Tester les paramètres SMTP
- Modifier les paramètres de domaine des machines virtuelles de votre organisation
- Utilisation sur plusieurs sites
- Configurer et gérer les déploiements multisite
- Comprendre comment fonctionnent les baux
- Modifier les stratégies vApp et Bail de modèle de vApp au sein de votre organisation
- Modifier les quotas par défaut des machines virtuelles de votre organisation
- Modifier les stratégies de mot de passe et de compte d'utilisateur au sein de votre organisation

Modifier le nom et la description de l'organisation

Vous pouvez modifier le nom complet et la description de votre organisation.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Sous **Paramètres**, cliquez sur **Général**.

   La liste des paramètres généraux tels que le nom de l'organisation, l'URL par défaut, le nom complet et description s'affiche.

3 Pour modifier le nom complet et la description de l'organisation, cliquez sur **Modifier**.

4 Appliquez les modifications nécessaires et cliquez sur **Enregistrer**.

Modifier vos paramètres d'e-mail

Vous pouvez vérifier et modifier les paramètres de messagerie par défaut qui ont été définis par l'administrateur système lors de la création de votre organisation.

vCloud Director envoie des e-mails d'alerte lorsque des informations importantes doivent être signalées, par exemple lorsqu'une banque de données manque d'espace. Par défaut, une organisation envoie des e-mails d'alerte aux administrateurs système ou à une liste d'adresses e-mail spécifiée au niveau du système à l'aide d'un serveur SMTP spécifié au niveau du système. Vous pouvez modifier les paramètres d'e-mail au niveau de l'organisation si vous souhaitez que vCloud Director envoie des alertes pour cette organisation à un ensemble d'adresses e-mail différent de celui spécifié au niveau du système ou si vous souhaitez que l'organisation utilise un serveur SMTP différent de celui spécifié au niveau du système pour envoyer des alertes.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Sous **Paramètres**, cliquez sur **E-mail**.

   Les paramètres de messagerie de votre organisation s'affichent.

3 Cliquez sur **Modifier**.

4 Modifiez les paramètres du serveur SMTP dans l'onglet **Serveur SMTP**.

   a Indiquez si vous souhaitez utiliser un serveur SMTP personnalisé ou le serveur par défaut.

   b Si vous choisissez d'utiliser un serveur SMTP personnalisé, entrez le nom d'hôte DNS ou l'adresse IP du serveur SMTP dans la zone de texte **nom du serveur SMTP**.

   c (Facultatif) Entrez le numéro de port du serveur SMTP.

   d (Facultatif) Indiquez si vous souhaitez exiger une authentification, puis entrez un nom d'utilisateur et un mot de passe.

5 Pour modifier les paramètres de notification, cliquez sur l'onglet **Paramètres de notification**.
   a Choisissez d'utiliser les paramètres de notification personnalisés.
   b Entrez l'adresse e-mail qui apparaît en tant qu'expéditeur des e-mails de l'organisation.
   c (Facultatif) Entrez le texte à utiliser comme préfixe de l'objet de l'e-mail.
   d (Facultatif) Indiquez si vous souhaitez envoyer des notifications à tous les administrateurs de l'organisation ou à des adresses e-mail spécifiques.
   e (Facultatif) Si vous choisissez d'envoyer des notifications à des adresses e-mail spécifiques, entrez les adresses e-mail en les séparant par une virgule.
6 Cliquez sur **Enregistrer**.

Tester les paramètres SMTP

Après avoir modifié les paramètres de messagerie de votre organisation, vous pouvez tester les paramètres SMTP.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1 Dans le menu principal (☰), sélectionnez **Administration**.
2 Sous **Paramètres**, cliquez sur **E-mail**.

   Les paramètres de messagerie de votre organisation s'affichent.
3 Cliquez sur **Tester**.
4 Entrez une adresse e-mail de destination et le mot de passe du serveur SMTP pour tester les paramètres SMTP, puis cliquez sur le bouton **Tester**.

Modifier les paramètres de domaine des machines virtuelles de votre organisation

Vous pouvez définir un domaine Windows par défaut que les machines virtuelles créées dans votre organisation peuvent joindre. Des machines virtuelles peuvent toujours joindre un domaine pour lequel elles possèdent des identifiants, que vous spécifiiez ou non un domaine par défaut.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Sous **Paramètres**, cliquez sur **Personnalisation invité**.

3 Sélectionnez l'activation de la jonction de domaine des machines virtuelles de l'organisation.

4 Entrez le nom de domaine, le nom d'utilisateur et le mot de passe.

   Les informations d'identification que vous entrez s'appliquent à un utilisateur de domaine régulier, pas à un administrateur de domaine.

5 (Facultatif) Entrez une unité d'organisation de compte.

6 Cliquez sur **Enregistrer**.

Utilisation sur plusieurs sites

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.

Le portail de locataires de vCloud Director fournit aux **administrateurs d'organisation** un moyen d'associer des organisations à des sites associés.

Pour plus d'informations sur les associations de sites, reportez-vous au *Guide du portail d'administration des fournisseurs de services vCloud Director*.

Configurer et gérer les déploiements multisite

Après qu'un **administrateur système** a associé deux sites, les **administrateurs d'organisation** de n'importe quel site membre peuvent commencer à associer leurs organisations.

Pour créer une association entre deux organisations (appelées ici Org-A et Org-B), vous devez être **administrateur d'organisation** des deux organisations pour pouvoir vous connecter à une organisation, récupérer ses données d'association locale et envoyer les données récupérées à l'autre organisation.

Important Le processus d'association de deux organisations peut être décomposé logiquement en deux opérations de couplage complémentaires. La première opération (dans cet exemple) couple Org-A sur Site-A avec Org-B sur Site-B. Vous devez ensuite coupler Org-B sur Site-B avec Org-A sur Site-A. L'association est incomplète tant que les deux couplages ne sont pas terminés.

Conditions préalables

- Les sites occupés par les organisations doivent être associés.
- Vous devez être **administrateur système** des deux sites ou **administrateur d'organisation** des deux organisations.

Procédure

1 Connectez-vous au portail de locataires de vCloud Director de Org-A sur Site-A pour récupérer ses données d'association locale.

   a Cliquez sur **Administration**.

   b Sous **Paramètres**, cliquez sur **Multisite**.

   c Pour télécharger les données au format XML, cliquez sur **Exporter des données d'association locale**.

   Le navigateur enregistre les données dans un fichier dans son dossier Téléchargements.

2 Connectez-vous au portail de locataires de vCloud Director de Org-B au Site-B pour envoyer les données d'association locale de Org-A au Site-A.

   a Cliquez sur **Administration**.

   b Sous **Paramètres**, cliquez sur **Multisite**.

   c Cliquez sur **Créer une association d'organisation**.

   Envoyez les données d'association que vous avez téléchargées à l'étape 1 vers Org-B en cliquant sur la flèche de téléchargement située au-dessous de la zone de texte **Fichier XML de la nouvelle association** et en sélectionnant les données d'association locale que vous avez téléchargées à l'étape 1.

   d Cliquez sur **Suivant** pour vérifier et envoyer les données.

   Le système couple Org-A au Site-A avec Org-B au Site-B.

   e Cliquez sur **Terminer** pour afficher l'organisation associée.

   f Pour afficher les détails de l'organisation associée ou supprimer l'association, cliquez sur la carte **Nom de l'organisation**.

3 Terminer l'association en répétant l'étape 1 et l'étape 2 pour récupérer les données d'association locale de Org-B et de les envoyer à Org-A.

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 d'utiliser 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 le supprime, en fonction de la stratégie d'organisation que vous définissez.

Modifier les stratégies vApp et Bail de modèle de vApp au sein de votre organisation

Vous pouvez passer en revue et modifier les stratégies par défaut qui ont été définies par l'administrateur système lors de la création de votre organisation.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Sous **Paramètres**, cliquez sur **Stratégies**.

   Vous pouvez afficher les stratégies par défaut que votre administrateur système a définies.
3. Cliquez sur **Modifier**.
4. Modifiez les baux de vApp.

   Les baux de vApp fournissent un certain niveau de contrôle sur les ressources de stockage et de calcul de l'organisation en spécifiant le temps d'exécution et de stockage maximal des vApp. Vous pouvez également spécifier le traitement appliqué aux vApp lors de l'expiration de leur bail de stockage.
   a. Entrez la durée maximale du bail d'exécution pour définir le temps d'exécution des vApp avant leur arrêt automatique.
   b. Sélectionnez l'action à effectuer en cas d'expiration de l'exécution, comme la mise hors tension ou l'interruption.
   c. Entrez le bail de stockage maximal pour définir la durée pendant laquelle les vApp arrêtés restent disponibles avant le nettoyage automatique.
   d. Sélectionnez une action de nettoyage du stockage telle que la suppression permanente des vApp ou leur déplacement vers les éléments ayant expirés.

5 Modifiez le bail de modèle de vApp.

Les baux de modèle de vApp fournissent un certain niveau de contrôle sur les ressources de stockage et de calcul de l'organisation en spécifiant le temps de stockage maximal des modèles de vApp. Vous pouvez également spécifier le traitement appliqué aux modèles de vApp lors de l'expiration de leur bail de stockage.

a Entrez le bail de stockage maximal pour définir la durée pendant laquelle les modèles de vApp arrêtés restent disponibles avant le nettoyage automatique.

b Sélectionnez une action de nettoyage du stockage telle que la suppression permanente des modèles de vApp ou leur déplacement vers les éléments ayant expirés.

6 Cliquez sur **OK**.

Modifier les quotas par défaut des machines virtuelles de votre organisation

Vous pouvez vérifier et modifier les stratégies de quota par défaut qui ont été définies par l'administrateur système lors de la création de votre organisation.

Les quotas déterminent le nombre de machines virtuelles que chaque utilisateur au sein de l'organisation peut stocker et mettre sous tension dans les centres de données virtuels de l'organisation. Les quotas que vous spécifiez agissent comme valeurs par défaut pour l'ensemble des nouveaux utilisateurs ajoutés à l'organisation. Les quotas définis au niveau de l'utilisateur sont prioritaires par rapport à ceux définis au niveau de l'organisation.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

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

2 Sous **Paramètres**, cliquez sur **Stratégies**.

Vous pouvez afficher les stratégies par défaut que votre administrateur système a définies.

3 Cliquez sur **Modifier**.

4 Choisissez entre un nombre illimité et un nombre spécifique de machines virtuelles.

5 Choisissez entre un nombre illimité et un nombre spécifique de machines virtuelles sous tension.

6 Cliquez sur **OK**.

Modifier les stratégies de mot de passe et de compte d'utilisateur au sein de votre organisation

Vous pouvez vérifier et modifier les stratégies de mot de passe et de compte d'utilisateur par défaut qui ont été définies par l'administrateur système lors de la création de votre organisation.

Les stratégies de mot de passe et de compte d'utilisateur définissent le comportement de vCloud Director lorsqu'un utilisateur entre un mot de passe non valide.

Conditions préalables

Cette opération nécessite les droits inclus dans le rôle prédéfini **Administrateur d'organisation** ou un ensemble de droits équivalent.

Procédure

1. Dans le menu principal (☰), sélectionnez **Administration**.
2. Sous **Paramètres**, cliquez sur **Stratégies**.

   Vous pouvez afficher les stratégies par défaut que votre administrateur système a définies.
3. Cliquez sur **Modifier**.
4. Activer le verrouillage d'un compte d'utilisateur après plusieurs tentatives de connexion non valides.
5. Entrez le nombre de tentatives de connexion non valides avant que le compte ne soit verrouillé.
6. Entrez l'intervalle de temps, en minutes, pendant lequel l'utilisateur dont le compte est verrouillé ne peut pas se reconnecter.
7. Cliquez sur **OK**.

Utilisation de la bibliothèque de services

18

Les éléments de la bibliothèque de services de vCloud Director sont des workflows vRealize Orchestrator qui étendent les capacités de gestion de cloud et permettent aux administrateurs des fournisseurs ou des locataires de surveiller et de manipuler différents services.

Ce chapitre contient les rubriques suivantes :

- Rechercher un service
- Exécuter un service

Rechercher un service

La page **Bibliothèque de services** dans le portail de locataires de vCloud Director répertorie l'ensemble des workflows vRealize Orchestrator qui sont importés dans vCloud Director et publiés dans votre organisation.

Conditions préalables

Cette opération nécessite que les droits de la bibliothèque de services soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, sélectionnez **Bibliothèque de services**.

   La liste des éléments de service s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche comporte le nom du service et une balise qui correspond à la catégorie de service dans laquelle l'instance de vRealize Orchestrator est importée.

2. Dans la zone de texte **Rechercher** en haut de la page, entrez le premier mot du nom du service ou du nom de la catégorie à laquelle appartient le service.

   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 carte comportant douze éléments par page, triés par nom dans l'ordre alphabétique.

Exécuter un service

Vous pouvez exécuter un service à partir de la page Bibliothèque de services dans le portail de locataires de vCloud Director.

Conditions préalables

Cette opération nécessite que les droits de la bibliothèque de services soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, sélectionnez **Bibliothèque de services**.

   La liste des éléments de service s'affiche dans une vue de carte composée de douze éléments par page, triés par nom dans l'ordre alphabétique. Chaque fiche comporte le nom du service et une balise qui correspond à la catégorie de service dans laquelle l'instance de vRealize Orchestrator est importée.
2. Recherchez le service que vous souhaitez exécuter.
3. Cliquez sur **Exécuter** sur la fiche du service.

   Une nouvelle boîte de dialogue s'ouvre. Vous devez entrer des valeurs pour les paramètres d'entrée requis du service.
4. Cliquez sur **Terminer** pour confirmer l'exécution du service.

Étape suivante

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.

Utilisation des définitions d'entités personnalisées

19

Les définitions d'entités personnalisées de vCloud Director sont des types d'objets liés aux types d'objets vRealize Orchestrator. Les utilisateurs au sein d'une organisation vCloud Director peuvent posséder, gérer et modifier ces types en fonction de leurs besoins. En exécutant des services, 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 d'une définition d'entité personnalisée
- Publier une entité personnalisée
- Supprimer une entité personnalisée

Rechercher une entité personnalisée

Vous pouvez rechercher les entités personnalisées qui ont été publiées dans votre organisation.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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 de l'objet vRealize Orchestrator auquel l'entité est liée, car ce sont les 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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 > Host**. 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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 d'une définition d'entité personnalisée

Vous pouvez supprimer un workflow vRealize Orchestrator de la liste des actions associées.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1 Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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 publiez 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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.

Conditions préalables

Cette opération nécessite que les droits de l'entité personnalisée soient inclus dans le rôle d'utilisateur prédéfini.

Procédure

1. Dans le menu principal (☰), sélectionnez **Bibliothèques**, puis, sous **Services**, 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.