Guide de l'opérateur de VMware SD-WAN

2020

VMware SD-WAN 4.1

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

Table des matières

À propos du Guide de l'opérateur de VMware

1

Le Guide de l'opérateur de VMware SD-WAN™ fournit des informations sur VMware SD-WAN Orchestrator, notamment sur la configuration et la gestion des clients et des partenaires qui utilisent Orchestrator.

Public visé

Ce guide est destiné aux opérateurs et aux fournisseurs de services qui maîtrisent les opérations SD-WAN et de mise en réseau.

Présentation de VMware SD-WAN Orchestrator

2

VMware SD-WAN Orchestrator fournit l'installation, la configuration et la surveillance en temps réel centralisées à l'échelle de l'entreprise, en plus de l'orchestration du flux de données via le réseau cloud.

SD-WAN Orchestrator est disponible en tant qu'interface utilisateur Web, dans laquelle vous pouvez configurer et gérer les éléments suivants :

- Clients (Customers)
- Partenaires
- Utilisateurs opérateurs (Operator Users)
- Passerelles et pools de passerelles
- Modes d'authentification d'Orchestrator

Navigateurs pris en charge

3

SD-WAN Orchestrator prend en charge les navigateurs suivants :

Navigateurs qualifiés	Version du navigateur
Google Chrome	77 - 79.0.3945.130
Mozilla Firefox	69.0.2 - 72.0.2
Microsoft Edge	42.17134.1.0 - 44.18362.449.0
Apple Safari	12.1.2 - 13.0.3

Note Pour une expérience optimale, VMware recommande Google Chrome ou Mozilla Firefox.

Note À partir de VMware SD-WAN version 4.0.0, la prise en charge d'Internet Explorer est obsolète.

Nouveautés

4

Nouveautés de la version 4.1.0

Fonctionnalité	Description
VMware Edge Network Intelligence	VMware Edge Network Intelligence est une solution AIOps indépendante du fournisseur et axée sur le dispositif Edge d'entreprise, qui garantit les performances du client pour l'utilisateur final et l'Internet des objets (IoT), la sécurité, la réparation spontanée au moyen d'un réseau LAN filaire et sans fil, SD-WAN et SASE (Secure Access service Edge). L'intégration de l'intelligence réseau Edge à VMware permet d'étendre la visibilité du SD-WAN à la branche, au campus et à la maison. Pour comprendre le fonctionnement d'Edge Network Intelligence, reportez-vous au *Guide de l'utilisateur de VMware Edge Network Intelligence* disponible à l'adresse https://docs.vmware.com/fr/VMware-Edge-Network-Intelligence/index.html. Lors de la création d'un client SD-WAN (entreprise ou partenaire), VMware SD-WAN Orchestrator autorise les super utilisateurs opérateurs, les administrateurs opérateurs standard, les super utilisateurs partenaires et les administrateurs partenaires standard à activer la fonctionnalité d'analyse du client. Pour connaître les étapes, consultez les sections suivantes : ■ Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator ■ Activer l'analyse pour un nouveau client ■ Activer l'analyse d'un client existant **Note** Pour plus d'informations sur la configuration de VMware Edge Network Intelligence, reportez-vous au *Guide de configuration de VMware Edge Network Intelligence* disponible à l'adresse https://docs.vmware.com/fr/VMware-SD-WAN-by-VeloCloud/index.html.

Versions précédentes de VMware

Pour obtenir de la documentation sur le produit pour les versions précédentes de VMware, contactez votre représentant VMware.

Installer SD-WAN Orchestrator 5

Cette section décrit l'installation de SD-WAN Orchestrator.

Ce chapitre contient les rubriques suivantes :

Conditions préalables

Cette section décrit les conditions préalables à remplir avant l'installation de SD-WAN Orchestrator.

Conditions préalables de l'instance

VMware recommande d'installer les applications Orchestrator et Gateway en tant que machine virtuelle (par exemple, instance d'invité) sur un hyperviseur existant.

SD-WAN Orchestrator nécessite les spécifications minimales de l'instance d'invité suivantes :

- 8 vCPU Intel à 2,5 GHz au minimum
- 16 Go de mémoire

  Note SD-WAN Orchestrator ne démarre pas avec moins de 10 Go de mémoire.

- 2 volumes persistants basés sur SSD de 1 To x 1 de 512 Go (extensible via LVM si nécessaire)
  - Nombre minimal d'IOPS : 5 000 IOPS
- Carte réseau de 1 Gbit/s
- Compatibilité de VM du serveur Ubuntu x64
- Adresse IP publique unique (disponibilité possible via NAT)

Configuration du pare-feu montant

Le pare-feu montant doit être configuré pour autoriser l'accès entrant HTTP (TCP/80) et HTTPS (TCP/443). Si un pare-feu avec état est en place, les connexions établies sortantes doivent également être autorisées afin de faciliter les mises à niveau et les mises à jour de sécurité.

Services externes

SD-WAN Orchestrator repose sur plusieurs services externes. Avant de procéder à une installation, vérifiez que les licences sont disponibles pour chacun des services.

Google Maps

Google Maps permet d'afficher des dispositifs Edge et des centres de données sur une carte. Pour utiliser cette fonctionnalité, il n'est pas nécessaire de créer un compte avec Google. Toutefois, l'accès à Internet doit être disponible pour l'instance de SD-WAN Orchestrator afin que le service soit disponible.

Le service est limité à 25 000 charges de carte chaque jour, pendant plus de 90 jours consécutifs. VMware ne prévoit pas de dépasser ces limites pour une utilisation nominale de SD-WAN Orchestrator. Pour plus d'informations, reportez-vous à la section Google Maps.

Twilio

Twilio est utilisé pour les alertes par SMS transmises aux clients d'entreprise afin de les informer des événements de pannes Edge ou de liaison. Vous devez créer un compte et l'approvisionner à l'adresse http://www.twilio.com .

Vous pouvez provisionner le compte dans SD-WAN Orchestrator via la page **Propriétés système (System Properties)** du portail opérateur. Le compte sera provisionné via une propriété système, comme décrit plus loin dans le guide. Pour plus d'informations, reportez-vous à la section Twilio.

MaxMind

MaxMind est un service de géolocalisation. Il permet de détecter automatiquement les emplacements d'Edge et de passerelle, ainsi que les noms de fournisseurs de services selon l'adresse IP. Si ce service est désactivé, vous devez mettre à jour manuellement les informations de géolocalisation. Vous pouvez provisionner le compte dans SD-WAN Orchestrator via la page **Propriétés système (System Properties)** du portail opérateur. Pour plus d'informations, reportez-vous à la section MaxMind.

Procédures d'installation

Cette section décrit l'installation.

Préparation de cloud-init

Cette section décrit comment utiliser le module cloud-init pour gérer l'initialisation précoce des instances.

À propos de cloud-init

Cloud-init est un module Linux responsable de la gestion de l'initialisation précoce des instances. S'il est disponible dans les distributions, il permet la configuration de nombreux paramètres communs de l'instance directement après l'installation. Cela crée une instance entièrement fonctionnelle configurée en fonction d'une série d'entrées.

Vous pouvez configurer le comportement de cloud-init via user-data. L'utilisateur peut fournir la valeur user-data au moment du lancement de l'instance. Pour ce faire, attachez un disque secondaire au format ISO que cloud-init recherche au premier démarrage. Ce disque contient toutes les données de configuration initiale qui sont appliquées à ce moment-là.

SD-WAN Orchestrator prend en charge cloud-init et toutes les configurations essentielles peuvent être packagées dans une image ISO.

Créer le fichier meta-data de cloud-init

Les options de configuration de l'installation finale sont définies à l'aide d'une paire de fichiers de configuration de cloud-init. Le premier fichier de configuration de l'installation contient les métadonnées. Créez ce fichier à l'aide d'un éditeur de texte et nommez-le `meta-data`. Ce fichier fournit des informations qui identifient l'instance de SD-WAN Orchestrator en cours d'installation. La valeur `instance-id` peut être n'importe quel nom d'identification et `local-hostname` doit être un nom d'hôte conforme aux normes de votre site, par exemple :

```
instance-id: vco01
local-hostname: vco-01
```

En outre, vous pouvez spécifier des informations sur l'interface réseau (si le réseau n'est pas configuré via DHCP, par exemple) :

```
instance-id: vco01
local-hostname: vco-01
network-interfaces: |
  auto eth0
  iface eth0 inet static
  address 10.0.1.2
  network 10.0.1.0
  netmask 255.255.255.0
  broadcast 10.0.1.255
  gateway 10.0.1.1
```

Créer le fichier user-data de cloud-init

Le second fichier d'options de configuration de l'installation est le fichier user-data. Ce fichier fournit des informations sur les utilisateurs du système. Créez-le à l'aide d'un éditeur de texte et appelez-le `user-data`. Ce fichier est utilisé pour permettre l'accès à l'installation de SD-WAN Orchestrator. Vous trouverez ci-après un exemple de l'apparence du fichier `user-data` :

```
#cloud-config
            password: Velocloud123
            chpasswd: {expire: False}
```

```
            ssh_pwauth: True
            ssh_authorized_keys:
              - ssh-rsa AAA...SDvz user1@yourdomain.com
              - ssh-rsa AAB...QTuo user2@yourdomain.com
            vco:
              super_users:
                list: |
                  user1@yourdomain.com:password1
                remove_default_users: True
              system_properties:
                 list: |
                    mail.smtp.port:34
                    mail.smtp.host:smtp.yourdomain.com
                    service.maxmind.enable:True
                    service.maxmind.license:todo_license
                    service.maxmind.userid:todo_user
                    service.twilio.phoneNumber:222123123
                    network.public.address:222123123
            write_files:
               - path: /etc/nginx/velocloud/ssl/server.crt
                 permissions: '0644'
                 content: "-----BEGIN CERTIFICATE-----\nMI….ow==\n-----END CERTIFICATE-----\n"
               - path: /etc/nginx/velocloud/ssl/server.key
                 permissions: '0600'
                 content: "-----BEGIN RSA PRIVATE KEY-----\nMII...D/JQ==\n-----END RSA
PRIVATE KEY-----\n"
               - path: /etc/nginx/velocloud/ssl/velocloudCA.crt
```

Ce fichier `user-data` active l'utilisateur par défaut, vcadmin, pour qu'il se connecte avec un mot de passe ou une clé SSH. L'utilisation des deux méthodes est possible, mais n'est pas nécessaire. La connexion par mot de passe est activée par les lignes `password` et `chpasswd`.

- La valeur `password` contient le mot de passe en texte brut de l'utilisateur vcadmin.
- La ligne `chpasswd` désactive l'expiration du mot de passe pour éviter que la première connexion demande immédiatement une modification du mot de passe. Cela est facultatif.

Note Si vous avez défini un mot de passe, il est recommandé de le modifier lors de votre première connexion, car le mot de passe a été stocké dans un fichier texte brut.

La ligne `ssh_pwauth` active la connexion SSH. La ligne `ssh_authorized_keys` commence un bloc d'une ou de plusieurs clés autorisées. Chaque clé SSH publique répertoriée sur les lignes `ssh-rsa` est ajoutée au fichier `~/.ssh/authorized_keys` de vcadmin.

Dans cet exemple, deux clés sont répertoriées. Dans cet exemple, la clé a été tronquée. Dans un fichier réel, la clé publique complète doit être répertoriée. Notez que les lignes `ssh-rsa` doivent être précédées de deux espaces, suivis d'un trait d'union, puis d'un autre espace.

La section `vco` spécifie les services de SD-WAN Orchestrator configurés.

`super_users` contient la liste des comptes de super opérateur de VMware et les mots de passe correspondants.

La section `system_properties` permet de personnaliser les propriétés système d'Orchestrator. Pour plus d'informations sur la configuration des propriétés système, reportez-vous à la section Chapitre 11 Propriétés système.

La section `write_files` permet de remplacer des fichiers sur le système. Par défaut, les services Web de SD-WAN Orchestrator sont configurés à l'aide d'un certificat SSL auto-signé. Pour fournir un autre certificat SSL, l'exemple ci-dessus remplace les fichiers `server.crt` et `server.key` dans le dossier `/etc/nginx/velocloud/ssl/` par des fichiers fournis par l'utilisateur.

Note Le fichier `server.key` doit être non chiffré. Dans le cas contraire, le service ne peut pas démarrer sans le mot de passe de la clé.

Créer un fichier ISO

Après avoir terminé vos fichiers, vous devez les packager dans une image ISO. Cette image ISO est utilisée comme CD de configuration virtuel avec la machine virtuelle. Cette image ISO, appelée `vco01-cidata.iso`, est créée à l'aide de la commande suivante sur un système Linux :

```
genisoimage -output vco01-cidata.iso -volid cidata -joliet -rock user-data meta-data
```

Transférez l'image ISO récemment créée dans la banque de données sur l'hôte exécutant VMware.

Installer sur VMware

VMware vSphere fournit un moyen de déployer et de gérer des ressources de machine virtuelle. Cette section explique comment exécuter l'instance de SD-WAN Orchestrator à l'aide de VMware vSphere Client.

Déployer le modèle OVA

Note Cette procédure suppose que vous connaissez VMware vSphere et n'est pas écrite pour une version spécifique de VMware vSphere.

1 Connectez-vous à vSphere Client.

2 Sélectionnez **Fichier (File) > Déployer le modèle OVF (Deploy OVF Template)**.

3 Répondez aux invites en indiquant des informations spécifiques à votre déploiement.

Champ	Description
Source	Tapez une URL ou accédez à l'emplacement du module OVA.
Détails du modèle OVF (OVF template details)	Vérifiez que vous avez désigné le modèle OVA correct pour cette installation.
Nom et emplacement (Name and location)	Nom de la machine virtuelle.
Stockage	Sélectionnez l'emplacement dans lequel stocker les fichiers de la machine virtuelle.

Champ	Description
Provisionnement (Provisioning)	Sélectionnez le type de provisionnement. Le type « dynamique » (thin) est recommandé pour la base de données et les volumes de journaux binaires.
Mappage réseau (Network mapping)	Sélectionnez le réseau pour chaque machine virtuelle à utiliser. **Important** Décochez **Mettre sous tension après le déploiement (Power On After Deployment)**. Si vous sélectionnez cette option, la machine virtuelle démarre et devra être démarrée ultérieurement après l'attachement de l'image ISO cloud-init.

4 Cliquez sur **Terminer (Finish)**.

Note En fonction de la vitesse de votre réseau, ce déploiement peut prendre plusieurs minutes.

Attacher l'image ISO en tant que CD/DVD à la machine virtuelle

1 Cliquez avec le bouton droit sur la machine virtuelle SD-WAN Orchestrator récemment ajoutée et sélectionnez **Modifier les paramètres (Edit Settings)**.

2 Dans la fenêtre **Propriétés de la machine virtuelle (Virtual Machine Properties)**, sélectionnez **Lecteur de CD/DVD (CD/DVD Drive)**.

3 Sélectionnez l'option **Utiliser une image ISO (Use an ISO image)**.

4 Naviguez pour trouver l'image ISO que vous avez précédemment créée (nommée `vco01-cidata.iso` dans ce document), puis sélectionnez-la. L'image ISO est disponible dans la banque de données vers laquelle vous l'avez chargée, dans le dossier que vous avez créé.

5 Sélectionnez **Se connecter lors de la mise sous tension (Connect on Power On)**.

6 Cliquez sur **OK** pour quitter l'écran **Propriétés (Properties)**.

Exécuter la machine virtuelle SD-WAN Orchestrator

Pour démarrer la machine virtuelle SD-WAN Orchestrator :

1 Cliquez sur la machine virtuelle pour la mettre en surbrillance, puis sélectionnez le bouton **Mettre sous tension (Power On)**.

2 Sélectionnez l'onglet **Console** pour surveiller le démarrage de la machine virtuelle.

Note Si vous avez configuré SD-WAN Orchestrator comme décrit dans ce document, vous devriez pouvoir vous connecter à la machine virtuelle à l'aide du nom d'utilisateur vcadmin et du mot de passe que vous avez définis lors de la création de l'image ISO cloud-init.

Installer sur KVM

Cette section explique comment exécuter SD-WAN Orchestrator à l'aide de libvirt. Ce déploiement a été testé dans Ubuntu 18.04 LTS.

Images

Pour le déploiement sur KVM, VMware fournit SD-WAN Orchestrator dans quatre images qcow.

- ROOTFS
- STORE
- STORE2
- STORE3

Les images sont provisionnées dynamiquement lors du déploiement.

Commencez par copier les images sur le serveur KVM. En outre, vous devez copier la build ISO cloud-init, comme décrit dans la section précédente.

Exemple XML

Note Pour les images du dossier `images/vco`, vous devez effectuer les modifications à partir du fichier XML.

```
<domain type='kvm' id='49'>
  <name>vco</name>
  <uuid>b0ff25bc-72b8-6ccb-e777-fdc0f4733e05</uuid>
  <memory unit='KiB'>12388608</memory>
  <currentMemory unit='KiB'>12388608</currentMemory>
  <vcpu>2</vcpu>
  <resource>
    <partition>/machine</partition>
  </resource>
  <os>
  <type>hvm</type>
  </os>
  <features>
    <acpi/>
    <apic/>
    <pae/>
  </features>
    <cpu mode='custom' match='exact'>
    <model fallback='allow'>SandyBridge</model>
    <vendor>Intel</vendor>
    <feature policy='require' name='vme'/>
    <feature policy='require' name='dtes64'/>
    <feature policy='require' name='invpcid'/>
    <feature policy='require' name='vmx'/>
    <feature policy='require' name='erms'/>
    <feature policy='require' name='xtpr'/>
    <feature policy='require' name='smep'/>
    <feature policy='require' name='pbe'/>
    <feature policy='require' name='est'/>
    <feature policy='require' name='monitor'/>
    <feature policy='require' name='smx'/>
    <feature policy='require' name='abm'/>
    <feature policy='require' name='tm'/>
```

```
    <feature policy='require' name='acpi'/>
    <feature policy='require' name='fma'/>
    <feature policy='require' name='osxsave'/>
    <feature policy='require' name='ht'/>
    <feature policy='require' name='dca'/>
    <feature policy='require' name='pdcm'/>
    <feature policy='require' name='pdpe1gb'/>
    <feature policy='require' name='fsgsbase'/>
    <feature policy='require' name='f16c'/>
    <feature policy='require' name='ds'/>
    <feature policy='require' name='tm2'/>
    <feature policy='require' name='avx2'/>
    <feature policy='require' name='ss'/>
    <feature policy='require' name='bmi1'/>
    <feature policy='require' name='bmi2'/>
    <feature policy='require' name='pcid'/>
    <feature policy='require' name='ds_cpl'/>
    <feature policy='require' name='movbe'/>
    <feature policy='require' name='rdrand'/>
  </cpu>
<clock offset='utc'/>
  <on_poweroff>destroy</on_poweroff>
  <on_reboot>restart</on_reboot>
  <on_crash>restart</on_crash>
  <devices>
    <emulator>/usr/bin/kvm-spice</emulator>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/images/vco/rootfs.qcow2'/>
      <target dev='hda' bus='ide'/>
      <alias name='ide0-0-0'/>
      <address type='drive' controller='0' bus='0' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/ images/vco/store.qcow2'/>
      <target dev='hdb' bus='ide'/>
      <alias name='ide0-0-1'/>
      <address type='drive' controller='0' bus='0' target='0' unit='1'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2'/>
      <source file='/ images/vco/store2.qcow2'/>
      <target dev='hdc' bus='ide'/>
      <alias name='ide0-0-2'/>
      <address type='drive' controller='0' bus='1' target='0' unit='0'/>
    </disk>
    <disk type='file' device='disk'>
      <driver name='qemu' type='qcow2' />
      <source file='/images/vco/store3.qcow2' />
      <target dev='hdd' bus='ide' />
      <alias name='ide0-0-3' />
      <address type='drive' controller='0' bus='1' target='0' unit='1' />
    </disk>
    <disk type='file' device='cdrom'>
```

```
      <driver name='qemu' type='raw'/>
      <source file='/ images/vco/seed.iso'/>
      <target dev='sdb' bus='sata'/>
      <readonly/>
      <alias name='sata1-0-0'/>
      <address type='drive' controller='1' bus='0' target='0' unit='0'/>
    </disk>
    <controller type='usb' index='0'>
      <alias name='usb0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x2'/>
    </controller>
    <controller type='pci' index='0' model='pci-root'>
      <alias name='pci.0'/>
    </controller>
    <controller type='ide' index='0'>
      <alias name='ide0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x01' function='0x1'/>
    </controller>
    <interface type='direct'>
      <source dev='eth0' mode='vepa'/>
    </interface>
    <serial type='pty'>
      <source path='/dev/pts/3'/>
      <target port='0'/>
      <alias name='serial0'/>
    </serial>
    <console type='pty' tty='/dev/pts/3'>
      <source path='/dev/pts/3'/>
      <target type='serial' port='0'/>
      <alias name='serial0'/>
    </console>
    <memballoon model='virtio'>
      <alias name='balloon0'/>
      <address type='pci' domain='0x0000' bus='0x00' slot='0x03' function='0x0'/>
    </memballoon>
  </devices>
  <seclabel type='none' />
<!--  <seclabel type='dynamic' model='apparmor' relabel='yes'/> -->
</domain>
```

Créer la machine virtuelle

Pour créer la machine virtuelle à l'aide des commandes virsh standard :

```
virsh define vco.xml
virsh start vco.xml
```

Installer sur AWS

Cette section décrit comment installer SD-WAN Orchestrator sur AWS.

Conditions préalables minimales de l'instance

Reportez-vous à la première section de l'installation de SD-WAN Orchestrator, intitulée Conditions préalables de l'instance et sélectionnez un type d'instance AWS correspondant à ces conditions préalables. Les conditions préalables du CPU et de la mémoire doivent être remplies. Exemple : utilisez l'instance c4.2xlarge au minimum ; instance r4.2xlarge au minimum

Demander une image AMI

Demandez un ID AMI à partir de VMware. Il est partagé avec le compte client. Préparez un ID de compte Amazon AWS lors de la demande d'accès AMI.

Installation

1 Lancez l'instance EC2 dans le cloud AWS.

Exemple : http://docs.aws.amazon.com/efs/latest/ug/gs-step-one-create-ec2-resources.html

2 Configurez le groupe de sécurité pour autoriser le protocole HTTP entrant (TCP/80) ainsi que le protocole HTTPS (TCP/443).

3 Après le lancement de l'instance, pointez le navigateur Web sur l'URL de connexion de l'opérateur :

`https://<name>/operator`

Tâches de configuration initiale

Effectuez les tâches de configuration initiale suivantes :

- Configurer les propriétés système
- Configurer le profil d'opérateur initial
- Configurer les comptes d'opérateur
- Créer des passerelles
- Configurer les pools de passerelle
- Créer un compte client/compte de partenaire

Installer un certificat SSL

Cette section décrit comment installer un certificat SSL.

Pour installer un certificat SSL :

1 Connectez-vous à la console de l'interface de ligne de commande (CLI) de SD-WAN Orchestrator via SSH. Si vous avez configuré SD-WAN Orchestrator comme indiqué ici, vous devez pouvoir vous connecter à la machine virtuelle avec le nom d'utilisateur `vcadmin` et le mot de passe que vous avez définis lors de la création de l'image ISO de cloud-init.

2 Générez la clé privée de SD-WAN Orchestrator.

Note Ne chiffrez pas la clé. Elle doit rester non chiffrée sur le système SD-WAN Orchestrator.

```
openssl genrsa -out server.key 2048
```

3 Générez une demande de certificat. Personnalisez `-subj` en fonction des informations de votre organisation.

```
openssl req -new -key server.key -out
server.csr -subj "/C=US/ST=California/L=Mountain View/O=Velocloud Networks
Inc./OU=Development/CN=vco.velocloud.net"
```

Description des champs Sujet (Subject) :

Champ	Description
C	pays
ST	état
L	localité (ville)
O	société
OU	département (facultatif)
CN	nom de domaine complet de SD-WAN Orchestrator

4 Envoyez `server.csr` à une autorité de certification pour la signature. Vous devez récupérer le certificat SSL (`server.crt`). Vérifiez qu'il est au format PEM.

5 Installez le certificat (qui nécessite un accès racine). Les certificats SSL de SD-WAN Orchestrator se trouvent dans `/etc/nginx/velocloud/ssl/`.

```
cp server.key server.crt /etc/nginx/velocloud/ssl/
chmod 600 /etc/nginx/velocloud/ssl/server.key
```

6 Redémarrez nginx.

```
systemctl restart nginx
```

Configurer les propriétés système

Cette section décrit comment configurer les propriétés système, qui fournissent un mécanisme permettant de contrôler le comportement à l'échelle du système de VMware.

Vous pouvez définir initialement les propriétés système à l'aide du fichier de configuration cloud-init (reportez-vous à la section *Créer le fichier meta-data de cloud-init*). Vous devez configurer les propriétés suivantes afin de garantir le bon fonctionnement du service.

Nom du système

Entrez un nom de domaine complet de VMware dans la propriété système `network.public.address`.

Google Maps

Google Maps permet d'afficher des dispositifs Edge et des centres de données sur une carte. Les cartes peuvent ne pas s'afficher sans clé de licence. Orchestrator continue à fonctionner correctement, mais les cartes de navigateur ne sont pas disponibles dans ce cas.

1 Connectez-vous à https://console.developers.google.com.

2 Créez un projet, s'il n'est pas déjà créé.

3 Localisez le bouton **Activer l'API (Enable API)**. Cliquez sous les **API Google Maps (Google Maps APIs)** et activez l'**API JavaScript de Google Maps (Google Maps JavaScript API)** et l'**API de géolocalisation de Google Maps (Google Maps Geolocation API)**.

4 Dans la partie gauche de l'écran, cliquez sur le lien **Informations d'identification (Credentials)**.

5 Sous la page informations d'identification (Credentials), cliquez sur **Créer des informations d'identification (Create Credentials)**, puis sélectionnez **Clé API (API key)**. Créez une clé API.

6 Définissez la propriété système `service.client.googleMapsApi.key` VMware sur la clé API.

7 Définissez `service.client.googleMapsApi.enable` sur « true »

Twilio

Twilio est un service de messagerie qui permet de recevoir des alertes de VMware par SMS. Il est facultatif. Vous pouvez entrer les détails du compte dans VMware via la page **Propriétés système (System Properties)** du portail opérateur. Les propriétés sont appelées :

- `service.twilio.enable` autorise la désactivation du service dans l'éventualité où aucun accès Internet n'est disponible pour VMware
- `service.twilio.accountSid`
- `service.twilio.authToken`
- `service.twilio.phoneNumber` au format `(nnn)nnn-nnnn`

Procurez-vous le service à l'adresse https://www.twilio.com.

MaxMind

MaxMind est un service de géolocalisation. Il permet de détecter automatiquement les emplacements d'Edge et de la passerelle, ainsi que les noms de fournisseurs de services selon une adresse IP. Si ce service est désactivé, vous devez mettre à jour manuellement les informations de géolocalisation. Vous pouvez entrer les détails du compte dans VMware via la page **Propriétés système (System Properties)** du portail opérateur. Vous pouvez configurer les éléments suivants :

- `service.maxmind.enable` autorise la désactivation du service dans l'éventualité où aucun accès Internet n'est disponible pour VMware

- `service.maxmind.userid` conserve l'identification d'utilisateur fournie par MaxMind lors de la création du compte
- `service.maxmind.license` conserve la clé de licence fournie par MaxMind

Procurez-vous la licence à l'adresse : https://www.maxmind.com/fr/geoip2-precision-city-service.

E-mail

Vous pouvez utiliser les services de messagerie pour l'envoi des messages d'activation Edge, ainsi que pour les alarmes et les notifications. Il n'est pas obligatoire, mais fortement recommandé de le configurer dans le cadre des opérations de VMware. Les propriétés système suivantes sont disponibles pour configurer le service de messagerie externe utilisé par Orchestrator :

- `mail.smtp.auth.pass` : mot de passe de l'utilisateur SMTP.
- `mail.smtp.auth.user` : utilisateur SMTP pour l'authentification.
- `mail.smtp.host` : serveur relais pour l'e-mail provenant de VMware.
- `mail.smtp.port` : port SMTP.
- `mail.smtp.secureConnection` : utilisez SSL pour le trafic SMTP.

Mettre à niveau SD-WAN Orchestrator

Cette section décrit comment mettre à niveau SD-WAN Orchestrator.

Pour mettre à niveau SD-WAN Orchestrator :

1 Téléchargez l'image sur le système SD-WAN Orchestrator à l'aide de n'importe quel outil de transfert de fichiers disponible dans votre infrastructure, par exemple « SCP ». Copiez l'image à l'emplacement suivant du système : `/var/lib/velocloud/software_update/vco_update.tar`.

2 Connectez-vous à la console SD-WAN Orchestrator et exécutez :

```
sudo /opt/vc/bin/vco_software_update
```

Note Si vous avez configuré SD-WAN Orchestrator comme décrit dans ce document, vous devriez pouvoir vous connecter à la machine virtuelle à l'aide du nom d'utilisateur `vcadmin` et du mot de passe que vous avez définis lors de la création de la configuration de cloud-init.

Pour obtenir des instructions sur la mise à niveau de SD-WAN Orchestrator avec le déploiement de la récupération d'urgence (DR), reportez-vous à la section Chapitre 18 Mettre à niveau SD-WAN Orchestrator à l'aide du déploiement de la récupération d'urgence.

Augmenter la taille du disque (VMware)

Tous les volumes de stockage sont configurés en tant que périphériques LVM. Vous pouvez les redimensionner en ligne en fournissant la technologie de virtualisation sous-jacente afin de

prendre en charge l'extension de disques en ligne. Les disques sont développés automatiquement via cloud-init lorsque la VM démarre.

Pour développer les disques après le démarrage :

1 Connectez-vous à la console système SD-WAN Orchestrator.

2 Identifiez les disques physiques qui prennent en charge le volume de base de données.

```
vgs -o +devices store
```

Exemple :

```
root@vco:~# vgs -o +devices db_data
   \  VG      #PV #LV #SN Attr   VSize   VFree   Devices
     store   1   1   0 wz--n- 500.00g 125.00g /dev/sdb(0)
```

3 Identifiez l'attachement du disque physique.

```
lshw -class volume
```

Exemple :

```
/dev/sdb is attached to scsi@2:0.1.0 (Host: scsi2 Channel: 00 Id: 01 Lun: 00)
```

```
root@vco:~# lshw -class volume
  *-volume
       description: EXT4 volume
       vendor: Linux
       physical id: 1
       bus info: scsi@2:0.0.0,1
       logical name: /dev/sda1
       logical name: /
       version: 1.0
       serial: 9d212247-77c4-4f98-a5c2-7f8470fa2da8
       size: 10239MiB
       capacity: 10239MiB
       capabilities: primary bootable journaled extended_attributes large_files huge_files
dir_nlink recover extents ext4 ext2 initialized
       configuration: created=2016-02-22 20:49:38 filesystem=ext4 label=cloudimg-
rootfs lastmountpoint=/ modified=2016-02-22 21:18:58 mount.fstype=ext4
mount.options=rw,relatime,data=ordered mounted=2016-10-06 23:22:04 state=mounted
  *-disk:1
       description: SCSI Disk
       physical id: 0.1.0
       bus info: scsi@2:0.1.0
       logical name: /dev/sdb
       serial: v5V2zm-Lvbh-Mfx3-W8ki-COI9-DAtP-RXndhu
       size: 500GiB
       capacity: 500GiB
       capabilities: lvm2
       configuration: sectorsize=512
  *-disk:2
       description: SCSI Disk
```

```
        physical id: 0.2.0
        bus info: scsi@2:0.2.0
        logical name: /dev/sdc
        serial: fTQFJ2-giAV-WsXL-1Wha-V305-oQkV-qqS3SA
        size: 100GiB
        capacity: 100GiB
        capabilities: lvm2
        configuration: sectorsize=512
```

4 Sur l'hôte de l'hyperviseur, localisez le disque attaché à la VM à l'aide des informations de bus. Exemple : `SCSI(0:1)`

5 Développer le disque virtuel. Pour obtenir des instructions, reportez-vous à l'article 1004047 de la base de connaissances VMware : http://kb.vmware.com/kb/1004047

6 Connectez-vous de nouveau à la console système SD-WAN Orchestrator.

7 Analysez de nouveau le volume physique redimensionné sur le périphérique de traitement par bloc. Exemple :

```
echo 1 > /sys/block/$DEVICE/device/rescan
```

Exemple :

```
echo 1 > /sys/block/sdb/device/rescan
```

8 Redimensionnez le disque physique LVM.

```
pvresize /dev/sdb
```

9 Déterminez la quantité d'espace libre dans le groupe de volumes de la base de données.

```
vgdisplay store |grep Free
```

Exemple :

```
root@vco:~# vgdisplay store |grep Free
Free  PE / Size       34560 / 135.00 GiB
```

10 Développez le volume logique de la base de données.

```
lvextend -r -L+#G /dev/store/data
```

Exemple :

```
root@vco1:~# lvextend -r -L+1G /dev/store/data
  Size of logical volume store/data changed from 400.00 GiB (102400 extents) to 401.00 GiB
(102656 extents).
  Logical volume store/data successfully resized.
resize2fs 1.44.1 (24-Mar-2018)
Filesystem at /dev/mapper/store-data is mounted on /store; on-line resizing required
old_desc_blocks = 50, new_desc_blocks = 51
The filesystem on /dev/mapper/store-data is now 105119744 (4k) blocks long.
```

11 Affichez la nouvelle taille du volume.

```
df -h /dev/store/data
```

Exemple :

```
root@vco:~# df -h /dev/store/data
Filesystem               Size  Used Avail Use% Mounted on
/dev/mapper/store-data  379G  1.2G  359G   1% /store
```

Se connecter à l'instance de SD-WAN Orchestrator à l'aide de SSO en tant qu'utilisateur opérateur

6

Cette section décrit comment se connecter à SD-WAN Orchestrator à l'aide de l'authentification unique (SSO) en tant qu'utilisateur opérateur.

Pour vous connecter à SD-WAN Orchestrator à l'aide de SSO en tant qu'utilisateur opérateur :

Note Si les autres mécanismes d'authentification échouent, il doit toujours y avoir un super utilisateur opérateur natif comme solution de secours.

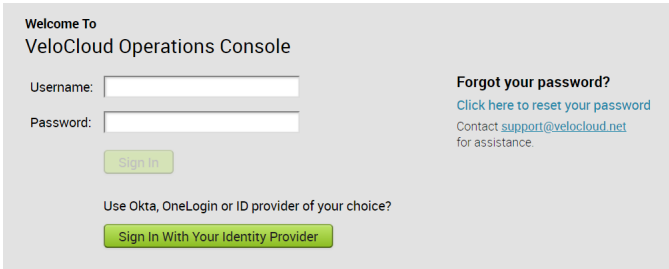
Conditions préalables

- Assurez-vous d'avoir configuré l'authentification SSO dans SD-WAN Orchestrator. Pour plus d'informations, reportez-vous à la section Configurer Single Sign On pour l'utilisateur opérateur.
- Assurez-vous d'avoir configuré les rôles, les utilisateurs et l'application OIDC pour SSO dans vos fournisseurs d'identité préférés. Pour plus d'informations, reportez-vous à la section Configurer un IDP pour l'authentification unique.

Procédure

1 Dans un navigateur Web, lancez une application SD-WAN Orchestrator en tant qu'utilisateur opérateur.

L'écran **Console des opérations VMware SD-WAN (VMware SD-WAN Operations Console)** s'affiche.



2 Cliquez sur **Connectez-vous avec votre fournisseur d'identité (Sign In With Your Identity Provider)**.

Le fournisseur d'identité configuré pour SSO authentifie l'utilisateur et le redirige vers l'URL de SD-WAN Orchestrator configurée.

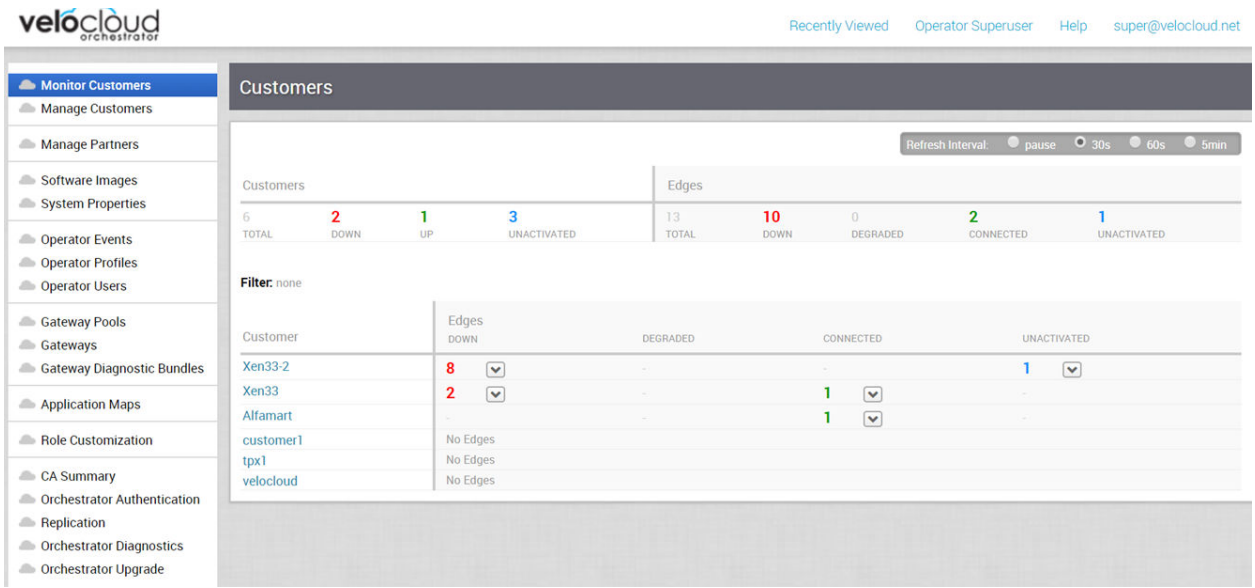
Note Une fois que les utilisateurs se sont connectés à l'instance de SD-WAN Orchestrator à l'aide de SSO, ils ne sont pas autorisés à se reconnecter en tant qu'utilisateurs natifs.

Surveiller les clients

7

En tant qu'utilisateur opérateur, vous pouvez surveiller l'état de vos clients, ainsi que les dispositifs Edge connectés aux clients.

Dans le portail de l'opérateur, cliquez sur **Surveiller les clients (Monitor Customers)**.



Dans le champ **Intervalle d'actualisation (Refresh Interval)**, vous pouvez suspendre la surveillance ou choisir l'intervalle de temps pour actualiser l'état de surveillance.

La page **Surveiller les clients (Monitor Customers)** affiche les détails suivants :

Clients (Customers) :

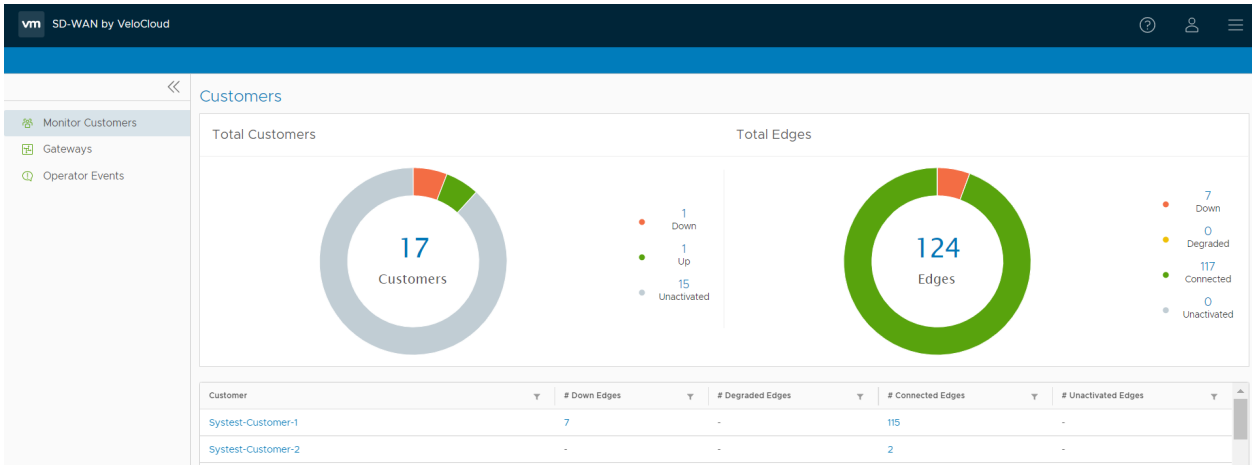
- Clients gérés par l'opérateur.
- Nombre de clients qui sont en service, inactifs et désactivés. Cliquez sur le nombre pour afficher les détails correspondants du client dans le panneau inférieur.
- Dans celui-ci, cliquez sur le lien d'accès au nom du client pour accéder au portail d'entreprise, où vous pouvez afficher et configurer d'autres paramètres correspondant au client sélectionné. Pour plus d'informations, reportez-vous au *Guide d'administration de VMware SD-WAN*.

Dispositifs Edge (Edges) :

- Dispositifs Edge associés aux clients.
- Nombre de dispositifs Edge inactifs, dégradés, connectés et désactivés. Cliquez sur le nombre pour afficher les détails correspondants des dispositifs Edge dans le panneau inférieur.
- Dans celui-ci, placez le curseur de la souris sur la flèche vers le bas affichée en regard du nombre de dispositifs Edge, pour afficher les détails de chaque dispositif Edge. Cliquez sur le lien vers le nom du dispositif Edge pour accéder au portail de surveillance d'entreprise, où vous pouvez afficher plus de détails correspondant au dispositif Edge sélectionné. Pour plus d'informations, reportez-vous au *Guide d'administration de VMware SD-WAN*.

Vous pouvez également afficher les clients et les passerelles associées à l'aide de la nouvelle interface utilisateur d'Orchestrator.

- Dans le portail opérateur, cliquez sur l'option **Ouvrir la nouvelle interface utilisateur d'Orchestrator (Open New Orchestrator UI)** disponible en haut de la fenêtre.
- Cliquez sur **Lancer la nouvelle interface utilisateur d'Orchestrator (Launch New Orchestrator UI)** dans la fenêtre contextuelle. L'interface utilisateur s'ouvre dans un nouvel onglet affichant les options de surveillance.



La nouvelle interface utilisateur d'Orchestrator ne fournit pas l'option d'actualisation automatique. Vous pouvez actualiser la fenêtre manuellement pour afficher les données actuelles.

Gérer les clients

8

L'option **Gérer les clients (Manage Customers)** vous permet de créer des clients, de configurer les capacités de client, de cloner la configuration existante et de configurer d'autres paramètres de client.

Dans le panneau Opérateur (Operator), cliquez sur **Gérer les clients (Manage Customers)**. Cliquez sur **Actions** pour effectuer les activités suivantes :

- **Nouveau client (New Customer)** : crée un client. Reportez-vous à la section Créer un client.
- **Cloner le client (Clone Customer)** : crée un client en clonant les configurations existantes à partir du client sélectionné. Reportez-vous à la section Cloner un client.
- **Modifier le client (Modify Customer)** : permet d'accéder aux **Paramètres système (System Settings)** dans le portail de l'entreprise, où vous pouvez configurer d'autres paramètres correspondant au client sélectionné. Vous pouvez également cliquer sur un nom de client pour accéder au portail de l'entreprise. Pour plus d'informations, reportez-vous au *guide d'administration de VMware SD-WAN*.
- **Supprimer le client (Delete Customer)** : supprime les clients sélectionnés. Assurez-vous d'avoir supprimé tous les dispositifs Edge associés au client sélectionné, avant de supprimer le client.
- **Transférer vers le partenaire (Transfer to Partner)** : attribue les clients sélectionnés à un partenaire. Vous pouvez sélectionner un partenaire existant dans la liste déroulante et décider de déléguer les privilèges à l'opérateur et au partenaire.
- **Publier à partir du partenaire (Release from Partner)** : publie le client sélectionné à partir du partenaire.
- **E-mail de support (Support Email) : Client sélectionné (Selected Customer)** : envoie des messages de support client au client sélectionné.
- **Attribuer un profil d'opérateur (Assign operator profile)** : ajoute un profil d'opérateur pour les clients sélectionnés.

  Note Cette option est disponible uniquement pour les super utilisateurs d'entreprise pour lesquels la fonctionnalité de gestion des images Edge est activée.

- **Mettre à jour la gestion des images Edge (Update Edge Image Management)** : permet d'activer ou de désactiver la fonctionnalité de gestion des images Edge pour les clients sélectionnés.
- **Mettre à jour les notifications préalables (Update Pre-Notifications)** : active ou désactive les alertes de notifications préalables pour les clients sélectionnés.
- **Mettre à jour les alertes client (Update Customer Alerts)** : active ou désactive les alertes pour les clients sélectionnés.
- **Rééquilibrer les passerelles (Rebalance Gateways)** : rééquilibre les passerelles des dispositifs Edge associés au client sélectionné.
- **Exporter tous les clients (Export All Customers)** : exporte les détails de tous les clients dans le portail de l'opérateur vers un fichier CSV. Le séparateur par défaut utilisé est la virgule (,), mais vous pouvez choisir de le remplacer par n'importe quel autre caractère spécial.
- **Exporter l'inventaire des dispositifs Edge client (Export Customer Edge Inventory)** : exporte les détails de l'inventaire de tous les dispositifs Edge associés à tous les clients vers un fichier CSV. Le séparateur par défaut utilisé est la virgule (,), mais vous pouvez choisir de le remplacer par n'importe quel autre caractère spécial.

Ce chapitre contient les rubriques suivantes :

Créer un client

Sur le portail opérateur, vous pouvez créer des clients et configurer les paramètres du client.

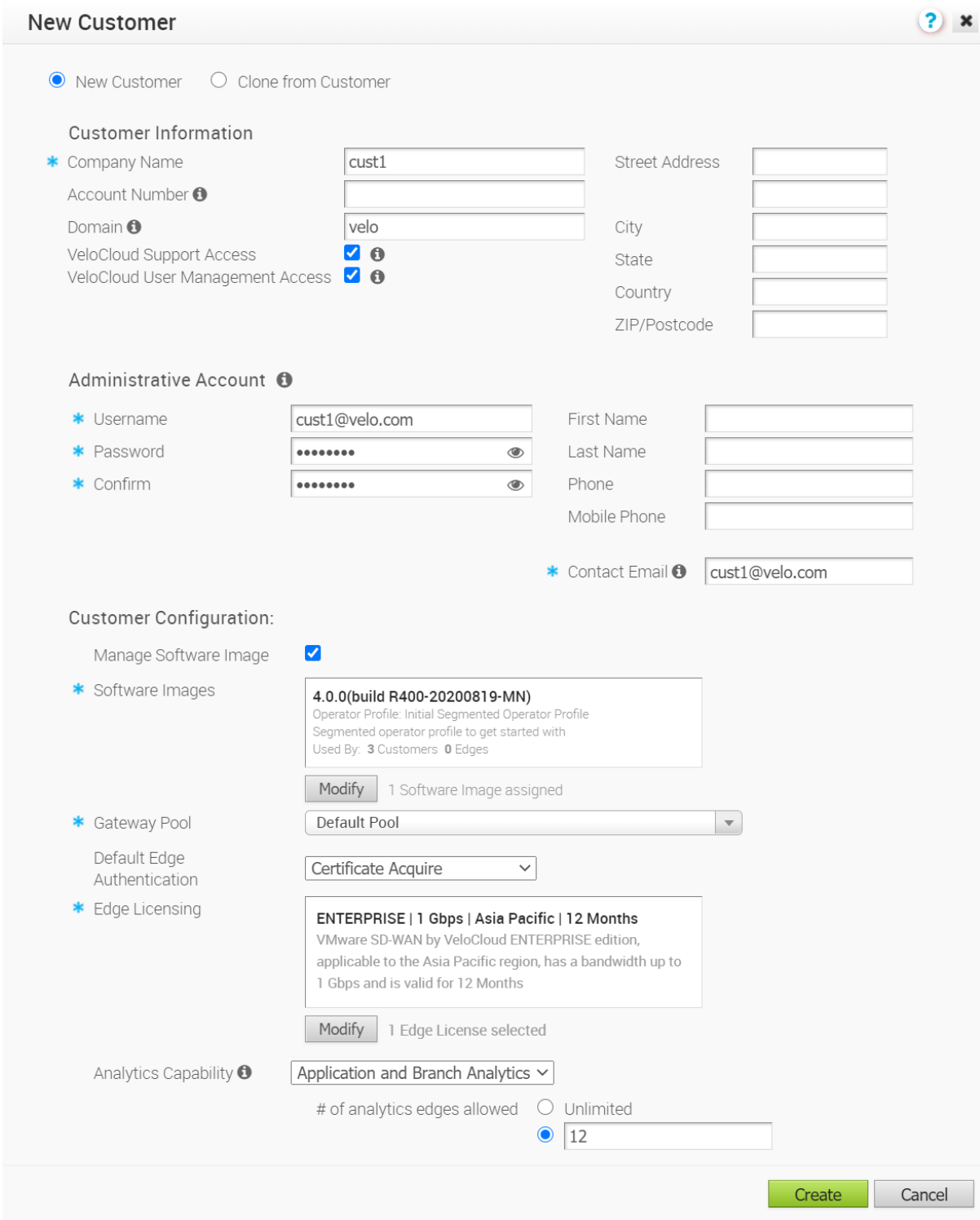
Seuls les super utilisateurs opérateurs et les administrateurs standard opérateurs peuvent créer un client.

Note En tant que super utilisateur opérateur, vous pouvez désactiver temporairement la création de clients en définissant la propriété système `session.options.disableCreateEnterprise` sur Vrai (True). Vous pouvez utiliser cette option lorsque SD-WAN Orchestrator dépasse la capacité d'utilisation.

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

1 Sur la page **Clients (Customers)**, cliquez sur **Nouveau client (New Customer)** ou sur **Actions > Nouveau client (New Customer)**.

2 Dans la fenêtre **Nouveau client (New Customer)**, entrez les informations suivantes. Vous pouvez également choisir l'option **Cloner à partir du client (Clone from Customer)** pour cloner les configurations à partir d'un client existant. Pour plus d'informations, reportez-vous à la section Cloner un client.



Informations sur le client (Customer Information)

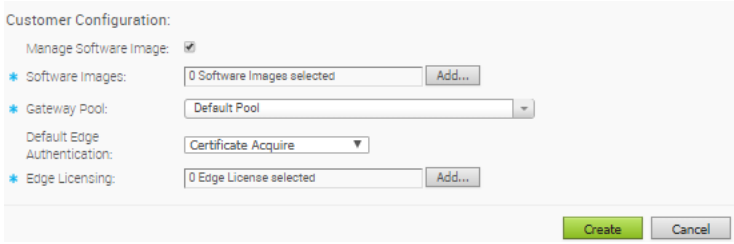
Option	Description
Nom de la société (Company Name)	Entrez le nom de votre société
Numéro de compte (Account Number)	Entrez un identifiant unique pour le client
Domaine (Domain)	Entrez le nom de domaine de votre société
Accès au support VeloCloud (VeloCloud Support Access)	Cette option est sélectionnée par défaut et donne accès au support VMware pour afficher et configurer les dispositifs Edge connectés au client, ou en résoudre les problèmes. Pour des raisons de sécurité, le support ne peut pas accéder aux informations identifiables de l'utilisateur ni les afficher.
Accès à la gestion des utilisateurs VeloCloud (VeloCloud User Management Access)	Cochez cette case pour activer le support VMware afin de faciliter la gestion des utilisateurs. Cette dernière comporte des options pour créer des utilisateurs, réinitialiser le mot de passe et configurer d'autres paramètres. Dans ce cas, le support a accès aux informations identifiables de l'utilisateur.
Adresse postale (Street Address), Ville (City), État (State), Pays (Country), Code postal (ZIP/Postcode)	Entrez les informations d'adresse appropriées dans les champs correspondants.

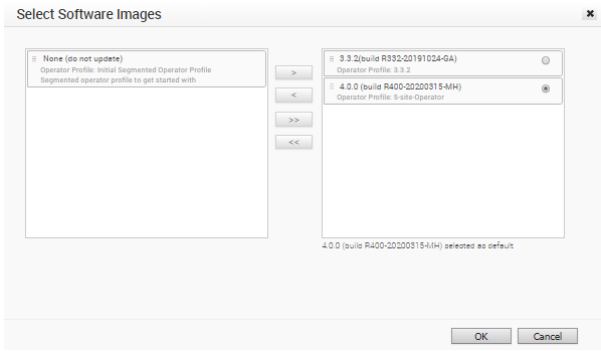
Compte administratif (Administrative Account)

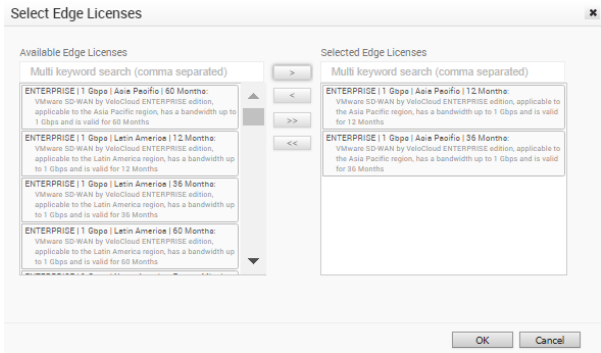
Option	Description
Nom d'utilisateur (Username)	Entrez le nom d'utilisateur au format **utilisateur@domaine.com**.
Mot de passe (Password)	Entrez un mot de passe pour l'administrateur.
Confirmer (Confirm)	Entrez à nouveau le mot de passe.
Prénom (First Name), Nom de famille (Last Name), Téléphone (Phone), Téléphone portable (Mobile Phone)	Entrez les informations, telles que le nom et le numéro de téléphone dans les champs appropriés.
Adresse e-mail de contact (Contact Email)	Entrez l'adresse e-mail. Les alertes relatives à l'état du service sont envoyées à cette adresse e-mail.

Configuration du client

En tant qu'utilisateur opérateur, vous pouvez gérer les images logicielles attribuées à une entreprise directement en attribuant un **Profil d'opérateur (Operator Profile)** à cette entreprise ou autoriser un super utilisateur d'entreprise à gérer la liste des images logicielles disponibles de cette entreprise en activant l'option **Gérer l'image logicielle (Manage Software Image)**.



Option	Description
Gérer l'image logicielle (Manage Software Image)	Cochez cette case si vous souhaitez autoriser un super utilisateur d'entreprise à gérer les images logicielles disponibles pour l'entreprise.
Images logicielles (Software Images)	Cliquez sur **Ajouter (Add)**. Ensuite, dans la fenêtre contextuelle **Sélectionner les images logicielles (Select Software Images)**, sélectionnez et attribuez les images logicielles à partir de la liste disponible pour l'entreprise, puis sélectionnez une image à utiliser par défaut.  **Note** Ce champ s'affiche lorsque vous cochez la case **Gérer l'image logicielle (Manage Software Image)**. Après avoir ajouté les images, vous pouvez modifier la liste des images logicielles attribuées à l'entreprise en cliquant sur **Modifier (Modify)** sous la zone **Configuration du client (Customer Configuration)**. **Note** Vous pouvez supprimer une image attribuée d'une entreprise uniquement si cette image n'est actuellement utilisée par aucun dispositif Edge au sein de cette entreprise.
Profil d'opérateur (Operator Profile)	Sélectionnez un profil d'opérateur à associer au client dans la liste disponible. Ce champ n'est pas disponible si la case **Gérer l'image logicielle (Manage Software Image)** est cochée. Pour plus d'informations sur les profils d'opérateurs, reportez-vous à la section Gérer les profils d'opérateur.

Option	Description
Pool de passerelles (Gateway Pool)	Sélectionnez un pool de passerelles existant dans la liste déroulante. Pour plus d'informations sur les pools de passerelles, reportez-vous à la section Pools de passerelles.
Authentification Edge par défaut (Default Edge Authentication)	Choisissez l'option par défaut dans la liste déroulante pour authentifier les dispositifs Edge associés au client.
Gestion des licences Edge (Edge Licensing)	Cliquez sur **Ajouter (Add)**. Ensuite, dans la fenêtre contextuelle **Sélectionner les licences Edge (Select Edge Licenses)**, sélectionnez et attribuez les licences Edge à partir de la liste disponible pour l'entreprise.  Après avoir ajouté les licences, vous pouvez cliquer sur **Modifier (Modify)** sous la zone **Configuration du client (Customer Configuration)** pour ajouter ou supprimer des licences. **Note** Vous pouvez utiliser les types de licences sur plusieurs dispositifs Edge. Il est recommandé de fournir à vos clients l'accès à tous les types de licences pour faire correspondre leur édition et leur région. Pour plus d'informations, reportez-vous à la section Chapitre 16 Gestion des licences Edge.
Capacité d'analyse	Autorise les super utilisateurs opérateurs et les administrateurs opérateurs standard à activer la fonctionnalité d'analyse pour un nouveau client. Pour plus d'informations, reportez-vous à la section Activer l'analyse pour un nouveau client. **Note** Cette option est disponible uniquement lorsque la fonctionnalité d'analyse est activée sur votre dispositif SD-WAN Orchestrator. Pour plus d'informations, reportez-vous à la section Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator.

Cliquez sur **Créer (Create)**.

Le nom du nouveau client s'affiche sur la page **Clients (Customers)**. Vous pouvez cliquer sur le nom du client pour accéder au portail d'entreprise et ajouter des configurations au client. Pour plus d'informations, reportez-vous à la rubrique Configurer les clients et à la section *Administration d'entreprise* du *Guide d'administration de VMware SD-WAN* disponible à l'adressehttps://docs.vmware.com/fr/VMware-SD-WAN-by-VeloCloud/index.html.

Cloner un client

Vous pouvez cloner les configurations à partir d'un client existant et créer un client avec les paramètres clonés.

Seuls les super utilisateurs opérateurs et les super utilisateurs MSP peuvent cloner un client.

Par défaut, les configurations suivantes sont clonées à partir du client sélectionné :

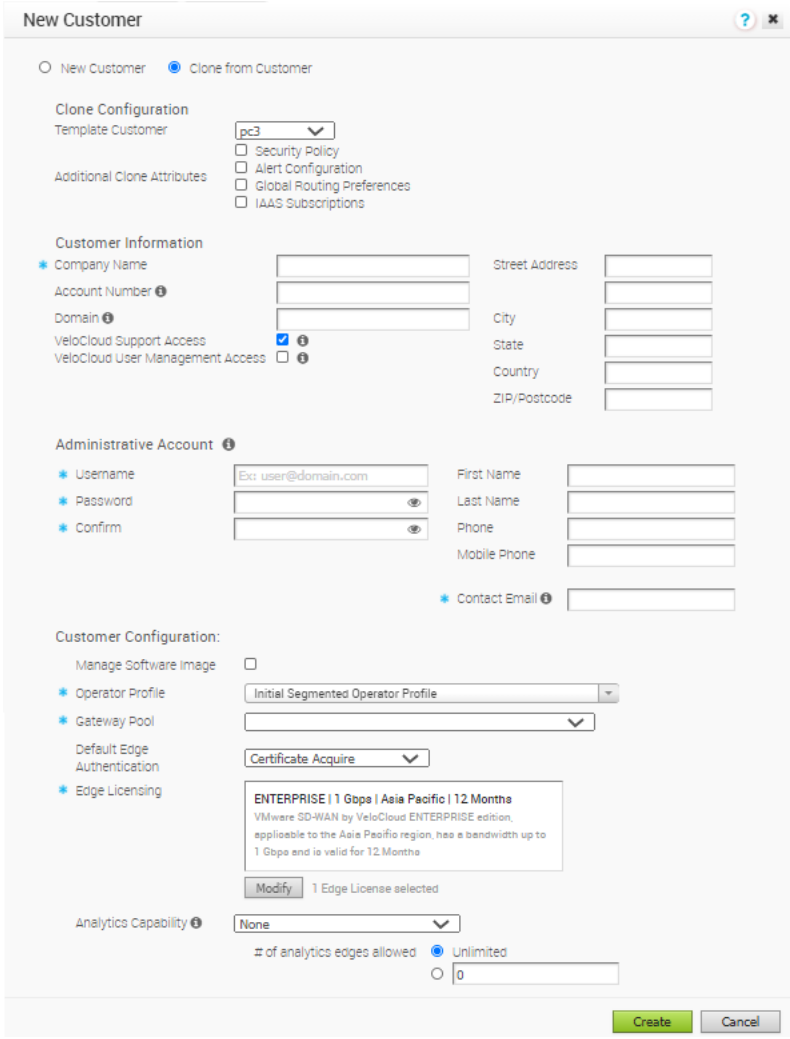
- Profils de configuration d'entreprise
- Services de réseau d'entreprise et objets tels que :
  - Services DNS
  - Noms de réseaux privés
  - Segments de réseau
- Capacités du client
- Schéma d'authentification Edge
- Groupes d'adresses et groupes de ports

Vous ne pouvez pas cloner une entreprise si elle comprend les éléments suivants :

- Profil avec des références Edge telles que des hubs, des clusters, etc.
- Profil contenant des références de la passerelle de partenaires
- Service de sécurité du cloud activé
- Non VMware SD-WAN Sites
- VNF ou licences de VNF
- Services d'authentification
- Objets NetFlow, tels que des collecteurs ou des filtres

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

1. Sur la page **Clients (Customers)**, sélectionnez le client à cloner, puis cliquez sur **Actions > Cloner le client (Clone Customer)**.
2. Dans la fenêtre **Nouveau client (New Customer)**, entrez les informations suivantes. Vous pouvez également choisir l'option **Nouveau client (New Customer)** pour créer un client sans cloner les configurations du client sélectionné. Reportez-vous à la section Créer un client.


New Customer
New Customer
Clone from Customer
Clone Configuration
Template Customer
pc3
Additional Clone Attributes
Security Policy
Alert Configuration
Global Routing Preferences
IAAS Subscriptions
Customer Information
Company Name
Account Number
Domain
VeloCloud Support Access
VeloCloud User Management Access
Street Address
City
State
Country
ZIP/Postcode
Administrative Account
Username
Ex: user@domain.com
Password
Confirm
First Name
Last Name
Phone
Mobile Phone
Contact Email
Customer Configuration:
Manage Software Image
Operator Profile
Initial Segmented Operator Profile
Gateway Pool
Default Edge Authentication
Certificate Acquire
Edge Licensing
ENTERPRISE | 1 Gbps | Asia Pacific | 12 Months
VMware SD-WAN by VeloCloud ENTERPRISE edition, applicable to the Asia Pacific region, has a bandwidth up to 1 Gbps and is valid for 12 Months
Modify
1 Edge License selected
Analytics Capability
None
# of analytics edges allowed
Unlimited
0
Create
Cancel

3 Sous **Cloner la configuration (Clone Configuration)**, vous pouvez configurer les détails suivants.

Option	Description
Modèle de client (Template Customer)	Par défaut, le client sélectionné est pris en compte à des fins de clonage. Si nécessaire, vous pouvez choisir un autre client dans la liste déroulante. Si un client ou une entreprise ne répond pas aux conditions de clonage appropriées, comme indiqué au début de cette section, il n'est pas disponible dans la liste déroulante. Cette liste n'affiche que le nom des clients pouvant être clonés.
Attributs de clone supplémentaires (Additional Clone Attributes)	Outre les configurations clonées par défaut, vous pouvez sélectionner les paramètres suivants à cloner, si nécessaire : ■ Stratégie de sécurité (Security Policy) ■ Configuration des alertes (Alert Configuration) ■ Préférences de routage global (Global Routing Preferences) ■ Abonnements IAAS (IAAS Subscriptions)

4 Entrez les détails pour **Informations sur le client (Customer Information)** et **Compte administratif (Administrative Account)**, comme indiqué à la section Créer un client.

5 Dans la section **Configuration du client (Customer Configuration)**, le profil d'opérateur, les images logicielles, le pool de passerelles et l'authentification Edge par défaut sont clonés à partir du client sélectionné. Si nécessaire, vous pouvez modifier les paramètres de configuration du client cloné.

   a Vous pouvez gérer l'image logicielle attribuée à une entreprise directement en attribuant un **Profil d'opérateur** à cette entreprise ou autoriser un super utilisateur d'entreprise à gérer les images logicielles disponibles pour cette entreprise en activant l'option **Gérer l'image logicielle (Manage Software Image)**. Pour plus d'informations sur l'option **Gérer l'image logicielle (Manage Software Image)**, reportez-vous à la section Créer un client.

   b Vous pouvez gérer les licences Edge attribuées à une entreprise en cliquant sur **Modifier (Modify)**. Dans la fenêtre contextuelle **Sélectionner les licences Edge (Select Edge Licenses)**, vous pouvez sélectionner et attribuer de nouvelles licences Edge pour le client, dans la liste disponible.

   c Vous pouvez activer la fonctionnalité d'analyse pour un client d'entreprise en sélectionnant et en attribuant une option dans le menu déroulant **Capacité d'analyse (Analytics Capability)**. Vous pouvez également définir le nombre maximal de dispositifs Edge d'analyse autorisés pouvant être configurés pour le client. Pour plus d'informations, reportez-vous à la section Activer l'analyse pour un nouveau client.

6 Cliquez sur **Créer (Create)**.

Le nom du nouveau client s'affiche sur la page **Clients (Customers)**. Le client est déjà configuré avec les paramètres clonés. Vous pouvez cliquer sur le nom du client pour accéder au portail d'entreprise et ajouter ou modifier les configurations. Pour plus d'informations sur les configurations et les paramètres du client, reportez-vous à la section Configurer les clients et au *Guide d'administration de VMware* disponible à l'adresse https://docs.vmware.com/fr/VMware-SD-WAN-by-VeloCloud/index.html.

Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator

VMware Edge Network Intelligence est une solution AIOps indépendante du fournisseur et axée sur le dispositif Edge d'entreprise, qui garantit les performances du client pour l'utilisateur final et l'Internet des objets (IoT), la sécurité, la réparation spontanée au moyen d'un réseau LAN filaire et sans fil, SD-WAN et SASE (Secure Access service Edge). L'intégration de VMware Edge Network Intelligence à VMware permet d'étendre la visibilité de SD-WAN au site distant, au campus et à la maison. Cette intégration aide VMware Edge Network Intelligence à obtenir des données de différents points d'observation pour chaque flux d'applications, ce qui inclut le contrôleur sans fil, le commutateur LAN, les services réseau, les dispositifs VMware SD-WAN Edge, VMware SD-WAN Hub et VMware SD-WAN Gateway, et les mesures de performances d'application. Pour plus d'informations, reportez-vous au *Guide de configuration de VMware Edge Network Intelligence*.

VMware fournit des propriétés système prédéfinies pour configurer la fonctionnalité VMware Edge Network Intelligence (ENI) dans le portail SD-WAN Orchestrator. Un super utilisateur opérateur peut ajouter ou modifier les valeurs des propriétés système pour activer le service d'analyse dans un dispositif SD-WAN Orchestrator.

Le tableau suivant décrit toutes les propriétés système liées à VMware Edge Network Intelligence.

Note Lors de l'activation d'ENI pour une instance de SD-WAN Orchestrator, en fonction de l'emplacement du centre de données ENI, vous devez configurer les valeurs appropriées pour les propriétés système suivantes : `service.analytics.configEndpoint`, `service.analytics.analyticsEndpointStatic` et `service.analytics.analyticsEndpointDynamic`, comme indiqué dans le tableau suivant.

Propriété système	Description	Valeur
session.options.enableEdgeAnalytics	Activez le service d'analyse sur un dispositif SD-WAN Orchestrator. Par défaut, l'analyse est activée pour les orchestrateurs hébergés dans le Cloud. **Note** Pour les dispositifs Orchestrator sur site, assurez-vous de définir cette propriété système sur *false*.	*true*
service.analytics.apiURL	URL de l'API d'analyse.	https://integration.nyansa.com/vco/api/v0/graphql
service.analytics.apiToken	Jeton d'API de l'API d'analyse. SD-WAN Orchestrator utilise l'URL et le jeton de l'API pour contacter le moteur d'analyse du cloud et créer des clients/dispositifs SD-WAN Edges dans le moteur d'analyse.	Pour les instances d'Orchestrator hébergées, les opérateurs VMware Edge peuvent générer ce jeton. En ce qui concerne les instances d'Orchestrator sur site, les utilisateurs opérateurs doivent contacter leur SE ou leur AE et leur demander d'envoyer par e-mail le DL des activations ENI pour demander le service.analytics.apiToken. Pour savoir comment contacter le fournisseur de prise en charge, reportez-vous aux pages https://kb.vmware.com/s/article/53907 et https://www.vmware.com/support/contacts/us_support.html.
service.analytics.configEndpoint	Point de terminaison de la configuration du service d'analyse.	■ config.nyansa.com : pour que les instances d'Orchestrator situées dans n'importe quelle région à l'exception de la zone EMEA se connectent à l'instance d'ENI des États-Unis. ■ config.eu.nyansa.com : pour que les instances d'Orchestrator situées dans la région EMEA se connectent à l'instance ENI EMEA.

Propriété système	Description	Valeur
service.analytics.analyticsEndpointStatic	Point de terminaison d'analyse de l'adresse IP statique du service d'analyse.	■ loupe-m2.nyansa.com : pour que les instances d'Orchestrator situées dans n'importe quelle région à l'exception de la zone EMEA se connectent à l'instance d'ENI des États-Unis. ■ loupe-m.eu.nyansa.com : pour que les instances d'Orchestrator situées dans la région EMEA se connectent à l'instance ENI EMEA.
service.analytics.analyticsEndpointDynamic	Point de terminaison d'analyse de l'adresse IP dynamique du service d'analyse.	■ loupe-m.nyansa.com : pour que les instances d'Orchestrator situées dans n'importe quelle région à l'exception de la zone EMEA se connectent à l'instance d'ENI des États-Unis. ■ loupe-m.eu.nyansa.com : pour que les instances d'Orchestrator situées dans la région EMEA se connectent à l'instance ENI EMEA.

Activer l'analyse pour un nouveau client

Lors de la création d'un client SD-WAN (entreprise ou partenaire), VMware SD-WAN Orchestrator permet aux super utilisateurs opérateurs et aux administrateurs opérateurs standard d'activer la fonctionnalité d'analyse du client. L'analyse permet de collecter des données à partir de différents points d'observation pour chaque flux d'applications, qui inclut le contrôleur sans fil, le commutateur LAN, les services réseau, les dispositifs VMware SD-WAN Edge, VMware SD-WAN Hub et VMware SD-WAN Gateway, et les mesures de performances d'application.

Pour activer l'analyse d'un nouveau client, procédez comme suit :

Conditions préalables

Assurez-vous que les propriétés système suivantes sont correctement définies dans SD-WAN Orchestrator :

- `session.options.enableEdgeAnalytics`
- `service.analytics.apiURL`
- `service.analytics.apiToken`

Pour plus d'informations, reportez-vous à la section Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator.

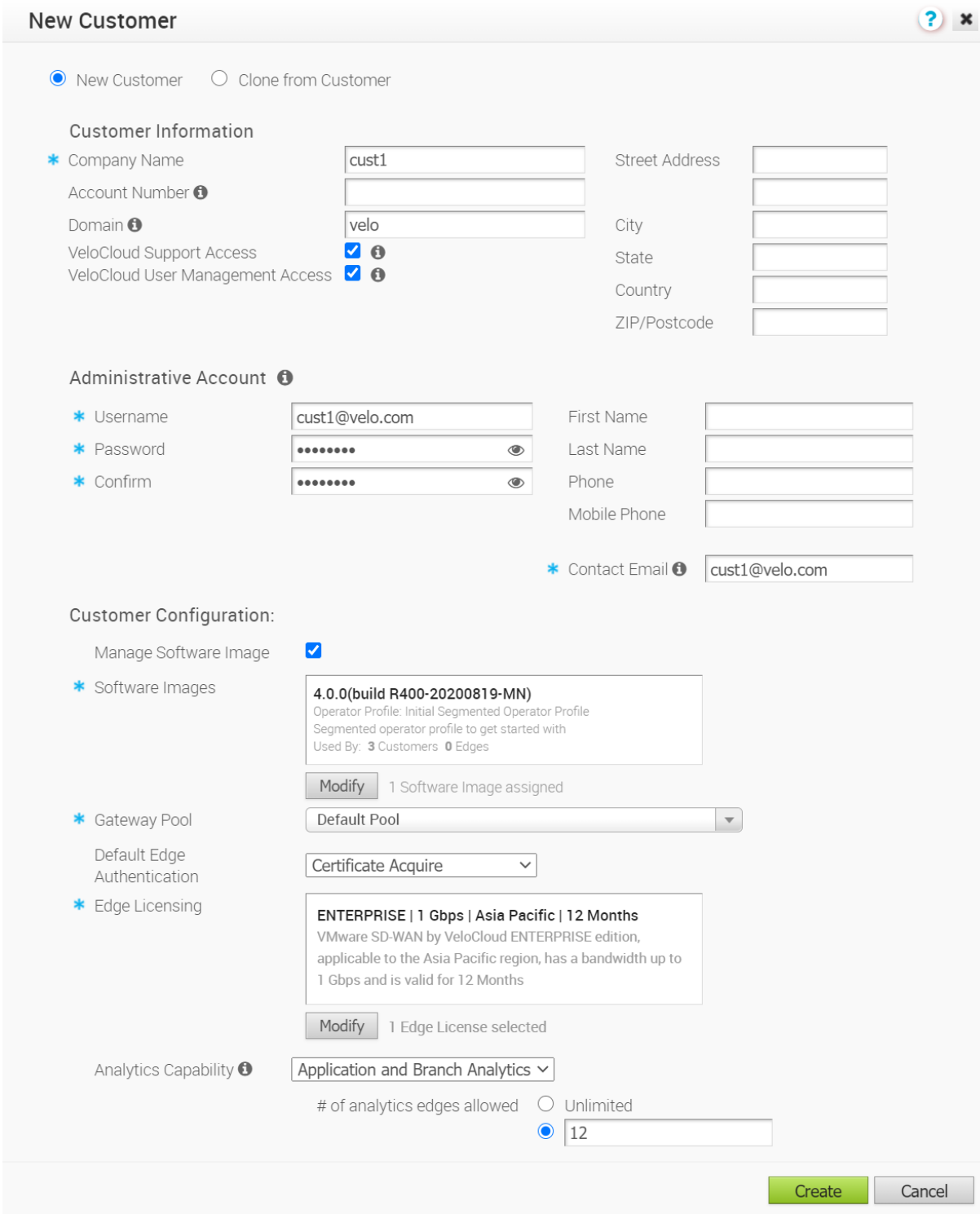
Procédure

1 Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

L'écran **Clients (Customers)** s'affiche.

2 Cliquez sur **Nouveau client (New customer)** ou sur **Actions > Nouveau client (New customer)**.

La boîte de dialogue **Nouveau client (New customer)** s'affiche.



3 Dans la boîte de dialogue **Nouveau client (New customer)**, entrez les informations sur le client, les détails du compte administratif et les détails de la configuration du client.

Note Assurez-vous de fournir un nom de domaine unique pour le client. Si le nom de domaine n'est pas unique, Orchestrator affiche le message d'erreur suivant.

```
Errors from analytics service: Subdomain is already taken
```

Pour plus d'informations, reportez-vous à la section Créer un client.

4 Sous **Configuration du client (Customer Configuration)**, dans le menu déroulant **Capacité d'analyse (Analytics Capability)**, sélectionnez l'une des options suivantes pour activer l'analyse :

- Analyse d'application et de branche (Application and Branch Analytics) : lors du provisionnement d'un dispositif Edge, permet à l'administrateur client de choisir uniquement l'analyse d'application et l'analyse de branche.
- Aucun (None) : cette option est sélectionnée par défaut et les données d'analyse sont désactivées pour le client.

5 Définissez le nombre maximal de dispositifs Edge qui peuvent être provisionnés en tant qu'analyse Edge en entrant une valeur numérique dans la zone de texte **Nombre d'analyses Edge autorisées (# of analytics edges allowed)**. Par défaut, l'option **Illimité (Unlimited)** est sélectionnée.

6 Cliquez sur **Créer (Create)**.

Résultats

Le nom du nouveau client s'affiche sur l'écran **Clients (Customers)**. Vous pouvez cliquer sur le nom du client pour accéder au portail d'entreprise et ajouter ou modifier des configurations de l'analyse pour le client.

Activer l'analyse d'un client existant

VMware SD-WAN Orchestrator autorise les super utilisateurs opérateurs et les administrateurs opérateurs standard à activer l'analyse d'un client SD-WAN existant (entreprise ou partenaire).

Pour activer l'analyse d'un client existant, procédez comme suit.

Conditions préalables

Assurez-vous que les propriétés système suivantes sont correctement définies dans SD-WAN Orchestrator :

- `session.options.enableEdgeAnalytics`
- `service.analytics.apiURL`
- `service.analytics.apiToken`

Pour plus d'informations, reportez-vous à la section Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator.

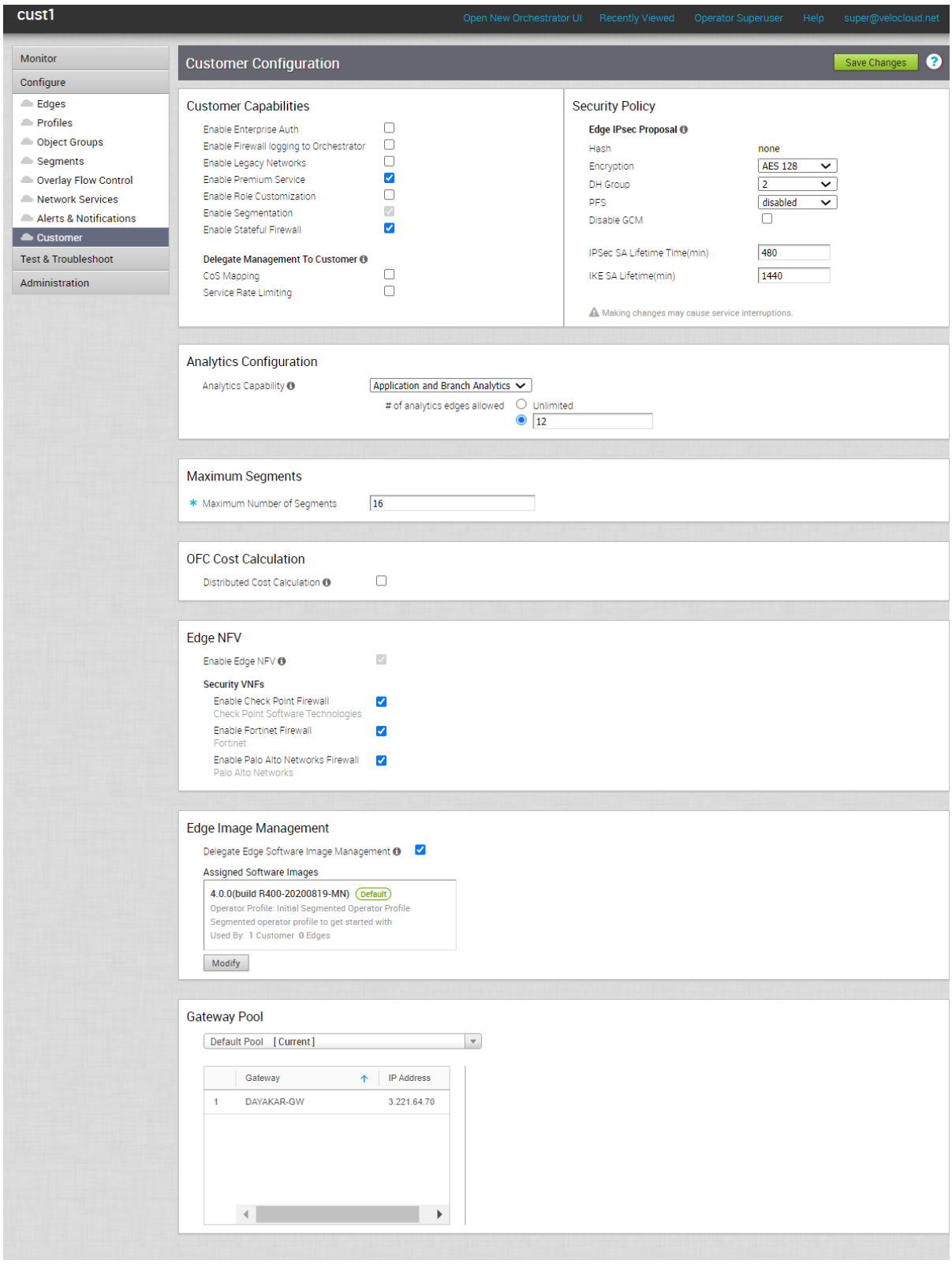
Procédure

1 Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

L'écran **Clients (Customers)** s'affiche.

2 Cliquez sur le nom du client spécifique pour lequel vous souhaitez activer les données d'analyse.

L'écran **Configuration du client (Customer Configuration)** s'affiche.


cust1
Open New Orchestrator UI
Recently Viewed
Operator Superuser
Help
super@velocloud.net
Monitor
Configure
Edges
Profiles
Object Groups
Segments
Overlay Flow Control
Network Services
Alerts & Notifications
Customer
Test & Troubleshoot
Administration
Customer Configuration
Save Changes
Customer Capabilities
Enable Enterprise Auth
Enable Firewall logging to Orchestrator
Enable Legacy Networks
Enable Premium Service
Enable Role Customization
Enable Segmentation
Enable Stateful Firewall
Delegate Management To Customer
CoS Mapping
Service Rate Limiting
Security Policy
Edge IPsec Proposal
Hash
none
Encryption
AES 128
DH Group
2
PFS
disabled
Disable GCM
IPSec SA Lifetime Time(min)
480
IKE SA Lifetime(min)
1440
Making changes may cause service interruptions.
Analytics Configuration
Analytics Capability
Application and Branch Analytics
# of analytics edges allowed
Unlimited
12
Maximum Segments
Maximum Number of Segments
16
OFC Cost Calculation
Distributed Cost Calculation
Edge NFV
Enable Edge NFV
Security VNFs
Enable Check Point Firewall
Check Point Software Technologies
Enable Fortinet Firewall
Fortinet
Enable Palo Alto Networks Firewall
Palo Alto Networks
Edge Image Management
Delegate Edge Software Image Management
Assigned Software Images
4.0.0(build R400-20200819-MN)
Default
Operator Profile: Initial Segmented Operator Profile
Segmented operator profile to get started with
Used By: 1 Customer 0 Edges
Modify
Gateway Pool
Default Pool [Current]
Gateway
IP Address
1
DAYAKAR-GW
3.221.64.70

3 Dans la zone **Configuration de l'analyse (Analytics Configuration)**, dans le menu déroulant **Capacité d'analyse (Analytics Capability)**, sélectionnez l'une des options suivantes pour activer l'analyse :

   - Analyse d'application et de branche (Application and Branch Analytics) : lors du provisionnement d'un dispositif Edge, permet à l'administrateur client de choisir uniquement l'analyse d'application et l'analyse de branche.
   - Aucun (None) : cette option est sélectionnée par défaut et les données d'analyse sont désactivées pour le client.

4 Définissez le nombre maximal de dispositifs Edge qui peuvent être provisionnés en tant qu'analyse Edge en entrant une valeur numérique dans la zone de texte **Nombre d'analyses Edge autorisées (# of analytics edges allowed)**. Par défaut, l'option **Illimité (Unlimited)** est sélectionnée.

5 Cliquez sur **Enregistrer les modifications (Save Changes)**.

Résultats

L'analyse est activée pour le client sélectionné. Vous pouvez cliquer sur le nom du client pour accéder au portail d'entreprise et ajouter ou modifier des configurations de l'analyse pour le client.

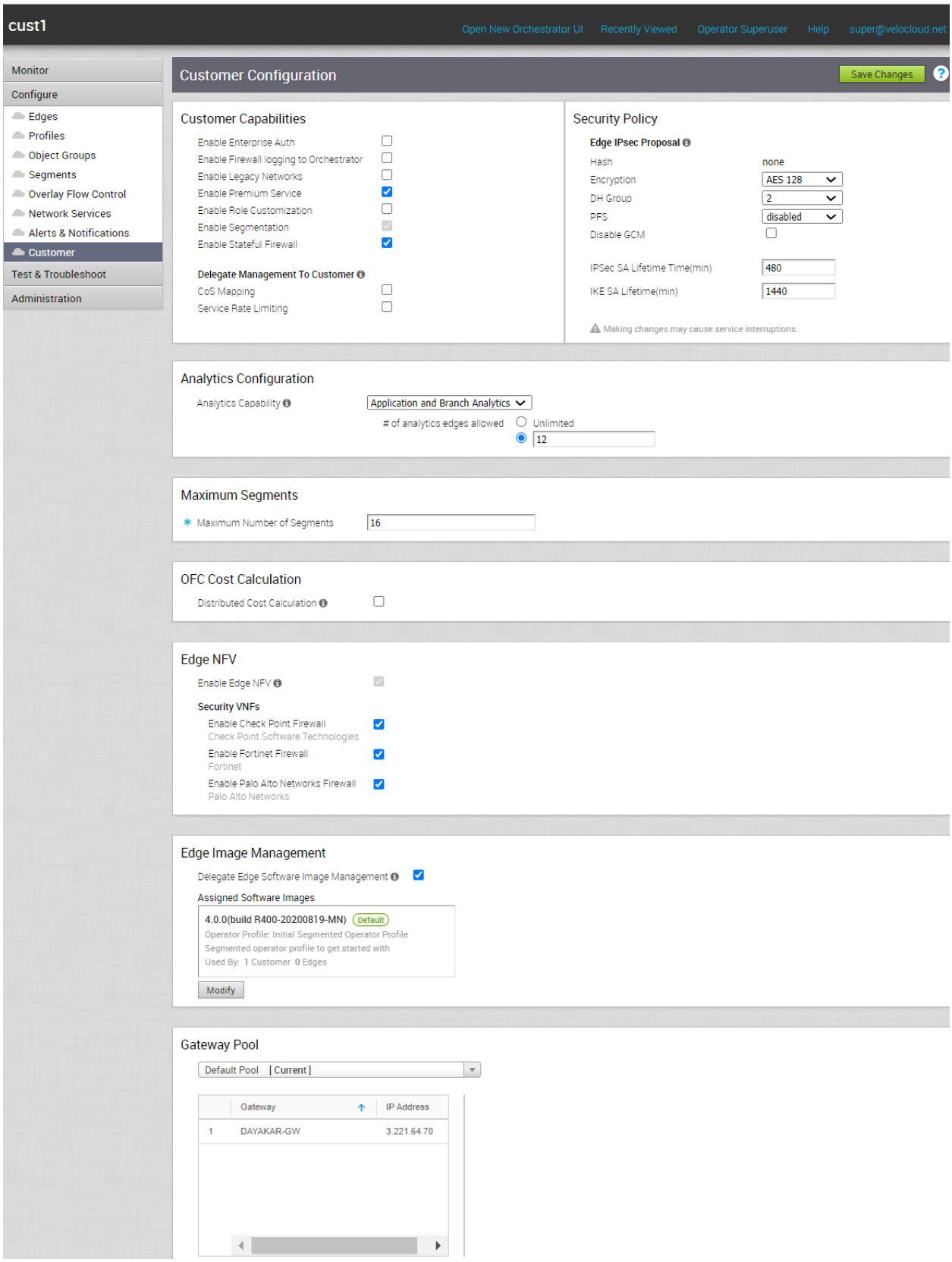
Configurer les clients

Après avoir créé un client, configurez les options et les paramètres des fonctionnalités auxquelles il peut accéder. En tant qu'opérateur, vous pouvez choisir les paramètres que le client ou l'entreprise peut modifier.

Lorsque vous créez un client, vous êtes redirigé vers la page **Configuration du client (Customer Configuration)** sur laquelle vous pouvez configurer les paramètres du client.

Vous pouvez également accéder à la page Configuration à partir de la page **Gérer les clients (Manage Customers)** du portail opérateur. Sélectionnez le client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

Sur le portail client ou d'entreprise, cliquez sur **Configurer (Configure) > Client (Customer)**, afin de pouvoir configurer les paramètres suivants.


cust1
Open New Orchestrator UI
Recently Viewed
Operator Superuser
Help
super@velocloud.net
Monitor
Configure
Edges
Profiles
Object Groups
Segments
Overlay Flow Control
Network Services
Alerts & Notifications
Customer
Test & Troubleshoot
Administration
Customer Configuration
Save Changes
Customer Capabilities
Enable Enterprise Auth
Enable Firewall logging to Orchestrator
Enable Legacy Networks
Enable Premium Service
Enable Role Customization
Enable Segmentation
Enable Stateful Firewall
Delegate Management To Customer
CoS Mapping
Service Rate Limiting
Security Policy
Edge IPsec Proposal
Hash
none
Encryption
AES 128
DH Group
2
PFS
disabled
Disable GCM
IPSec SA Lifetime Time(min)
480
IKE SA Lifetime(min)
1440
Making changes may cause service interruptions.
Analytics Configuration
Analytics Capability
Application and Branch Analytics
# of analytics edges allowed
Unlimited
12
Maximum Segments
Maximum Number of Segments
16
OFC Cost Calculation
Distributed Cost Calculation
Edge NFV
Enable Edge NFV
Security VNFs
Enable Check Point Firewall
Check Point Software Technologies
Enable Fortinet Firewall
Fortinet
Enable Palo Alto Networks Firewall
Palo Alto Networks
Edge Image Management
Delegate Edge Software Image Management
Assigned Software Images
4.0.0(build R400-20200819-MN)
Default
Operator Profile: Initial Segmented Operator Profile
Segmented operator profile to get started with
Used By: 1 Customer 0 Edges
Modify
Gateway Pool
Default Pool [Current]
Gateway
IP Address
1
DAYAKAR-GW
3.221.64.70

Vous pouvez configurer les paramètres suivants :

- **Capacités du client (Customer Capabilities)** : activez ou désactivez les paramètres auxquels le client sélectionné peut accéder, qu'il peut configurer et modifier. Reportez-vous à la section Configurer les capacités des clients.
- **Stratégie de sécurité (Security Policy)** : choisissez de mettre à jour les stratégies de sécurité existantes lorsque vous créez des tunnels IPSec entre deux dispositifs Edge. Reportez-vous à la section Configurer la stratégie de sécurité.
- **Configuration de l'analyse (Analytics Configuration)** : autorise les super utilisateurs opérateurs et les administrateurs opérateurs standard à activer l'analyse pour un client SD-WAN existant. Reportez-vous à la section Activer l'analyse d'un client existant.

  Note Cette option est disponible uniquement lorsque la fonctionnalité d'analyse est activée sur un dispositif SD-WAN Orchestrator. Pour plus d'informations, reportez-vous à la section Activer VMware Edge Network Intelligence sur un dispositif VMware SD-WAN Orchestrator.
- **Nombre maximal de segments (Maximum Segments)** : entrez le nombre maximal de segments pouvant être configurés. La plage est comprise entre 1 et 16 et la valeur par défaut est de 16.
- **Calcul du coût d'OFC (OFC Cost Calculation)** : choisissez de distribuer le calcul du coût des routes aux dispositifs Edge et aux passerelles, afin de réduire la consommation des ressources et la charge d'Orchestrator. Reportez-vous à la section Configurer le calcul du coût distribué.
- **Plusieurs balises DSCP par calcul de chemin de flux (Multiple-DSCP tags per Flow Path Calculation)** : choisissez d'activer le calcul de chemin pour un seul flux avec plusieurs étiquettes DSCP. Reportez-vous à la section Configurer le calcul du chemin à l'aide de plusieurs étiquettes DSCP par flux.
- **NFV d'Edge (Edge NFV)** : activez NFV sur les dispositifs Edge pour déployer des VNF de sécurité. Reportez-vous à la section Configurer NFV et VNF pour les dispositifs Edge.
- **Gestion des images Edge (Edge Image Management)** : gérez les images logicielles Edge attribuées à une entreprise. Reportez-vous à la section Gérer les images logicielles.
- **Pool de passerelles (Gateway Pool)** : choisissez un pool de passerelles à attribuer à l'entreprise. Reportez-vous à la section Associer un pool de passerelles.
- **Autres paramètres (Other Settings)** : cette option n'est disponible que lorsque vous avez activé l'option **Contrat d'utilisateur (User Agreement)**. Vous pouvez choisir de remplacer les paramètres d'affichage par défaut du contrat d'utilisateur en sélectionnant l'option appropriée dans la liste déroulante **Affichage du contrat d'utilisateur (User Agreement Display)**. Par défaut, le client hérite du mode d'affichage défini dans les propriétés système. Pour plus d'informations, reportez-vous à la section Chapitre 20 Gérer les contrats d'utilisateur.

Après avoir modifié les configurations, cliquez sur **Enregistrer les modifications (Save Changes)**.

Configurer les capacités des clients

Vous pouvez activer ou désactiver les capacités suivantes pour un client sélectionné :

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

Sur la page **Configuration du client (Customer Configuration)**, activez ou désactivez les **Capacités du client (Customer Capabilities)** :

Note Pour activer les capacités du client, une valeur `True` doit être attribuée à toutes les propriétés système qui lui sont associées. Pour plus d'informations, reportez-vous à la section Chapitre 11 Propriétés système.

- **Activer l'authentification d'entreprise (Enable Enterprise Auth)** : par défaut, seul l'opérateur peut activer ou désactiver l'authentification à deux facteurs pour une entreprise. Lorsque vous activez cette capacité, les administrateurs d'entreprise peuvent configurer eux-mêmes l'authentification à deux facteurs.
- **Activer la journalisation du pare-feu dans Orchestrator (Enable Firewall logging to Orchestrator)** : permet à un utilisateur d'entreprise d'activer ou de désactiver la journalisation des informations de pare-feu dans Orchestrator, au niveau du profil et au niveau du dispositif Edge. Lorsque la journalisation du pare-feu est activée, vous pouvez surveiller les journaux du pare-feu sur le portail d'entreprise.
- **Activer les réseaux hérités (Enable Legacy Networks)** : permet à une entreprise d'utiliser des réseaux hérités. Vous ne pouvez pas activer cette option si vous utilisez un profil d'opérateur basé sur un segment.
- **Activer le service Premium (Enable Premium Service)** : permet d'utiliser les services Premium.
- **Activer la personnalisation des rôles (Enable Role Customization)** : permet d'activer ou de désactiver un super utilisateur d'entreprise afin de personnaliser les privilèges de rôle des autres utilisateurs de l'entreprise.
- **Activer la segmentation (Enable Segmentation)** : permet de configurer des segments.
- **Activer le pare-feu avec état (Enable Stateful Firewall)** : permet à un utilisateur d'entreprise d'activer ou de désactiver la fonctionnalité de pare-feu avec état au niveau du profil et du dispositif Edge.
- **Déléguer la gestion au client (Delegate Management To Customer)** : les options suivantes sont toujours visibles par les clients. Lorsque vous activez ces options, les clients peuvent modifier les paramètres.
  - Mappage de CoS (CoS Mapping)

- Limitation du débit pour les services (Service Rate Limiting)

Note Les options **Activer le service Premium (Enable Premium Service)**, **Activer la segmentation (Enable Segmentation)** et **Activer le pare-feu avec état (Enable Stateful Firewall)** sont activées par défaut.

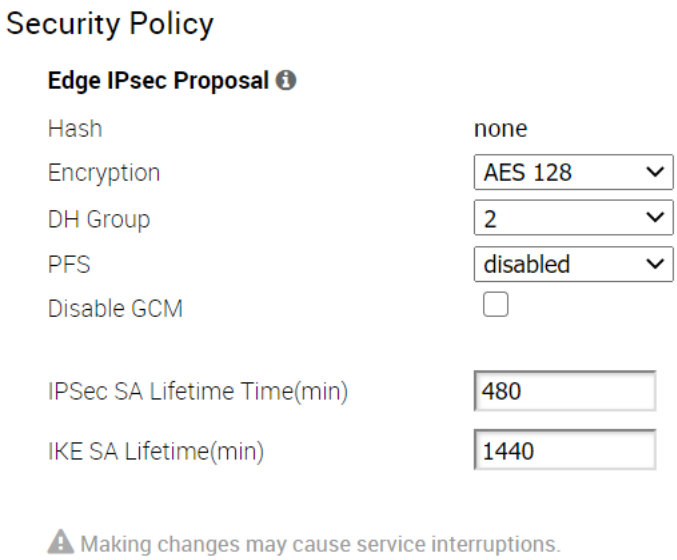
Après avoir choisi les capacités, cliquez sur **Enregistrer les modifications (Save Changes)**.

Configurer la stratégie de sécurité

Lors de la création de tunnels IPSec entre deux dispositifs Edge, vous pouvez modifier les paramètres de configuration de la stratégie de sécurité au niveau de la configuration du client.

Procédure

1. Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.
2. Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.
3. Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**. La page **Configuration du client (Customer Configuration)** s'affiche.



4 Dans la zone de **Stratégie de sécurité (Security Policy)**, vous pouvez configurer les paramètres de sécurité suivants :

a **Hachage (Hash)** : par défaut, aucun algorithme d'authentification n'est configuré pour l'en-tête VPN. Lorsque le mode Galois/Compteur (GCM) est désactivé, vous pouvez sélectionner l'un des éléments suivants comme algorithme d'authentification pour l'en-tête VPN, dans la liste déroulante qui s'affiche :

- SHA 1
- SHA 256
- SHA 384
- SHA 512

b **Chiffrement (Encryption)** : AES 128-mode Galois/Compteur (GCM), AES 256-GCM, AES 128-Chaînage de chiffrement de blocs (CBC) et AES 256-CBC sont les modes d'algorithme de chiffrement utilisés pour fournir la confidentialité. Sélectionnez **AES 128** ou **AES 256** comme taille de clé des algorithmes AES de chiffrement des données. Le mode d'algorithme de chiffrement par défaut est AES 128-GCM, lorsque la case **Désactiver GCM (Disable GCM)** n'est pas cochée.

c **Groupe DH (DH Group)** : sélectionnez l'algorithme de groupe Diffie-Hellman (DH) à utiliser lors de l'échange d'une clé prépartagée. Le groupe DH définit la puissance de l'algorithme en bits. Les groupes DH pris en charge sont 2, 5, 14, 15 et 16. Il est recommandé d'utiliser le groupe DH 14.

d **PFS** : sélectionnez le niveau PFS (Perfect Forward Secrecy) pour renforcer la sécurité. Les niveaux de PFS pris en charge sont 2, 5, 14, 15 et 16. Par défaut, PFS est désactivé.

e **Désactiver GCM (Disable GCM)** : par défaut, AES 128-GCM est activé. Si nécessaire, cochez la case pour désactiver ce mode. La désactivation de la case active le mode AES 128-CBC.

f **Durée de vie IPsec SA (IPsec SA Lifetime)** : moment où le renouvellement de clés du protocole IPSec (Internet Security Protocol) est initié pour les dispositifs Edge. La durée de vie IPsec minimale est de 3 minutes et la valeur maximale est de 480 minutes. La valeur par défaut est de 480 minutes.

g **Durée de vie IKE SA (IKE SA Lifetime)** : moment où le renouvellement de clés de l'échange de clés Internet (IKE, Internet Security Protocol) est initié pour les dispositifs Edge. La durée de vie IKE minimale est de 10 minutes et la valeur maximale est de 1 440 minutes. La valeur par défaut est de 1 440 minutes.

Note Il n'est pas recommandé de configurer des valeurs de durée de vie faibles pour IPsec (moins de 10 minutes) et IKE (moins de 30 minutes), car cela peut provoquer une interruption du trafic dans certains déploiements en raison des renouvellements de clés. Les valeurs de durée de vie faibles sont destinées uniquement à des fins de débogage.

5 Après avoir configuré les paramètres, cliquez sur **Enregistrer les modifications (Save Changes)**.

Note Lorsque vous modifiez les paramètres de sécurité, les modifications peuvent entraîner des interruptions des services actuels. Par ailleurs, ces paramètres peuvent réduire le débit global et augmenter le temps requis pour la configuration du tunnel VCMP, ce qui peut affecter la configuration du tunnel dynamique branche vers branche et la récupération après une défaillance du dispositif Edge dans un cluster.

Configurer le calcul du coût distribué

Par défaut, Orchestrator est activement impliqué dans l'apprentissage des routes dynamiques. Les dispositifs Edge et les passerelles VMware SD-WAN reposent sur Orchestrator pour calculer les préférences de routes initiales et les renvoyer au dispositif Edge et à la passerelle. La fonctionnalité Calcul du coût distribué (Distributed Cost Calculation) permet de distribuer le calcul du coût des routes aux dispositifs Edge et aux passerelles.

Note L'activation de **Calcul du coût distribué (Distributed Cost Calculation)** est recommandée pour tous les clients.

Cette méthode par défaut d'implication d'Orchestrator dans le calcul de route dynamique et la distribution de ces routes aux dispositifs Edge et aux passerelles présente les inconvénients suivants :

- Si Orchestrator subit une charge élevée, le délai de convergence des routes est considérablement élevé (par exemple, jusqu'à 40 secondes pour plus de 2 000 routes), car Orchestrator utilise ce délai pour calculer la préférence pour toutes les routes synchronisées et renvoie ces préférences aux dispositifs Edge et aux passerelles.
- L'utilisation d'Orchestrator pour le calcul des routes signifie que les nouvelles routes dynamiques apprises alors qu'Orchestrator était inaccessible ne sont pas annoncées tant qu'Orchestrator n'est pas de nouveau accessible.

Lorsqu'une entreprise cliente utilise Calcul du coût distribué (Distributed Cost Calculation), Orchestrator n'est plus activement impliqué dans le calcul des préférences de routes et, au lieu de cela, les routes sont correctement insérées dans l'ordre par dispositif Edge et passerelle instantanément lors de leur apprentissage, puis transmettent ces préférences à Orchestrator.

Lorsque vous choisissez d'activer Calcul du coût distribué (Distributed Cost Calculation) pour les dispositifs Edge et les passerelles, cette fonctionnalité présente les avantages suivants :

- Minimise l'incidence sur l'apprentissage des routes lorsqu'un dispositif Orchestrator est inaccessible.
- Le délai de convergence des routes est réduit de minutes à secondes dans les grands réseaux avec des milliers de routes dynamiques.
- Les délais réseau sont considérablement réduits.
- Fournit une convergence instantanée du plan de données.

- Prend en charge la réorganisation améliorée et l'épinglage des routes sur Overlay Flow Control.
- Fournit une option d'actualisation des routes sur la page **Overlay Flow Control**. À chaque modification de la stratégie Overlay Flow Control, l'option Actualiser les routes (Refresh Routes) applique immédiatement les modifications aux routes existantes, sans nécessiter le redémarrage du dispositif Edge ou de la passerelle.

L'activation de Calcul du coût distribué (Distributed Cost Calculation) a les incidences suivantes sur le réseau d'entreprise du client :

- Toutes les routes dynamiques locales sont actualisées, et la préférence et l'action d'annonce de ces routes sont mises à jour. Ces informations mises à jour sont annoncées à la passerelle, à Orchestrator et enfin à l'entreprise. Le réseau du client doit entièrement recréer la table de routage, ce qui prendra moins de 5 secondes pour la plupart des déploiements client. Un déploiement client à grande échelle (par exemple, plus de 100 000 routes) peut prendre jusqu'à 2 minutes. Le trafic client de tous les sites est affecté pendant la reconstruction de la table de routage.
- Tout flux existant utilisant ces routes peut potentiellement être affecté par la modification des entrées de routage.

Note Il est recommandé d'activer Calcul du coût distribué (Distributed Cost Calculation) dans une fenêtre de maintenance afin de minimiser l'incidence sur l'entreprise du client.

Pour configurer Calcul du coût distribué (Distributed Cost Calculation) :

Conditions préalables

Assurez-vous de ce qui suit avant d'activer la fonctionnalité Calcul du coût distribué (Distributed Cost Calculation).

- Tous les dispositifs Edge et les passerelles doivent utiliser la version logicielle 3.4.0 ou une version ultérieure.
- L'image logicielle associée au profil d'opérateur doit utiliser la version 3.4.0 ou une version ultérieure.

Procédure

1. Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.
2. Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.
3. Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

4 Sur la page **Configuration du client (Customer Configuration)**, accédez à la section **Calcul du coût d'OFC (OFC Cost Calculation)** et cochez la case **Calcul du coût distribué (Distributed Cost Calculation)** pour déléguer le calcul du coût des routes aux dispositifs Edge et aux passerelles.

Note Une fois que vous avez activé **Calcul du coût distribué (Distributed Cost Calculation)**, vous ne pouvez plus rétrograder les dispositifs Edge et les passerelles vers une version antérieure à la version 3.4.0, sauf si vous désactivez également **Calcul du coût distribué (Distributed Cost Calculation)**. Cette fonctionnalité ne fonctionne pas sur un réseau si un dispositif Edge ou une passerelle de ce réseau utilise une version logicielle antérieure à la version 3.4.0.

5 Cliquez sur **Enregistrer les modifications (Save Changes)**.

Note Après avoir activé **Calcul du coût distribué (Distributed Cost Calculation)**, il est recommandé d'actualiser les routes sur la page Overlay Flow Control.

Résultats

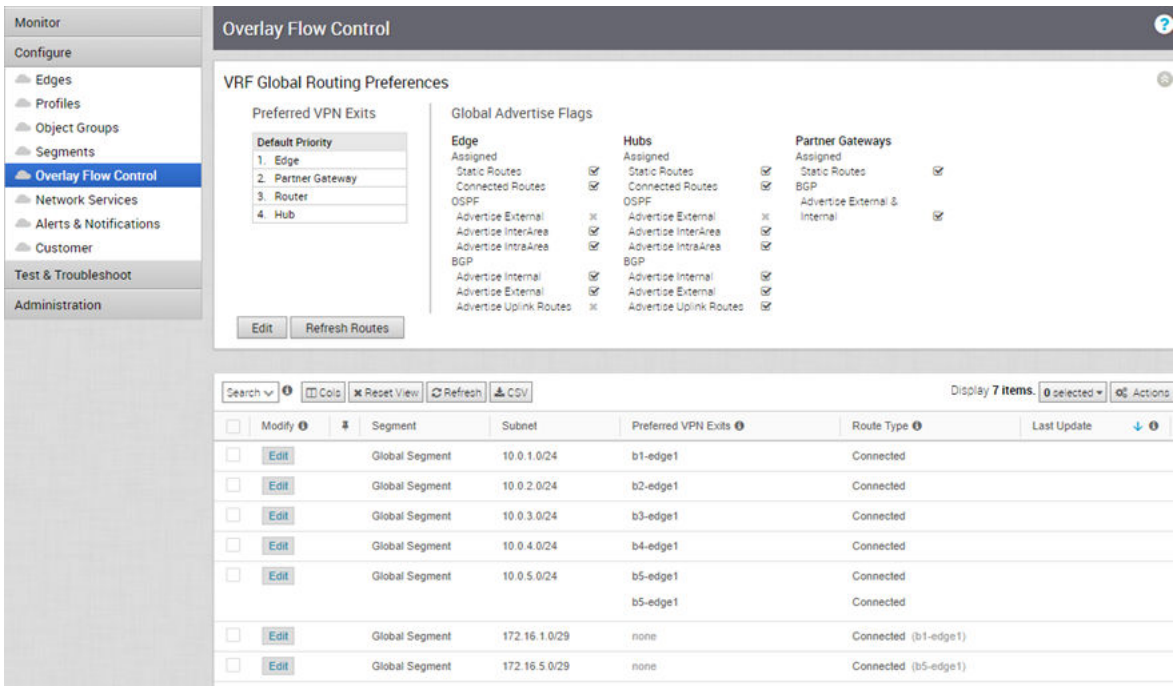
Une fois que l'option **Calcul du coût distribué (Distributed Cost Calculation)** est activée, toutes les routes dynamiques sont attribuées avec de nouvelles préférences et une action d'annonce selon le Calcul du coût distribué (Distributed Cost Calculation) et les nouvelles informations sont propagées sur le réseau d'entreprise.

Orchestrator n'est plus activement impliqué dans le calcul des préférences de routes et, au lieu de cela, les routes sont correctement insérées dans l'ordre par dispositif Edge et passerelle instantanément lors de leur apprentissage. Ces préférences sont ensuite communiquées à Orchestrator.

La stratégie Overlay Flow Control est envoyée aux dispositifs Edge et aux passerelles dans les mises à jour de configuration du plan de contrôle. Les dispositifs Edge et les passerelles envoient les routes avec le coût calculé et l'action d'annonce à Orchestrator. Les dispositifs Edge et les passerelles gèrent l'ordre des routes en fonction des attributs de coût et de route.

Pour afficher un résumé de toutes les routes de votre réseau, cliquez sur **Configurer (Configure) > Overlay Flow Control** sur le portail d'entreprise. Vous pouvez afficher les routes et l'action d'annonce sur la page **Overlay Flow Control**.

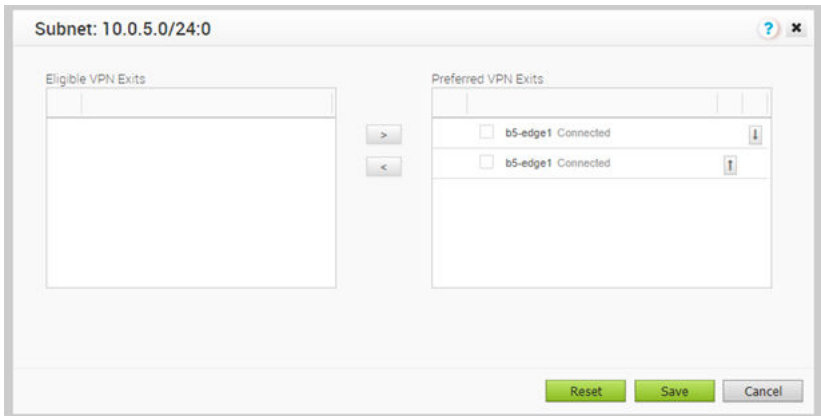
Après avoir activé **Calcul du coût distribué (Distributed Cost Calculation)**, l'option **Actualiser les routes (Refresh Routes)** est disponible sur la page **Overlay Flow Control**.



Lorsque vous cliquez sur **Actualiser les routes (Refresh Routes)**, cette option force les dispositifs Edge et les passerelles à recalculer les coûts des routes apprises et à les envoyer à Orchestrator. En outre, les modifications apportées à l'Overlay Flow Control sont appliquées immédiatement sur les nouvelles routes apprises et les actuelles.

Note Il est recommandé d'utiliser l'option **Actualiser les routes (Refresh Routes)** dans une fenêtre de maintenance, car l'option a une incidence sur le réseau semblable à l'effet causé par l'activation du Calcul du coût distribué (Distributed Cost Calculation).

Vous pouvez réinitialiser le calcul du coût des sous-réseaux lorsque des routes épinglées sont disponibles. Cliquez sur l'option **Modifier (Edit)** d'un sous-réseau.



Cliquez sur **Réinitialiser (Reset)**, ce qui permet à Orchestrator d'effacer les routes épinglées, de recalculer le coût du sous-réseau sélectionné en fonction de la stratégie et d'envoyer les résultats aux dispositifs Edge et aux passerelles.

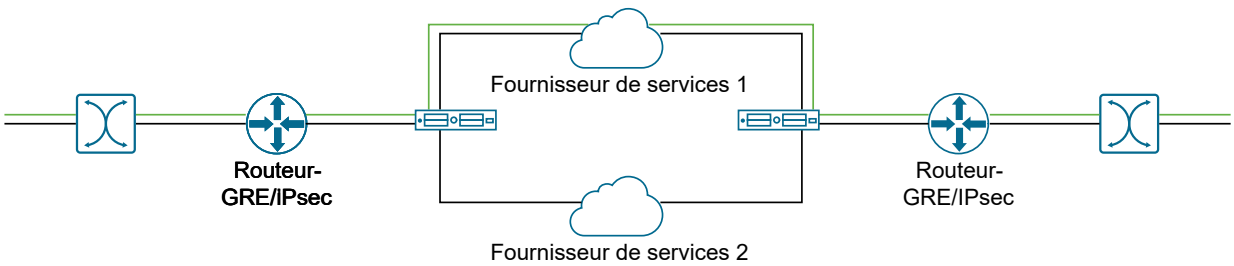
Note L'option **Réinitialiser (Reset)** n'est disponible que lorsque l'option Calcul du coût distribué (Distributed Cost Calculation) est activée.

Configurer le calcul du chemin à l'aide de plusieurs étiquettes DSCP par flux

Les dispositifs Edge classent les flux de trafic en fonction des premiers paquets du flux. Vous pouvez créer des stratégies d'entreprise avec une application basée sur DSCP (Differentiated Service Code Point) et avec différents marquages DSCP pour déterminer le traitement du flux.

Par défaut, les dispositifs Edge classent les flux en fonction des premiers paquets reçus dans le flux. La stratégie d'entreprise et le marquage QoS déterminent le traitement du flux. Une fois le flux classé, une entrée avec cinq informations de tuple du flux est créée dans la table du cache de flux. Les paquets suivants dans le flux utiliseront la recherche des cinq tuples dans la table de cache de flux.

Pour les topologies de réseau avec des périphériques réseau de couche 3 procédant à une encapsulation et/ou un chiffrement avant que le trafic n'arrive sur le dispositif Edge, cela crée une stimulation pour que le dispositif Edge transfère le trafic en fonction de la stratégie d'entreprise. Le trafic en provenance des utilisateurs finaux est multiplexé dans un seul flux avec les mêmes adresses IP source et de destination et les mêmes protocoles par le périphérique d'encapsulation/de chiffrement de couche 3, comme illustré dans l'image suivante.



L'effet du multiplexage des flux d'utilisateurs dans un tunnel unique crée une polarisation du transfert de flux à l'aide des cinq tuples de la table de cache du flux, ce qui entraîne la non-utilisation des liens WAN.

Le calcul du chemin avec plusieurs étiquettes DSCP par flux permet d'inclure la valeur DSCP, en plus des cinq tuples, dans la recherche dans la table de cache de flux. Utilisez le calcul du chemin avec plusieurs balises DSCP lorsque le trafic d'utilisateur d'origine est encapsulé dans un autre tunnel, comme GRE ou IPsec, et que les étiquettes DSCP sont conservées dans le nouvel en-tête IP. Cette option active le calcul du chemin pour un flux unique avec plusieurs étiquettes DSCP, qui se compose de la même adresse IP source et de destination, et fournit des différenciations de chemin en fonction des étiquettes DSCP dans le flux.

Lorsque vous activez l'option **Plusieurs balises DSCP par calcul de chemin de flux (Multiple-DSCP tags per Flow Path Calculation)**, les dispositifs Edge peuvent différencier les flux de trafic en fonction des étiquettes signalées DSCP.

Pour activer l'option Plusieurs balises DSCP par calcul de chemin de flux (Multiple-DSCP tags per Flow Path Calculation) :

1 Dans le portail de l'opérateur, cliquez sur **Propriétés système (System Properties)**.

2 Cliquez sur **Nouvelle propriété système (New System Property)**.

3 Dans la fenêtre **Nouvelle propriété système (New System Property)**, créez une propriété système avec les paramètres suivants :

- **Nom (Name)** : *session.options.enableFlowParametersConfig*
- **Type de données (Data Type)** : *Boolean*
- **Valeur (Value)** : *True*

4 Cliquez sur **Enregistrer (Save)**.

5 Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

6 Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

7 Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

8 Sur la page **Configuration du client (Customer Configuration)**, accédez à la section **Plusieurs balises DSCP par calcul de chemin de flux (Multiple-DSCP tags per Flow Path Calculation)**, puis cochez la case **Inclure la valeur DSCP dans la recherche de flux (Include DSCP value as part of flow lookup)**.

   Note Cette option est disponible uniquement lorsque la valeur de la propriété système **session.options.enableFlowParametersConfig** est définie sur True.

9 Cliquez sur **Enregistrer les modifications (Save Changes)**.

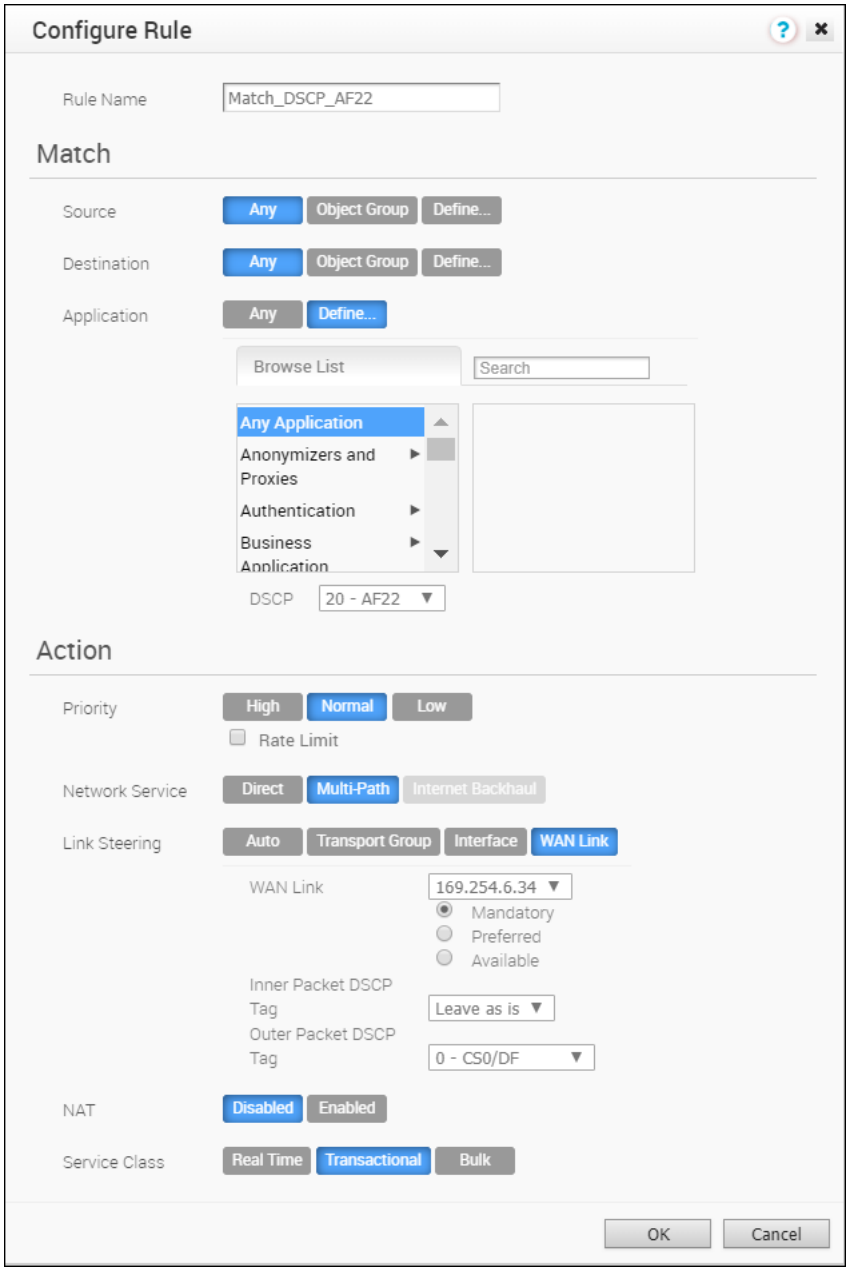
10 Dans les dispositifs Edge, différents flux sont créés en fonction de différentes étiquettes DSCP.

Note Lorsque vous activez l'option **Inclure la valeur DSCP dans la recherche de flux (Include DSCP value as part of flow lookup)**, l'interopérabilité avec les versions précédentes n'est pas définie.

Lors de la configuration de la stratégie d'entreprise pour un dispositif Edge, vous pouvez choisir de faire correspondre une étiquette DSCP à une application.

- Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Dispositifs Edge (Edges)**.
- Sélectionnez un dispositif Edge, puis cliquez sur l'onglet **Stratégie d'entreprise (Business Policy)**.
- Cliquez sur **Nouvelle règle (New Rule)** ou sur **Actions > Nouvelle règle (New Rule)**.

- Dans la fenêtre **Configurer la règle (Configure Rule)**, cliquez sur **Définir (Define)** pour **Application** et sélectionnez une application dans la liste. Choisissez une étiquette DSCP dans la liste déroulante.



- Choisissez les actions appropriées en fonction des besoins dans la zone de **Action**.
- Cliquez sur **OK**.

Lorsque le trafic arrive sur le dispositif Edge, si le flux de trafic correspond à l'application et à la balise DSCP sélectionnées, l'action correspondante est effectuée.

Vous pouvez créer d'autres stratégies d'entreprise avec différentes étiquettes DSCP pour les faire correspondre à différents flux de trafic et appliquer des traitements différents à ces flux. Pour plus d'informations sur les stratégies d'entreprise, reportez-vous au *Guide d'administration de VMware SD-WAN.*

Limitations :

- Le calcul du chemin avec plusieurs étiquettes DSCP par flux ne s'applique pas à SD-WAN Gateways. Vous pouvez activer cette option uniquement pour les tunnels entre deux dispositifs Edge, dans les scénarios suivants :
  - Entre deux dispositifs Edge via un hub
  - Réseau en étoile
  - Entre deux branches, dynamique

  Vous pouvez utiliser cette option pour le déploiement sur site où la passerelle est utilisée uniquement pour la fonctionnalité de plan de contrôle et non pour le trafic du plan de données.
- Le calcul du chemin avec plusieurs étiquettes DSCP par flux est destiné uniquement au trafic GRE ou IPSec. Le trafic Internet direct ne transporte pas plusieurs étiquettes DSCP dans un même flux.
- Une fois que vous avez activé l'option de calcul du chemin, lorsque le flux de trafic se compose de paquets ayant les mêmes informations de cinq tuples, mais des marquages DSCP différents, la traduction NAT côté LAN peut ne pas fonctionner comme prévu.

Configurer NFV et VNF pour les dispositifs Edge

Vous pouvez activer la virtualisation des fonctions réseau (NFV, Network Function Virtualization) sur les dispositifs Edge et déployer des fonctions de réseau virtuel (VNF, Virtual Network Functions) sur les dispositifs Edge à l'aide de pare-feu tiers.

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

Sur la page **Configuration du client (Customer Configuration)**, la section **NFV d'Edge (Edge NFV)** permet d'activer NFV sur les dispositifs Edge et permet aux clients de déployer des VNF tiers sur des plates-formes Edge adaptées au service.

Actuellement, les modèles de plates-formes Edge aptes au service sont les suivants : 520V et 840. En tant qu'utilisateur opérateur, lorsque vous activez la virtualisation des fonctions réseau (NFV, Network Function Virtualization) d'Edge, les clients peuvent configurer et déployer des VNF et des licences de VNF à partir de leurs services réseau.

- **Activer la NFV d'Edge (Enable Edge NFV)** : sélectionnez cette option pour permettre de déployer des VNF sur des dispositifs Edge. Après le déploiement d'une ou de plusieurs VNF sur des dispositifs Edge, vous ne pouvez pas désactiver cette option.

- **VNF de sécurité (Security VNFs)** : cochez les cases appropriées en regard des VNF tierces pour déployer les VNF de sécurité correspondantes sur les dispositifs Edge.

Après avoir sélectionné les VNF de sécurité, cliquez sur **Enregistrer les modifications (Save Changes)**.

Gérer les images logicielles

Vous pouvez gérer les images du logiciel Edge attribuées à une entreprise directement en attribuant un profil d'opérateur à cette entreprise ou autoriser un super utilisateur d'entreprise à gérer les images logicielles.

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

Sur la page **Configuration du client (Customer Configuration)**, la section **Gestion des images Edge (Edge Image Management)** affiche le profil d'opérateur actuel associé au client d'entreprise sélectionné. En tant que super utilisateur opérateur, vous pouvez sélectionner et attribuer un autre profil d'opérateur dans la liste des profils d'opérateurs disponibles pour le client, si nécessaire.

Lors du basculement vers un autre profil d'opérateur, prenez en considération les restrictions suivantes :

- Si vous passez d'un profil d'opérateur basé sur un segment à un profil d'opérateur basé sur un réseau, les dispositifs Edge de l'entreprise pour le profil basé sur un segment ne reçoivent pas de mises à jour d'images logicielles.
- Si vous passez d'un profil d'opérateur basé sur un réseau à un profil d'opérateur basé sur un segment, les dispositifs Edge de l'entreprise pour le profil basé sur un réseau ne reçoivent pas de mises à jour d'images logicielles.

Si vous souhaitez qu'un super utilisateur d'entreprise gère des images logicielles du dispositif Edge, vous devez activer la case **Déléguer la gestion des images logicielles Edge (Delegate Edge Software Image Management)**. Une fois que vous activez l'option **Déléguer la gestion des images logicielles Edge (Delegate Edge Software Image Management)** et que vous cliquez sur **Enregistrer les modifications (Save Changes)**, toutes les images logicielles attribuées au client d'entreprise s'affichent. Cliquez sur **Modifier (Modify)** pour ajouter ou supprimer une image logicielle du client sélectionné.

Note Vous pouvez supprimer une image attribuée d'un client d'entreprise uniquement s'il ne s'agit pas d'une image par défaut et si elle n'est actuellement utilisée par aucun dispositif Edge du client d'entreprise.

Associer un pool de passerelles

Vous pouvez associer un pool de passerelles à une entreprise. Les dispositifs Edge de l'entreprise se connectent aux sites à l'aide des passerelles du pool de passerelles.

Sur le portail opérateur, accédez à **Gérer les clients (Manage Customers)**.

Sélectionnez un client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.

Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Clients (Customers)**.

Sur la page **Configuration du client (Customer Configuration)**, la section **Pool de passerelles (Gateway pool)** affiche le pool de passerelles actuel associé au client d'entreprise sélectionné. Si nécessaire, vous pouvez choisir un autre pool de passerelles disponible dans la liste déroulante et cliquer sur **Enregistrer les modifications (Save Changes)**.

Si les passerelles disponibles dans le pool de passerelles ont été attribuées avec le rôle de passerelle de partenaires, vous pouvez les transférer vers les partenaires. Sélectionnez l'option **Activer le transfert aux partenaires (Enable Partner Handoff)** pour configurer les options de transfert pour les segments et les passerelles. Pour plus d'informations, reportez-vous à la section Configurer le transfert aux partenaires.

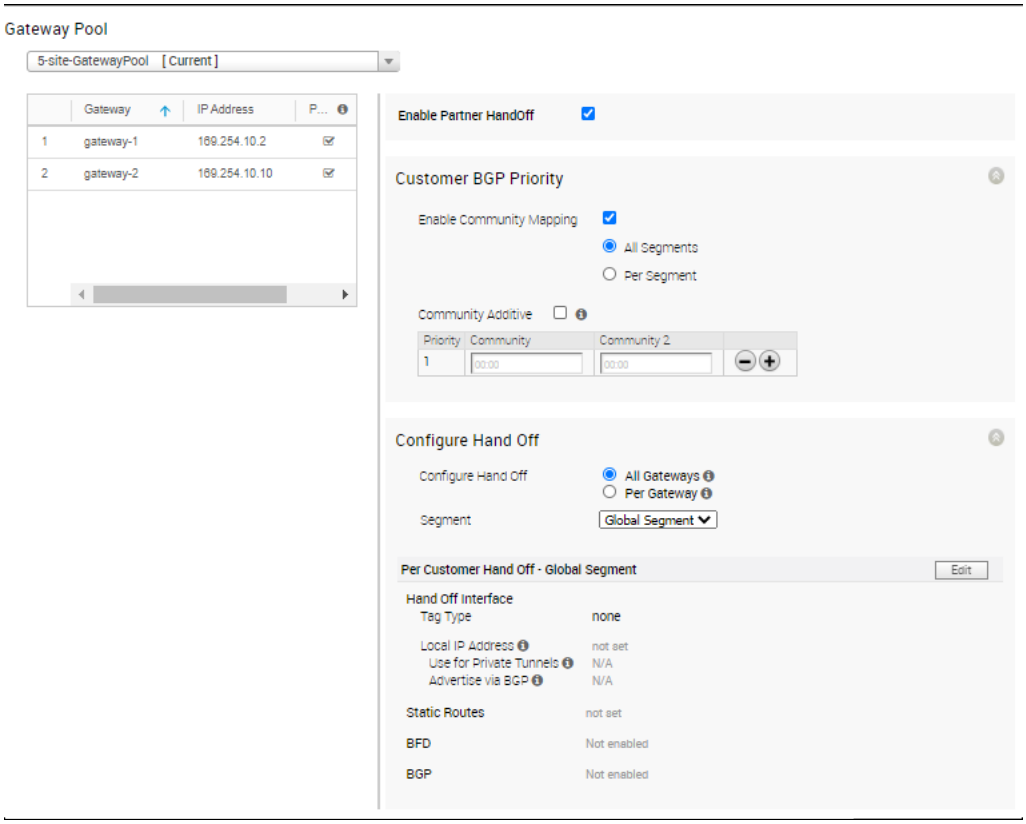
Configurer le transfert aux partenaires

Vous pouvez configurer une passerelle pour le transfert aux partenaires. La passerelle fait office de passerelle de partenaires et vous pouvez configurer l'interface de transfert, les routes statiques, BGP, BFD et d'autres paramètres.

Vérifiez que la passerelle à transférer est attribuée avec le rôle de passerelle de partenaires. Sur le portail Orchestrator, cliquez sur **Passerelles (Gateways)**, puis sur le lien d'accès à une passerelle existante. Dans la section **Propriétés (Properties)** de la passerelle sélectionnée, vous pouvez activer le rôle de passerelle de partenaires.

Pour configurer les paramètres de transfert, accédez à la page **Configuration du client (Customer Configuration)**.

- Dans le portail de l'opérateur, cliquez sur **Gérer les clients (Manage Customers)**.
- Sélectionnez le client, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au client.
- Sur le portail client ou d'entreprise, cliquez sur **Configurer (Configure) > Client (Customer)**.
- Dans **Configuration du client (Customer Configuration)**, accédez à la section **Pool de passerelles (Gateway Pool)** et cochez la case **Activer le transfert aux partenaires (Enable Partner Handoff)**.



Configurez les paramètres suivants :

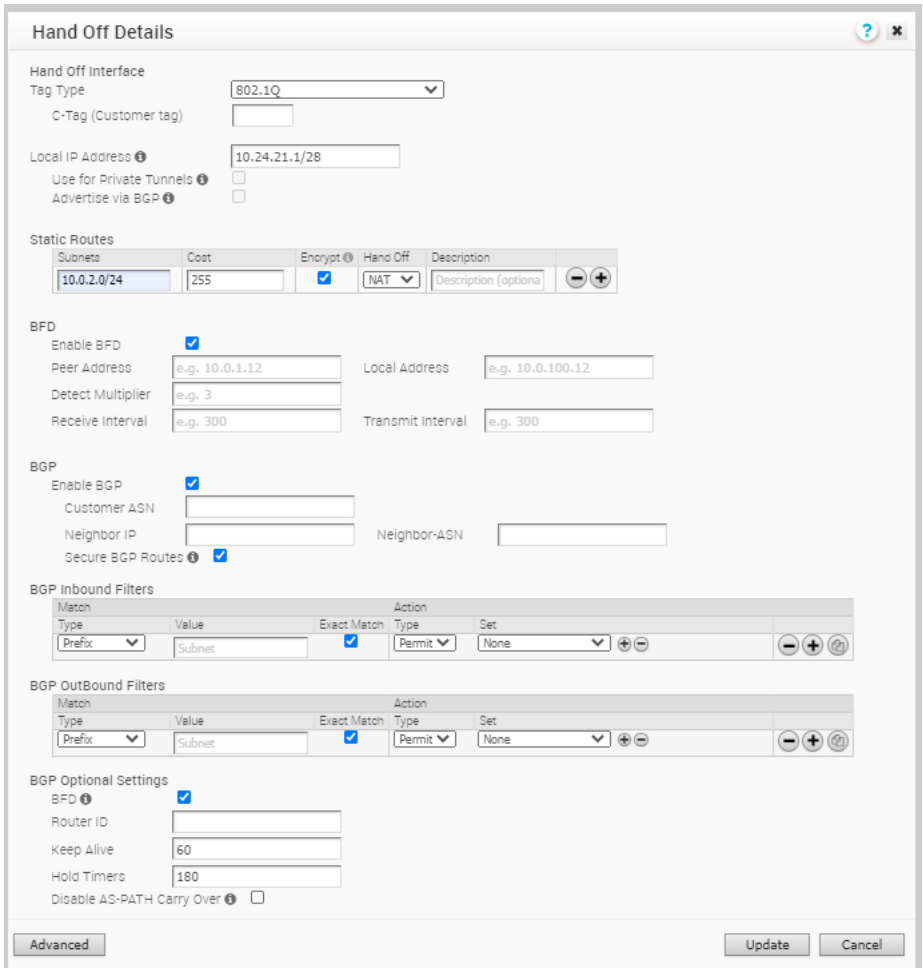
Priorité BGP du client (Customer BGP Priority)

- Sélectionnez **Activer le mappage de la communauté (Enable Community Mapping)** pour définir les attributs de la communauté, qui sont balisés dans les routes annoncées BGP.
- Par défaut, le mappage de la communauté est défini sur tous les segments. Pour configurer les attributs de la communauté d'un segment spécifique, choisissez **Par segment (Per Segment)** et sélectionnez le segment dans la liste déroulante.
- Cochez la case **Additif de la communauté (Community Additive)** pour activer l'option d'additif associée à une configuration de communauté automatique particulière. Cette option conserve les attributs de la communauté entrants pour un préfixe reçu à partir de la superposition et ajoute la communauté automatique configurée au préfixe, sur la passerelle de partenaires. Par conséquent, le côté PE (Provider Edge) de MPLS reçoit des préfixes avec tous les attributs de la communauté, y compris les attributs de la communauté automatique.
- Entrez les attributs de la communauté dans les champs **Communauté (Community)** et **Communauté 2 (Community 2)**. Cliquez sur l'icône Plus (**+**) pour ajouter d'autres attributs de la communauté.

Configurer le transfert (Configure Hand Off)

- Par défaut, la configuration du transfert est appliquée à toutes les passerelles. Pour configurer une passerelle spécifique, choisissez **Par passerelle (Per Gateway)** et sélectionnez la passerelle dans la liste déroulante.
- Par défaut, la configuration du transfert est appliquée à tous les segments. Pour configurer un segment spécifique, sélectionnez **Segment** dans la liste déroulante.
- Pour configurer toutes les passerelles, cliquez sur l'option **Modifier (Edit)**. Si vous avez sélectionné une passerelle spécifique, cliquez sur le lien **Cliquer ici pour configurer (Click here to configure)**.

La fenêtre **Détails du transfert (Hand Off Details)** s'affiche et vous pouvez configurer les éléments suivants :



Option	Description
Interface de transfert (Hand Off Interface)	
Type de balise (Tag Type)	Choisissez le type de balise qui correspond à l'encapsulation dans laquelle la passerelle transfère le trafic client vers le routeur. Vous trouverez ci-après les types de balises disponibles : ■ **Aucun (None)** : non balisé. Choisissez cette option lors du transfert d'un locataire unique ou d'un transfert vers le VRF (Virtual Routing and Forwarding) des services partagés. ■ **802.1q** : balise VLAN unique. ■ **802.1ad / QinQ(0x8100) / QinQ(0x9100)** : deux balises VLAN.
VLAN de transport (Transport VLAN)	Cette option n'est disponible que lorsque vous choisissez le type de balise 802.1ad / QinQ(0x8100) / QinQ(0x9100). Choisissez le type de balise permettant de configurer les VLAN de transport.
Balise C (balise client) (C-Tag [Customer tag])	Entrer la balise VLAN du client
Balise S (balise de service) (S-Tag [Service Tag])	Entrer la balise VLAN définie par le fournisseur de services
Adresse IP locale (Local IP Address)	Entrez l'adresse IP locale de l'interface de transfert logique.
Utiliser pour les tunnels privés (Use for Private Tunnels)	Cochez cette case pour que les liens WAN privés se connectent à l'adresse IP privée de la passerelle de partenaires. Si la connectivité WAN privée est activée sur une passerelle, Orchestrator effectue un audit pour vérifier que l'adresse IP locale est unique pour chaque passerelle d'une entreprise.
Annoncer via BGP (Advertise via BGP)	Cochez la case pour annoncer automatiquement l'adresse IP WAN privée de la passerelle de partenaires via BGP. La connectivité est fournie à l'aide de l'adresse IP locale existante.
Routes statiques (Static Routes) : cliquez sur l'icône Plus (**+**) pour ajouter d'autres routes.	
Sous-réseaux (Subnets)	Entrez l'adresse IP du sous-réseau de la route statique que la passerelle doit annoncer au dispositif Edge.
Coût (Cost)	Entrez le coût pour appliquer la pondération sur les routes. La plage est comprise entre 0 et 255.
Chiffrer (Encrypt)	Cochez cette case pour chiffrer le trafic entre Edge et la passerelle.
Transférer (Hand off)	Sélectionnez le type de transfert VLAN ou NAT.
Description (Description)	Entrez éventuellement un texte descriptif pour la route statique.
BFD	

Option	Description
Activer BFD (Enable BFD)	Cochez cette case pour activer l'abonnement BFD pour les voisins BGP et pour configurer les paramètres BFD.
Adresse de l'homologue (Peer Address)	Entrez l'adresse IP de l'homologue distant pour initier une session BFD.
Adresse locale (Local Address)	Entrez une adresse IP configurée localement pour l'écouteur de l'homologue. Cette adresse est utilisée pour l'envoi de paquets.
Multiplicateur de détection (Detect Multiplier)	Entrez le multiplicateur de temps de détection. L'intervalle de transmission à distance est multiplié par cette valeur pour déterminer le temporisateur de détection pour la perte de connexion. La plage est comprise entre 3 et 50, et la valeur par défaut est de 3.
Intervalle de réception (Receive Interval)	Entrez l'intervalle de temps minimal, en millisecondes, pendant lequel le système peut recevoir les paquets de contrôle de l'homologue BFD. La plage est comprise entre 300 et 60 000 millisecondes, et la valeur par défaut est de 300 millisecondes.
Intervalle de transmission (Transmit Interval)	Entrez l'intervalle de temps minimal, en millisecondes, pendant lequel le système local peut envoyer les paquets de contrôle BFD. La plage est comprise entre 300 et 60 000 millisecondes, et la valeur par défaut est de 300 millisecondes.
BGP	
Activer BGP (Enable BGP)	Cochez cette case pour activer BGP et paramétrer la configuration BGP.
ASN du client (Customer ASN)	Entrez le numéro de système autonome du client.
Adresse IP du voisin (Neighbor IP)	Entrez l'adresse IP du réseau voisin configuré.
ASN du voisin (Neighbor-ASN)	Entrez l'ASN du réseau voisin.
Routes BGP sécurisées (Secure BGP Routes)	Cochez cette case pour activer le chiffrement pour le transfert de données sur les routes BGP.
Filtres entrants/sortants du BGP (BGP Inbound/Outbound Filters) : cliquez sur l'icône plus (**+**) pour ajouter d'autres filtres.	
Type (Correspondance) (Type [Match])	Choisissez le type de l'attribut BGP à prendre en compte pour la correspondance avec le flux de trafic. Vous pouvez choisir **Préfixe (Prefix)** ou **Communauté (Community)**.
Valeur (Value)	Entrez la valeur en fonction de l'attribut BGP sélectionné comme type.
Correspondance exacte (Exact Match)	Cochez la case pour une correspondance exacte avec les attributs.
Type (Action)	Choisissez l'action à effectuer si la valeur de la correspondance est Vrai (True). Vous pouvez autoriser ou refuser le trafic.

Option	Description
Définir (Set)	Vous pouvez définir les valeurs des attributs pour les routes correspondant aux critères de filtre. Choisissez parmi les attributs suivants et entrez les valeurs correspondantes à définir pour les routes correspondantes : ■ Aucun (None) : les attributs des routes correspondantes restent identiques. ■ Préférence locale (Local Preference) ■ Communauté : vous pouvez également activer l'option **Additif de la communauté (Community Additive)**. ■ Mesure (Metric) ■ Préfixe de chemin AS (AS-Path-Prepend)
Paramètres BGP facultatifs (BGP Optional Settings)	
BFD	Cochez la case pour vous abonner à la session BFD.
ID de routeur (Router ID)	Entrez l'ID de routeur pour identifier le routeur BGP.
Survie (Keep Alive)	Entrez la durée de survie BGP en secondes. Le temporisateur par défaut est de 60 secondes.
Temporisateurs de retenue (Hold Timers)	Entrez la durée de retenue BGP en secondes. Le temporisateur par défaut est de 180 secondes.
Désactiver la transmission AS-PATH (Disable AS-PATH Carry Over)	Cochez cette case pour désactiver la transmission AS-PATH, ce qui influence la valeur AS-PATH sortante pour faire en sorte que les routeurs L3 optent pour un chemin d'accès à un routeur PE (Provider Edge). Si vous sélectionnez cette option, veillez à régler votre réseau pour éviter les boucles de routage. Il est recommandé de ne pas cocher cette case.

Cliquez sur **Mettre à jour (Update)** pour enregistrer les paramètres. En outre, cliquez sur **Enregistrer les modifications (Save Changes)** sur la page **Configuration du client (Customer Configuration)** pour activer les paramètres.

Gérer les partenaires

9

L'option **Gérer les partenaires (Manage Partners)** vous permet de créer des partenaires qui peuvent gérer de manière indépendante un groupe de clients.

Dans le panneau Opérateur (Operator), cliquez sur **Gérer les partenaires (Manage Partners)**. Cliquez sur **Actions** pour effectuer les activités suivantes :

- **Nouveau partenaire (New Partner)** : crée un partenaire. Reportez-vous à la section Créer un partenaire.
- **Modifier le partenaire (Modify Partner)** : permet d'accéder à la rubrique **Présentation du partenaire (Partner Overview)** dans le portail de partenaires, dans lequel vous pouvez configurer d'autres paramètres correspondant au partenaire sélectionné. Vous pouvez également cliquer sur un nom de partenaire pour accéder au portail de partenaires. Pour plus d'informations, reportez-vous à la section Configurer les informations sur les partenaires.
- **Supprimer un partenaire (Delete Partner)** : supprime les partenaires sélectionnés. Assurez-vous d'avoir supprimé tous les clients associés au partenaire sélectionné, avant de supprimer le partenaire.
- **Ajouter des profils d'opérateur (Add Operator Profiles)** : attribue un profil d'opérateur aux partenaires sélectionnés, qui spécifie les paramètres réseau gérés par SD-WAN Orchestrator. Après avoir sélectionné les partenaires, cliquez sur **Actions > Ajouter des profils d'opérateur (Add Operator Profiles)**. Dans la fenêtre **Ajouter un profil aux partenaires sélectionnés (Add Profile to Selected Partners)**, sélectionnez un profil dans le menu déroulant **Profil d'opérateur (Operator profile)**, puis cliquez sur **Envoyer (Submit)**.

  Note Le menu déroulant **Profil d'opérateur (Operator profile)** affiche uniquement les profils d'opérateurs ayant des images qui ne sont pas obsolètes.

  Pour plus d'informations sur les profils d'opérateurs, reportez-vous à la section Gérer les profils d'opérateur.

Ce chapitre contient les rubriques suivantes :

Créer un partenaire

Sur le portail opérateur, vous pouvez créer des partenaires et configurer les paramètres afin que les partenaires puissent gérer eux-mêmes un groupe de clients.

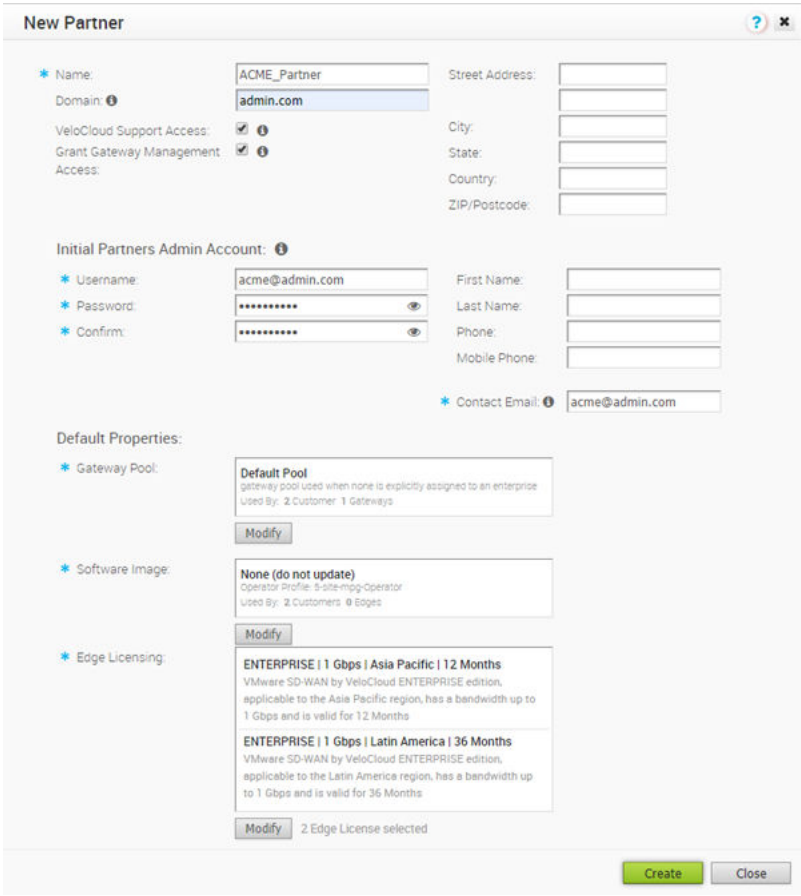
Seuls les super utilisateurs opérateurs, les opérateurs standard et les opérateurs experts commerciaux peuvent créer un partenaire.

Note En tant que super utilisateur opérateur, vous pouvez désactiver temporairement la création de partenaires en définissant la propriété système `session.options.disableCreateEnterpriseProxy` sur Vrai (True). Vous pouvez utiliser cette option lorsque SD-WAN Orchestrator dépasse la capacité d'utilisation.

Sur le portail opérateur, accédez à **Gérer les partenaires (Manage Partners)**.

1 Sur la page **Gérer les partenaires (Manage Partners)**, cliquez sur **Nouveau partenaire (New Partner)** ou sur **Actions > Nouveau partenaire (New Partner)**.

2 Dans la fenêtre **Nouveau partenaire (New Partner)**, entrez les informations suivantes :



Option	Description
Nom (Name)	Entrer le nom du partenaire
Domaine (Domain)	Entrer le nom de domaine du partenaire
Accès au support VeloCloud (VeloCloud Support Access)	Cette option est sélectionnée par défaut et accorde l'accès au support VMware pour afficher, configurer et dépanner les paramètres du partenaire.
Accorder l'accès à la gestion des passerelles (Grant Gateway Management Access)	Cochez cette case pour permettre au partenaire de créer et de gérer les passerelles.
Adresse postale (Street Address), Ville (City), État (State), Pays (Country), Code postal (ZIP/Postcode)	Entrez les informations d'adresse appropriées dans les champs correspondants.

Tableau 9-1. Compte d'administrateur des partenaires initiaux (Initial Partners Admin Account)

Option	Description
Nom d'utilisateur (Username)	Entrez le nom d'utilisateur au format **utilisateur@domaine.com**.
Mot de passe (Password)	Entrez un mot de passe pour le partenaire.
Confirmer (Confirm)	Entrez à nouveau le mot de passe.

Tableau 9-1. Compte d'administrateur des partenaires initiaux (Initial Partners Admin Account) (suite)

Option	Description
Prénom (First Name), Nom de famille (Last Name), Téléphone (Phone), Téléphone portable (Mobile Phone)	Entrez les informations, telles que le nom et le numéro de téléphone dans les champs appropriés.
E-mail du contact (Contact Email)	Entrez l'adresse e-mail. Les alertes relatives à l'état du service sont envoyées à cette adresse e-mail.

Propriétés par défaut (Default Properties)

Par défaut, les propriétés suivantes sont attribuées aux clients gérés par le partenaire. Si nécessaire, le partenaire peut modifier les paramètres de chaque client.

Tableau 9-2.

Option	Description
Pool de passerelles (Gateway Pool)	Pour sélectionner le pool de passerelles SD-WAN Gateway Pool dans la liste disponible, cliquez sur **Ajouter (Add)**. Après avoir ajouté les pools SD-WAN Gateway Pools, vous pouvez cliquer sur **Modifier (Modify)** pour ajouter ou supprimer des pools. Pour plus d'informations sur les pools de passerelles SD-WAN Gateway Pools, reportez-vous à la section Chapitre 13 Gérer les pools de passerelles et les passerelles.
Image logicielle (Software Image)	Pour sélectionner l'image logicielle dans la liste disponible, cliquez sur **Ajouter (Add)**. Après avoir ajouté l'image logicielle, vous pouvez cliquer sur **Modifier (Modify)** pour ajouter ou supprimer les images. Pour plus d'informations sur les images logicielles, reportez-vous à la section Chapitre 10 Images logicielles.
Gestion des licences Edge	Pour sélectionner les licences SD-WAN Edge dans la liste disponible, cliquez sur **Ajouter (Add)**. Après avoir ajouté les licences, vous pouvez cliquer sur **Modifier (Modify)** pour ajouter ou supprimer les licences. Cette option est disponible uniquement lorsque la valeur de la propriété système **session.options.enableEdgeLicensing** est définie sur True. **Note** Vous pouvez utiliser les types de licences sur plusieurs dispositifs VMware SD-WAN Edges. Il est recommandé de fournir aux partenaires l'accès à tous les types de licences pour faire correspondre leur édition et leur région. Pour plus d'informations, reportez-vous à la section Chapitre 16 Gestion des licences Edge.

Cliquez sur **Créer (Create)**.

Le nouveau nom du partenaire s'affiche sur la page **Gérer les partenaires (Manage Partners)**. Vous pouvez cliquer sur le nom du partenaire pour accéder au portail partenaire et ajouter d'autres configurations au partenaire. Reportez-vous à la section Configurer les informations sur les partenaires.

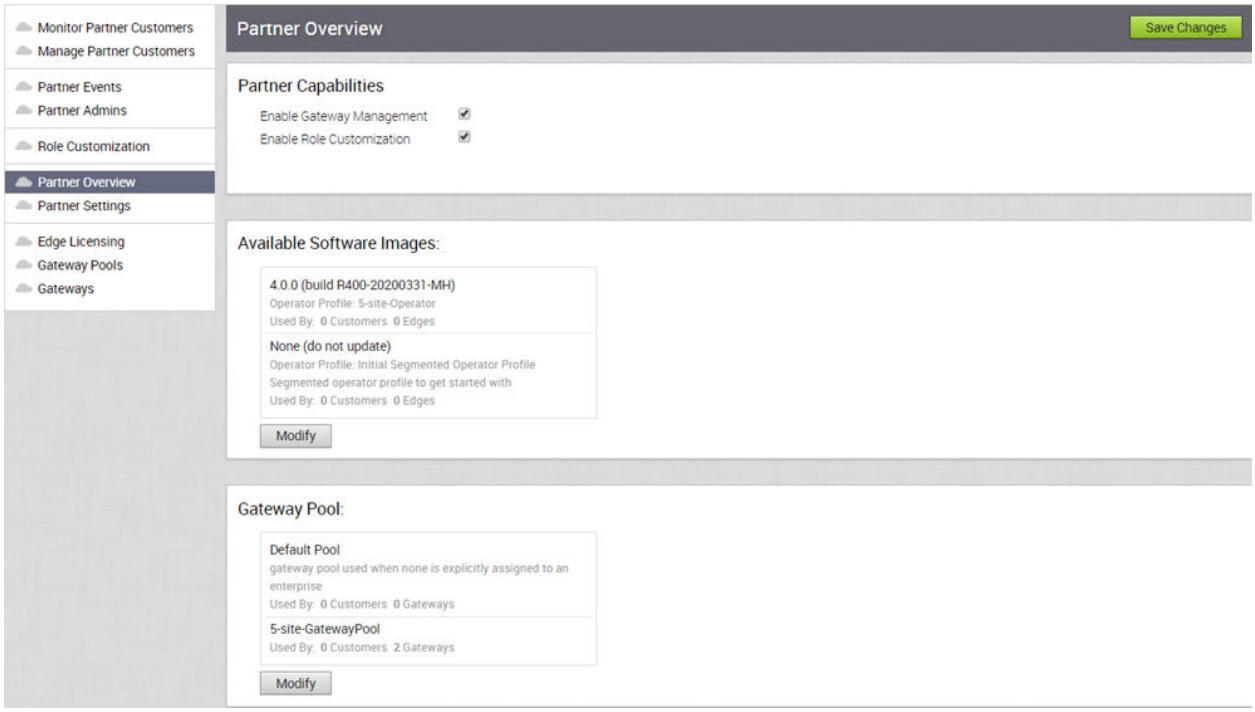
Configurer les informations sur les partenaires

Après avoir créé un partenaire, configurez les options et les paramètres de fonctionnalité auxquels le partenaire peut accéder. En tant qu'opérateur, vous pouvez choisir les paramètres que le partenaire peut modifier et utiliser pour configurer les utilisateurs d'entreprise du partenaire.

Lorsque vous créez un partenaire, vous êtes redirigé vers la page **Présentation du partenaire (Partner Overview)** sur laquelle vous pouvez configurer les paramètres du client.

Vous pouvez également accéder à la page Présentation (Overview) à partir de la page **Gérer les partenaires (Manage Partners)** du portail Orchestrator. Sélectionnez le partenaire, puis cliquez sur **Actions > Modifier (Modify)** ou sur le lien d'accès au partenaire.

Dans le portail de partenaires, cliquez sur **Présentation du partenaire (Partner Overview)** et configurez les paramètres suivants.



Fonctionnalités des partenaires

Vous pouvez activer ou désactiver les capacités suivantes pour le partenaire sélectionné :

- **Activer la gestion des passerelles (Enable Gateway Management)** : autorise l'activation ou la désactivation des utilisateurs partenaires pour créer, configurer et gérer leurs propres passerelles.

- **Activer la personnalisation des rôles (Enable Role Customization)** : permet d'activer ou de désactiver un super utilisateur partenaire afin de personnaliser les privilèges de rôle des autres utilisateurs partenaires et des utilisateurs d'entreprise du partenaire. Cette option est activée par défaut.

Images logicielles disponibles (Available Software Images)

Affiche toutes les images logicielles attribuées au partenaire. Cliquez sur **Modifier (Modify)** pour ajouter ou supprimer les images logicielles dans la liste.

Note Vous ne pouvez pas supprimer les images logicielles attribuées à un client.

Pool de passerelles (Gateway Pool)

Affiche les pools de passerelles associés au partenaire sélectionné. Cliquez sur **Modifier (Modify)** pour ajouter ou supprimer les pools de passerelles dans la liste.

Note Vous ne pouvez pas supprimer les pools de passerelle attribués à un client.

Images logicielles

10

Le portail d'Orchestrator permet aux super utilisateurs opérateurs et aux administrateurs standard opérateurs de gérer les images logicielles des dispositifs Edge associés.

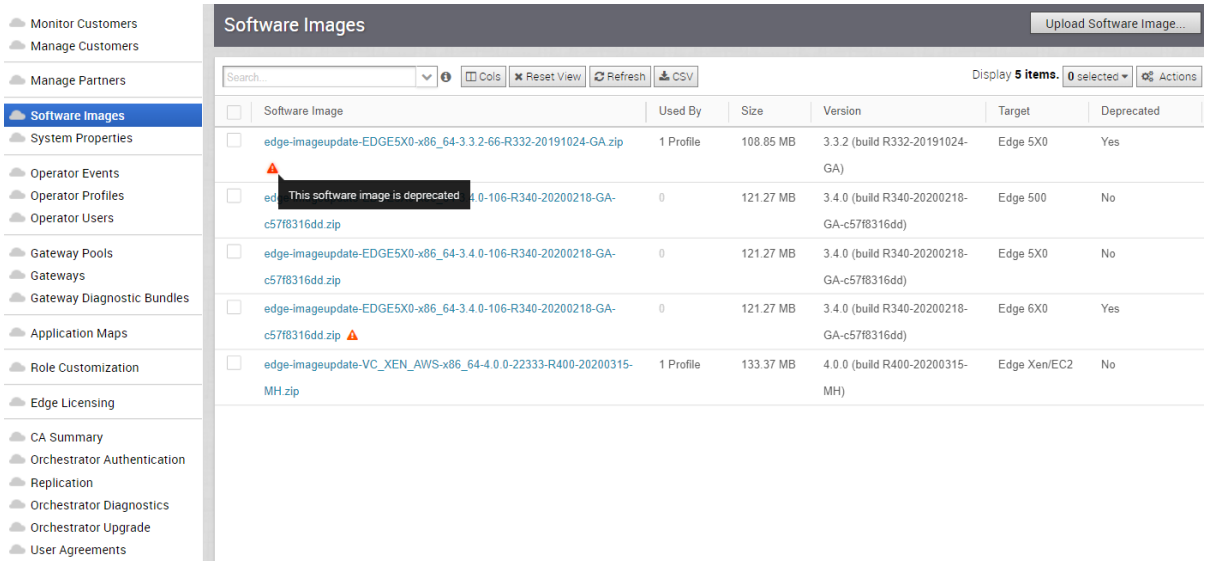
En tant que super utilisateur opérateur, vous pouvez télécharger une nouvelle image logicielle, modifier les images logicielles existantes et supprimer une image logicielle associée aux dispositifs Edge.

Procédure

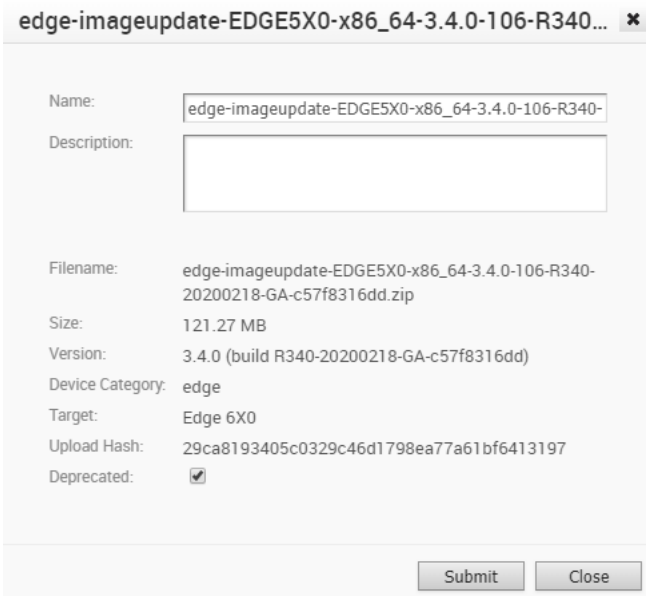
1 Pour télécharger une nouvelle image logicielle, dans le portail de l'opérateur, cliquez sur **Images logicielles (Software Images)**.

2 Cliquez sur **Charger une image logicielle (Upload Software Image)** et choisissez un fichier image (format ZIP) à charger à partir de votre stockage local. Orchestrator valide le module et le charge sur le portail. Vous pouvez charger plusieurs images logicielles sur le portail.

3 Les modules chargés s'affichent sur la page **Images logicielles (Software Images)**.



4 Pour modifier une image logicielle chargée, cliquez sur le lien d'accès au nom de l'image ou sélectionnez l'image et cliquez sur **Actions > Modifier l'image logicielle (Modify Software Image)**. La fenêtre contextuelle **Mise à jour de l'image du dispositif Edge (Edge Image Update)**.



5 Vous pouvez mettre à jour le nom et la description du module de l'image logicielle, si nécessaire.

6 Cochez la case **Obsolète (Deprecated)** pour indiquer que l'image logicielle est obsolète, puis cliquez sur **OK**.

L'image logicielle obsolète est signalée et apparaît sur la page **Images logicielles (Software Images)**.

Note Une fois l'image indiquée comme obsolète, elle ne figure plus dans la liste des images logicielles ou des versions disponibles pouvant être attribuées aux profils d'opérateurs, aux clients ou aux dispositifs Edge.

Note Les profils d'opérateurs existants qui contiennent une image obsolète sont signalés pour informer l'utilisateur que la version logicielle du profil contient une image logicielle obsolète.

7 Pour supprimer un module du portail, sélectionnez l'image et cliquez sur **Actions > Supprimer l'image logicielle (Delete Software Image)**.

Étape suivante

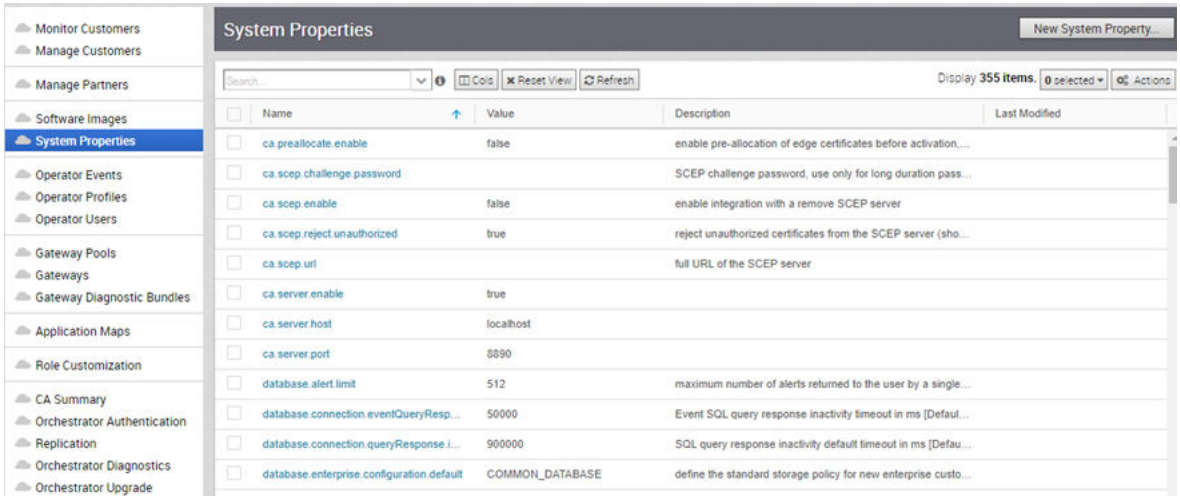
Pour mettre à niveau les dispositifs Edge d'une entreprise avec une image logicielle spécifique, reportez-vous à la section Gérer les profils d'opérateur.

Propriétés système

11

VMware fournit des propriétés système permettant de configurer diverses fonctionnalités et options disponibles dans le portail d'Orchestrator.

Dans le portail de l'opérateur, accédez à la page **Propriétés système (System Properties)**, qui répertorie les propriétés système prédéfinies disponibles.



Pour configurer les propriétés système :

1 Cliquez sur **Nouvelle propriété système (New System Property)** pour ajouter une nouvelle propriété.

2 Dans la fenêtre **Nouvelle propriété système (New System Property)**, entrez un nom pour la nouvelle propriété et choisissez le **Type de données (Data Type)** dans la liste déroulante.

3 Entrez la **Valeur (Value)** de la propriété en fonction du type de données.

4 Entrez une description pour la propriété.

5 Cliquez sur **Enregistrer (Save)**.

6 Pour modifier les valeurs d'une propriété, cliquez sur le lien vers la propriété ou sélectionnez la propriété, puis cliquez sur **Actions > Modifier la propriété système (Modify System Property)**.

7 Pour supprimer une propriété, sélectionnez la propriété et cliquez sur **Actions > Supprimer la propriété système (Delete System Property)**.

Vous pouvez utiliser le champ **Rechercher (Search)** pour rechercher une propriété système spécifique. Reportez-vous à la section Liste des propriétés système, qui répertorie certaines des propriétés système que vous pouvez modifier en tant qu'opérateur.

Note Il est recommandé de contacter le support de VMware avant de modifier les propriétés système.

Ce chapitre contient les rubriques suivantes :

Liste des propriétés système

En tant qu'opérateur, vous pouvez ajouter ou modifier les valeurs des propriétés système.

Les tableaux suivants décrivent certaines des propriétés système. En tant qu'opérateur, vous pouvez définir les valeurs de ces propriétés.

Tableau 11-1. E-mails d'alerte

Propriété système	Description
vco.alert.mail.to	Lorsqu'une alerte est déclenchée, une notification est immédiatement envoyée à la liste des adresses e-mail fournies dans le champ Valeur (Value) de cette propriété système. Vous pouvez entrer plusieurs ID d'e-mail séparés par des virgules. Si la propriété ne contient aucune valeur, la notification n'est pas envoyée. La notification est conçue pour alerter le personnel en charge du support ou des opérations de VMware des problèmes imminents avant d'en informer le client.
vco.alert.mail.cc	Lorsque des e-mails d'alerte sont envoyés à un client, une copie est envoyée aux adresses e-mail indiquées dans le champ Valeur (Value) de cette propriété système. Vous pouvez entrer plusieurs ID d'e-mail séparés par des virgules.
mail.*	Plusieurs propriétés système sont disponibles pour contrôler les e-mails d'alerte. Vous pouvez définir les paramètres de messagerie tels que les propriétés SMTP, le nom d'utilisateur, le mot de passe, etc.

Tableau 11-2. Alertes

Propriété système	Description
vco.alert.enable	Active ou désactive globalement la génération d'alertes pour les opérateurs et les clients d'entreprise.
vco.enterprise.alert.enable	Active ou désactive globalement la génération d'alertes pour les clients d'entreprise.
vco.operator.alert.enable	Active ou désactive globalement la génération d'alertes pour les opérateurs.

Tableau 11-3. Autorité de certification

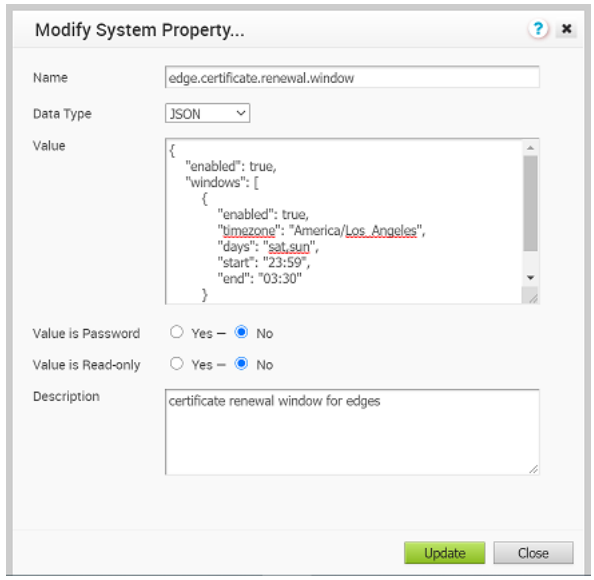
Propriété système	Description
edge.certificate.renewal.window	Cette propriété système facultative permet à l'opérateur de définir une ou plusieurs fenêtres de maintenance au cours desquelles le renouvellement du certificat du dispositif Edge est activé. Les certificats planifiés pour le renouvellement en dehors des fenêtres sont différés jusqu'à ce que l'heure actuelle s'affiche dans l'une des fenêtres activées. Activer la propriété système : Pour activer cette propriété système, entrez « true » pour « enabled » dans la première partie de la zone de texte **Valeur (Value)** dans la boîte de dialogue **Modifier la propriété système (Modify System Property)**. Un exemple de la première partie de cette propriété système, lorsqu'elle est activée, s'affiche ci-dessous. Les opérateurs peuvent définir plusieurs fenêtres pour limiter les jours et les heures du jour durant lesquels les renouvellements du dispositif Edge sont activés. Vous pouvez définir chaque fenêtre selon un jour ou une liste de jours (séparés par une virgule) et des heures de début et de fin. Vous pouvez spécifier les heures de début et de fin par rapport au fuseau horaire local d'un dispositif Edge ou par rapport à l'heure UTC. Reportez-vous à l'image ci-dessous à titre d'exemple.  **Note** Si les attributs sont absents, la valeur par défaut est activée « false ». Lors de la définition des attributs de fenêtres, respectez les points suivants : ■ Utilisez les fuseaux horaires IANA, et non PDT ou PST (par exemple, Amérique/Los_Angeles). Pour plus d'informations, reportez-vous à la section https://en.wikipedia.org/wiki/List_of_tz_database_time_zones.

Tableau 11-3. Autorité de certification (suite)

Propriété système	Description
	■ Utilisez UTC pour les jours (par exemple, SAM, DIM). ■ Séparés par une virgule. ■ Jours en trois lettres en anglais. ■ Non sensible à la casse. ■ Utilisez le format de l'heure militaire 24 heures uniquement (HH:MM) pour les heures de début (par exemple, 01:30) et les heures de fin (par exemple, 05:30). Si les valeurs susmentionnées sont manquantes, les valeurs par défaut des attributs dans chaque définition de fenêtre sont les suivantes : ■ Si le paramètre « enabled » est manquant, la valeur par défaut = false. ■ Si le paramètre « timezone » est manquant, la valeur par défaut = « local ». ■ Si l'un des paramètres « days » ou les heures de début et de fin sont manquants, les valeurs par défaut sont les suivantes : ■ Si le paramètre « days » est manquant, le début ou la fin est appliqué à chaque jour de la semaine (lun, mar, mer, jeu, ven, sam, dim). ■ Si les heures de début et de fin sont manquantes, n'importe quelle heure du jour spécifié correspond (début = 00:00 et fin = 23:59). ■ REMARQUE : l'un des paramètres « days » ou les heures de début et de fin doivent être présents. S'ils sont toutefois manquants, les valeurs par défaut sont indiquées ci-dessus. Désactiver la propriété système : Cette propriété système est désactivée par défaut, ce qui signifie que le certificat est renouvelé automatiquement après son expiration. Le paramètre « enabled » est défini sur « false » dans la première partie de la zone de texte **Valeur (Value)** dans la boîte de dialogue **Modifier la propriété système (Modify System Property)**. Un exemple de cette propriété, lorsqu'elle est désactivée, s'affiche ci-dessous. { « enabled » : false, « windows » : [{ REMARQUE : cette propriété système nécessite l'activation de PKI.
gateway.certificate.renewal.window	Cette propriété système facultative permet à l'opérateur de définir une ou plusieurs fenêtres de maintenance au cours desquelles le renouvellement du certificat de la passerelle est activé. Les certificats planifiés pour le renouvellement en dehors des fenêtres sont différés jusqu'à ce que l'heure actuelle s'affiche dans l'une des fenêtres activées. Activer la propriété système :

Tableau 11-3. Autorité de certification (suite)

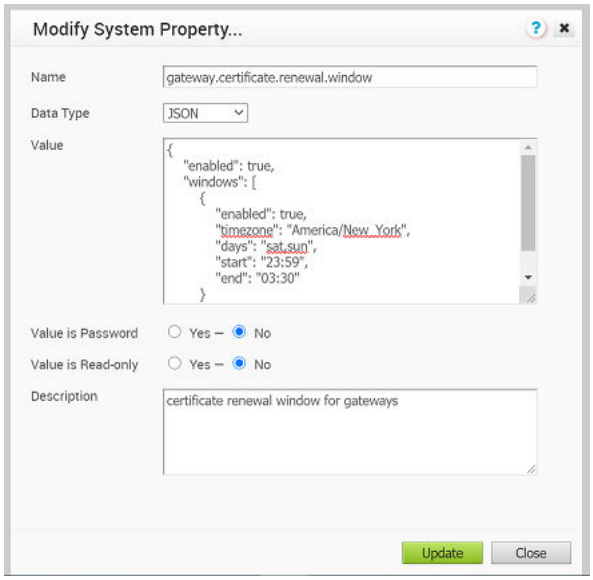
Propriété système	Description
	Pour activer cette propriété système, entrez « true » pour « enabled » dans la première partie de la zone de texte **Valeur (Value)** dans la boîte de dialogue **Modifier la propriété système (Modify System Property)**. Reportez-vous à l'image ci-dessous à titre d'exemple. Les opérateurs peuvent définir plusieurs fenêtres pour limiter les jours et les heures du jour durant lesquels les renouvellements du dispositif Edge sont activés. Vous pouvez définir chaque fenêtre selon un jour ou une liste de jours (séparés par une virgule) et des heures de début et de fin. Vous pouvez spécifier les heures de début et de fin par rapport au fuseau horaire local d'un dispositif Edge ou par rapport à l'heure UTC. Reportez-vous à l'image ci-dessous à titre d'exemple.  **Note** Si les attributs sont absents, la valeur par défaut est activée « false ». Lors de la définition des attributs de fenêtres, respectez les points suivants : ■ Utilisez les fuseaux horaires IANA, et non PDT ou PST (par exemple, Amérique/Los_Angeles). Pour plus d'informations, reportez-vous à la section https://en.wikipedia.org/wiki/List_of_tz_database_time_zones. ■ Utilisez UTC pour les jours (par exemple, SAM, DIM). ■ Séparés par une virgule. ■ Jours en trois lettres en anglais. ■ Non sensible à la casse. ■ Utilisez le format de l'heure militaire 24 heures uniquement (HH:MM) pour les heures de début (par exemple, 01:30) et les heures de fin (par exemple, 05:30).

Tableau 11-3. Autorité de certification (suite)

Propriété système	Description
	Si les valeurs susmentionnées sont manquantes, les valeurs par défaut des attributs dans chaque définition de fenêtre sont les suivantes : ■ Si le paramètre « enabled » est manquant, la valeur par défaut = false. ■ Si le paramètre « timezone » est manquant, la valeur par défaut = « local ». ■ Si l'un des paramètres « days » ou les heures de début et de fin sont manquants, les valeurs par défaut sont les suivantes : ■ Si le paramètre « days » est manquant, le début ou la fin est appliqué à chaque jour de la semaine (lun, mar, mer, jeu, ven, sam, dim). ■ Si les heures de début et de fin sont manquantes, n'importe quelle heure du jour spécifié correspond (début = 00:00 et fin = 23:59). ■ REMARQUE : l'un des paramètres « days » ou (fin et début) doivent être présents. S'ils sont toutefois manquants, les valeurs par défaut sont indiquées ci-dessus. Désactiver la propriété système : Cette propriété système est désactivée par défaut, ce qui signifie que le certificat est renouvelé automatiquement après son expiration. Le paramètre « enabled » est défini sur « false » dans la première partie de la zone de texte **Valeur (Value)** dans la boîte de dialogue **Modifier la propriété système (Modify System Property)**. Un exemple de cette propriété, lorsqu'elle est désactivée, s'affiche ci-dessous. { « enabled » : false, « windows » : [{ REMARQUE : cette propriété système nécessite l'activation de PKI.

Tableau 11-4. Rétention des données

Propriété système	Description
retention.highResFlows.days	Cette propriété système permet aux opérateurs de configurer la rétention des données de statistiques de flux haute résolution n'importe où entre 1 et 90 jours.
retention.lowResFlows.months	Cette propriété système permet aux opérateurs de configurer la rétention des données de statistiques de flux faible résolution n'importe où entre 1 et 365 jours.
session.options.maxFlowstatsRetentionDays	Cette propriété permet aux opérateurs d'interroger plus de deux semaines de données de statistiques de flux.

Tableau 11-5. Dispositifs Edge

Propriété système	Description
edge.offline.limit.sec	Si Orchestrator ne détecte pas de pulsation sur un dispositif Edge pendant la durée spécifiée, l'état du dispositif Edge passe en mode hors ligne.
edge.link.unstable.limit.sec	Lorsqu'Orchestrator ne reçoit pas de statistiques de lien pour un lien pendant la durée spécifiée, le lien passe en mode instable.
edge.link.disconnected.limit.sec	Lorsqu'Orchestrator ne reçoit pas de statistiques de lien pour un lien pendant la durée spécifiée, le lien est déconnecté.
edge.deadbeat.limit.days	Si un dispositif Edge n'est pas actif pendant le nombre de jours spécifié, le dispositif Edge n'est pas pris en compte pour la génération des alertes.
vco.operator.alert.edgeLinkEvent.enable	Active ou désactive globalement les alertes d'opérateur pour les événements de liens Edge.
vco.operator.alert.edgeLiveness.enable	Active ou désactive globalement les alertes d'opérateur pour les événements de réactivité Edge.

Tableau 11-6. Activation du dispositif Edge (Edge Activation)

Propriété système	Description
edge.activation.key.encode.enable	Base64 encode les paramètres de l'URL d'activation pour masquer les valeurs lorsque l'e-mail d'activation du dispositif Edge est envoyé au contact du site.
edge.activation.trustedIssuerReset.enable	Réinitialise la liste d'émetteurs de certificats approuvés du dispositif Edge pour qu'elle ne contienne que l'autorité de certification Orchestrator. L'ensemble du trafic TLS à partir du dispositif Edge est limité par la nouvelle liste d'émetteurs.
network.public.certificate.issuer	Définissez la valeur de **network.public.certificate.issuer** sur celle du codage PEM de l'émetteur de certificats de serveur Orchestrator, lorsque **edge.activation.trustedIssuerReset.enable** est défini sur Vrai (True). Cette action ajoute l'émetteur de certificats de serveur à l'émetteur approuvé du dispositif Edge, en plus de l'autorité de certification Orchestrator.

Tableau 11-7. Surveillance

Propriété système	Description
vco.monitor.enable	Active ou désactive globalement la surveillance des états des entités d'entreprise et d'opérateur. Définir la valeur sur **False** empêche SD-WAN Orchestrator de modifier les états d'entité et de déclencher des alertes.
vco.enterprise.monitor.enable	Active ou désactive globalement la surveillance des états des entités d'entreprise.
vco.operator.monitor.enable	Active ou désactive globalement la surveillance des états des entités d'opérateur.

Tableau 11-8. Notifications

Propriété système	Description
vco.notification.enable	Active ou désactive globalement la remise des notifications d'alerte à l'opérateur et aux entreprises.
vco.enterprise.notification.enable	Active ou désactive globalement la remise des notifications d'alerte aux entreprises.
vco.operator.notification.enable	Active ou désactive globalement la remise des notifications d'alerte à l'opérateur.

Tableau 11-9. Réinitialisation et verrouillage du mot de passe

Propriété système	Description
vco.enterprise.resetPassword.token.expirySeconds	Durée après laquelle le lien de réinitialisation du mot de passe pour un utilisateur d'entreprise expire.
vco.enterprise.authentication.passwordPolicy	Définit la stratégie d'expiration du mot de passe et d'historique des mots de passe pour les utilisateurs d'entreprise. Modifiez le modèle JSON dans le champ Valeur (Value) pour définir les éléments suivants : **expiration (expiry)** : ■ **activer (enable)** : définissez cette option sur **true** pour activer l'expiration automatique des mots de passe des utilisateurs d'entreprise. ■ **jours (days)** : entrez le nombre de jours pendant lesquels un mot de passe d'entreprise peut être utilisé avant l'expiration forcée. **historique (history)** : ■ **activer (enable)** : définissez cette option sur **true** pour activer l'enregistrement des mots de passe précédents des utilisateurs d'entreprise. ■ **nombre (count)** : entrez le nombre de mots de passe précédents à enregistrer dans l'historique. Lorsqu'un utilisateur d'entreprise tente de modifier le mot de passe, le système ne lui permet pas d'entrer un mot de passe déjà enregistré dans l'historique.
enterprise.user.lockout.defaultAttempts	Nombre de fois que l'utilisateur d'entreprise peut essayer de se connecter. Si la connexion échoue pendant le nombre de fois spécifié, le compte est verrouillé.
enterprise.user.lockout.defaultDurationSeconds	Durée de verrouillage du compte d'utilisateur d'entreprise.
enterprise.user.lockout.enabled	Active ou désactive l'option de verrouillage pour les échecs de connexion de l'entreprise.
vco.operator.resetPassword.token.expirySeconds	Durée après laquelle le lien de réinitialisation du mot de passe pour un utilisateur opérateur expire.

Tableau 11-9. Réinitialisation et verrouillage du mot de passe (suite)

Propriété système	Description
vco.operator.authentication.passwordPolicy	Définit la stratégie d'expiration du mot de passe et d'historique des mots de passe pour les utilisateurs opérateurs. Modifiez le modèle JSON dans le champ Valeur (Value) pour définir les éléments suivants : **expiration (expiry)** : ■ **activer (enable)** : définissez cette option sur **true** pour activer l'expiration automatique des mots de passe des utilisateurs opérateurs. ■ **jours (days)** : entrez le nombre de jours pendant lesquels un mot de passe d'opérateur peut être utilisé avant l'expiration forcée. **historique (history)** : ■ **activer (enable)** : définissez cette option sur **true** pour activer l'enregistrement des mots de passe précédents des utilisateurs opérateurs. ■ **nombre (count)** : entrez le nombre de mots de passe précédents à enregistrer dans l'historique. Lorsqu'un utilisateur opérateur tente de modifier le mot de passe, le système ne lui permet pas d'entrer un mot de passe déjà enregistré dans l'historique.
operator.user.lockout.defaultAttempts	Nombre de fois que l'utilisateur opérateur peut essayer de se connecter. Si la connexion échoue pendant le nombre de fois spécifié, le compte est verrouillé.
operator.user.lockout.defaultDurationSeconds	Durée de verrouillage du compte de l'utilisateur opérateur.
operator.user.lockout.enabled	Active ou désactive l'option de verrouillage pour les échecs de connexion de l'opérateur.

Tableau 11-10. API de limite de débit

Propriété système	Description
vco.api.rateLimit.enabled	Autorise les super utilisateurs opérateurs à activer ou désactiver la fonctionnalité de limite de débit au niveau du système. Par défaut, cette valeur est définie sur **Faux (False)**. **Note** Le limiteur de débit n'est pas réellement activé, c'est-à-dire, il ne rejette pas les demandes d'API qui dépassent les limites configurées, sauf si le paramètre **vco.api.rateLimit.mode.logOnly** est désactivé.
vco.api.rateLimit.mode.logOnly	Permet au super utilisateur opérateur d'utiliser la limite de débit dans un mode **LOG_ONLY**. Lorsque la valeur est définie sur **Vrai (True)** et si une limite de débit est dépassée, cette option journalise uniquement l'erreur et déclenche des mesures correspondantes permettant aux clients d'effectuer des demandes sans limite de débit. Lorsque la valeur est définie sur **Faux (False)**, l'API de demande est limitée par des stratégies définies et HTTP 429 est renvoyé.

Tableau 11-10. API de limite de débit (suite)

Propriété système	Description
vco.api.rateLimit.rules.global	Permet de définir un ensemble de stratégies applicables globalement utilisées par le limiteur de débit dans un tableau JSON. Par défaut, la valeur est un tableau vide. Chaque type d'utilisateur (opérateur, partenaire et client) peut effectuer jusqu'à 500 demandes toutes les 5 secondes. Le nombre de demandes est soumis à une modification en fonction du modèle de comportement des demandes limitées du débit. Le tableau JSON comporte les paramètres suivants : **Types** : les objets de type représentent des contextes différents dans lesquels les limites de débit sont appliquées. Vous trouverez ci-après les différents objets de type disponibles : ■ **SYSTEM** : spécifie une limite globale partagée par tous les utilisateurs. ■ **OPERATOR_USER** : limite pouvant être définie en général pour tous les utilisateurs opérateurs. ■ **ENTERPRISE_USER** : limite pouvant être définie en général pour tous les utilisateurs d'entreprise. ■ **MSP_USER** : limite pouvant être définie en général pour tous les utilisateurs MSP. ■ **ENTERPRISE** : limite pouvant être partagée entre tous les utilisateurs d'une entreprise et qui s'applique à toutes les entreprises du réseau. ■ **PROXY** : limite pouvant être partagée entre tous les utilisateurs d'un proxy et qui s'applique à tous les proxies. **Stratégies (Policies)** : ajoutez des règles aux stratégies pour appliquer les demandes qui correspondent à la règle, en configurant les paramètres suivants : ■ **Correspondance (Match)** : entrez le type de demandes à mettre en correspondance : ■ **Tout (All)** : limitez le débit de toutes les demandes correspondant à l'un des objets de type. ■ **METHOD** : limitez le débit de toutes les demandes correspondant au nom de méthode spécifié. ■ **METHOD_PREFIX** : limitez le débit de toutes les demandes correspondant au groupe de méthodes spécifié. ■ **Règles (Rules)** : entrez les valeurs des paramètres suivants : ■ **maxConcurrent** : nombre de tâches pouvant être effectuées simultanément. ■ **reservoir** : nombre de tâches pouvant être effectuées avant que le limiteur n'arrête leur exécution.

Tableau 11-10. API de limite de débit (suite)

Propriété système	Description
	■ **reservoirRefreshAmount** : valeur permettant de définir le réservoir sur le moment d'utilisation du paramètre **reservoirRefreshInterval**. ■ **reservoirRefreshInterval** : pour chaque milliseconde de **reservoirRefreshInterval**, la valeur **reservoir** est automatiquement mise à jour sur la valeur de **reservoirRefreshAmount**. La valeur **reservoirRefreshInterval** doit être un multiple de 250 (5 000 pour le clustering). **Activé (Enabled)** :vous pouvez activer ou désactiver chaque type de limite en incluant la clé **enabled** dans **APIRateLimiterTypeObject**. Par défaut, la valeur du paramètre **enabled** est Vrai (True), même si la clé n'est pas incluse. Vous devez inclure la clé **"enabled": false** pour désactiver les limites de type individuelles. L'exemple suivant montre un exemple de fichier JSON avec les valeurs par défaut : `[{ "type": "OPERATOR_USER", "policies": [{ "match": { "type": "ALL" }, "rules": { "reservoir": 500, "reservoirRefreshAmount": 500, "reservoirRefreshInterval": 5000 } }] }, { "type": "MSP_USER", "policies": [{ "match": { "type": "ALL" }, "rules": { "reservoir": 500, "reservoirRefreshAmount": 500, "reservoirRefreshInterval": 5000 } }] }, { "type": "ENTERPRISE_USER", "policies": [{`

Tableau 11-10. API de limite de débit (suite)

Propriété système	Description

	<pre>"match": {
	"type": "ALL"
	},
	"rules": {
	"reservoir": 500,
	"reservoirRefreshAmount": 500,
	"reservoirRefreshInterval": 5000
	}
	}
	]
	}
	]</pre>
	Note Il est recommandé de ne pas modifier les valeurs par défaut des paramètres de configuration.

vco.api.rateLimit.rules.enterprise.default	Comprend l'ensemble par défaut de stratégies spécifiques à l'entreprise appliquées aux clients récemment créés. Les propriétés spécifiques au client sont stockées dans la propriété **vco.api.rateLimit.rules.enterprise** d'entreprise.
vco.api.rateLimit.rules.enterpriseProxy.default	Comprend l'ensemble par défaut de stratégies spécifiques à l'entreprise appliquées aux partenaires récemment créés. Les propriétés spécifiques au partenaire sont stockées dans la propriété **vco.api.rateLimit.rules.enterpriseProxy** de proxy d'entreprise.

Pour plus d'informations sur la limite du débit, reportez-vous à la section Demandes d'API de limite de débit.

Tableau 11-11. Diagnostics à distance

Propriété système	Description
network.public.address	Spécifie l'adresse d'origine du navigateur/le nom d'hôte DNS qui est utilisé(e) pour accéder à l'interface utilisateur de SD-WAN Orchestrator.
network.portal.websocket.address	Permet de définir un(e) autre nom d'hôte DNS/adresse pour accéder à l'interface utilisateur de SD-WAN Orchestrator à partir d'un navigateur, si l'adresse du navigateur n'est pas la même que la valeur de la propriété système `network.public.address`. Comme les diagnostics à distance utilisent désormais une connexion WebSocket, pour garantir la sécurité Web, l'adresse d'origine du navigateur qui est utilisée pour accéder à l'interface utilisateur d'Orchestrator est validée pour les demandes entrantes. Dans la plupart des cas, cette adresse est identique à la propriété système `network.public.address`. Dans de rares cas, l'interface utilisateur d'Orchestrator est accessible à l'aide d'un(e) autre nom d'hôte DNS/adresse différent(e) de la valeur définie dans la propriété système `network.public.address`. Dans ce cas, vous pouvez définir cette propriété système sur l'autre nom d'hôte DNS/adresse. Par défaut, cette valeur n'est pas définie.
session.options.websocket.portal.idle.timeout	Permet de définir la durée totale (en secondes) pendant laquelle la connexion WebSocket du navigateur reste active même si elle ne présente aucune activité. Par défaut, la connexion du navigateur WebSocket reste active pendant 300 secondes même si elle ne présente aucune activité.

Tableau 11-12. Réinitialisation du mot de passe en libre-service

Propriété système	Description
vco.enterprise.resetPassword.twoFactor.mode	Définit le mode de l'authentification de second niveau de la réinitialisation du mot de passe pour tous les utilisateurs d'entreprise. Actuellement, seul le mode SMS est pris en charge.
vco.enterprise.resetPassword.twoFactor.required	Active ou désactive l'authentification à deux facteurs pour la réinitialisation du mot de passe des utilisateurs d'entreprise.
vco.enterprise.selfResetPassword.enabled	Active ou désactive la réinitialisation du mot de passe en libre-service pour les utilisateurs d'entreprise.
vco.enterprise.selfResetPassword.token.expirySeconds	Durée après laquelle le lien de réinitialisation du mot de passe en libre-service pour un utilisateur d'entreprise expire.
vco.operator.resetPassword.twoFactor.required	Active ou désactive l'authentification à deux facteurs pour la réinitialisation du mot de passe des utilisateurs opérateurs.

Tableau 11-12. Réinitialisation du mot de passe en libre-service (suite)

Propriété système	Description
vco.operator.selfResetPassword.enabled	Active ou désactive la réinitialisation du mot de passe en libre-service pour les utilisateurs opérateurs.
vco.operator.selfResetPassword.token.expirySeconds	Durée après laquelle le lien de réinitialisation du mot de passe en libre-service pour un utilisateur opérateur expire.

Tableau 11-13. Authentification à deux facteurs

Propriété système	Description
vco.enterprise.authentication.twoFactor.enable	Active ou désactive l'authentification à deux facteurs pour les utilisateurs d'entreprise.
vco.enterprise.authentication.twoFactor.mode	Définit le mode de l'authentification de second niveau pour les utilisateurs d'entreprise. Actuellement, seul SMS est pris en charge en tant que mode d'authentification de second niveau.
vco.enterprise.authentication.twoFactor.require	Définit l'authentification à deux facteurs comme obligatoire pour les utilisateurs d'entreprise.
vco.operator.authentication.twoFactor.enable	Active ou désactive l'authentification à deux facteurs pour les utilisateurs opérateurs.
vco.operator.authentication.twoFactor.mode	Définit le mode de l'authentification de second niveau pour les utilisateurs opérateurs. Actuellement, seul SMS est pris en charge en tant que mode d'authentification de second niveau.
vco.operator.authentication.twoFactor.require	Définit l'authentification à deux facteurs comme obligatoire pour les utilisateurs opérateurs.

Tableau 11-14. Configuration VNF

Propriété système	Description

edge.vnf.extraImageInfos	Définit les propriétés d'une image VNF.
	Vous pouvez entrer les informations suivantes pour une image VNF, au format JSON dans le champ **Valeur (Value)** :
	`[ { "vendor": "Nom du fournisseur (Vendor Name)", "version": "Version d'image VNF (VNF Image Version)", "checksum": "Valeur de total de contrôle VNF (VNF Checksum Value)", "checksumType": "Type de total de contrôle VNF (VNF Checksum Type)" } ]`
	Exemple de fichier JSON pour l'image de pare-feu Check Point :
	`[ { "vendor": "checkPoint", "version": "r80.40_no_workaround_46", "checksum": "bc9b06376cdbf210cad8202d728f1602b79cfd7d", "checksumType": "sha-1" } ]`
	Exemple de fichier JSON de système d'exploitation pour l'image de pare-feu Fortinet :
	`[ { "vendor": "fortinet", "version": "624", "checksum": "6d9e2939b8a4a02de499528c745d76bf75f9821f", "checksumType": "sha-1" } ]`

edge.vnf.metric.record.limit	Définit le nombre d'enregistrements à stocker dans la base de données
enterprise.capability.edgeVnfs.enable	Active le déploiement de VNF sur les modèles de dispositifs Edge pris en charge.
enterprise.capability.edgeVnfs.securityVnf.checkPoint	Active la VNF du pare-feu de réseaux Check Point
enterprise.capability.edgeVnfs.securityVnf.fortinet	Active la VNF du pare-feu de réseaux Fortinet
enterprise.capability.edgeVnfs.securityVnf.paloAlto	Active la VNF du pare-feu de Palo Alto Networks

Tableau 11-14. Configuration VNF (suite)

Propriété système	Description
session.options.enableVnf	Active la fonctionnalité VNF
vco.operator.alert.edgeVnfEvent.enable	Active ou désactive globalement les alertes d'opérateur pour les événements VNF des dispositifs Edge.
vco.operator.alert.edgeVnfInsertionEvent.enable	Active ou désactive globalement les alertes d'opérateur pour les événements d'insertion de VNF des dispositifs Edge.

Tableau 11-15. VPN

Propriété système	Description
vpn.disconnect.wait.sec	Intervalle de temps pendant lequel le système doit attendre avant de déconnecter un tunnel VPN.
vpn.reconnect.wait.sec	Intervalle de temps pendant lequel le système doit attendre avant de reconnecter un tunnel VPN.

Gérer les opérateurs

12

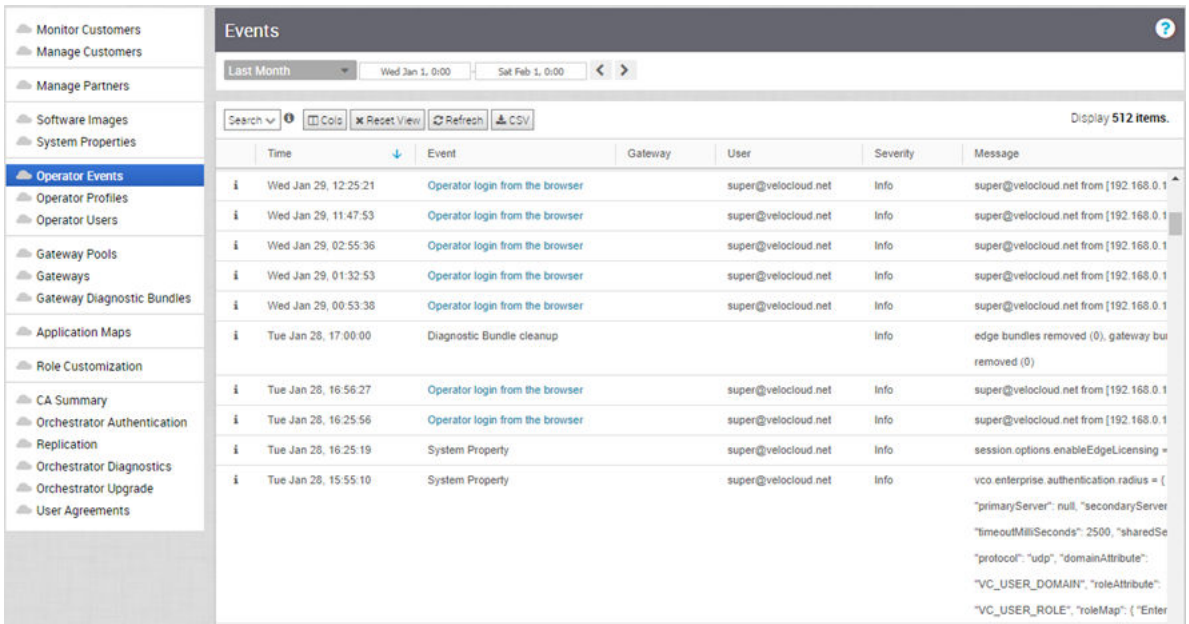
Dans le portail de l'opérateur, vous pouvez configurer et gérer des profils d'opérateur et des utilisateurs opérateurs. Vous pouvez également afficher les événements déclenchés par des opérateurs.

Ce chapitre contient les rubriques suivantes :

Surveiller les événements d'opérateur

Les événements d'opérateur sont déclenchés par les activités des opérateurs. Ils permettent de déterminer l'état du système VMware.

Dans le portail de l'opérateur, cliquez sur **Événements d'opérateur (Operator Events)**.



La page affiche les événements d'opérateur récents. Vous pouvez cliquer sur le lien vers les événements pour afficher plus de détails.

Pour afficher les anciens événements, cliquez sur le menu déroulant en haut de la page et choisissez la durée dans la liste. Sinon, vous pouvez également entrer les dates de début et de fin en haut de la page pour définir une durée personnalisée.

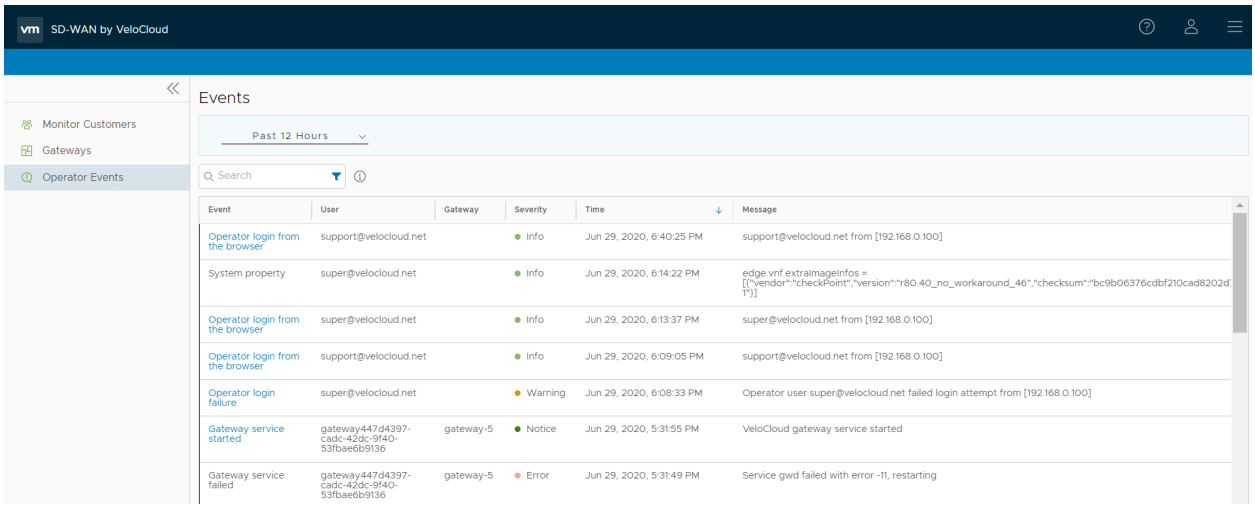
Une fois que vous avez choisi ou configuré la durée, la page affiche les événements déclenchés au cours de la période sélectionnée.

La page affiche les options suivantes :

- **Rechercher (Search)** : entrez un terme pour rechercher un détail spécifique. Cliquez sur la flèche déroulante pour filtrer la vue selon des critères spécifiques.
- **Colonnes (Cols)** : cliquez dessus et sélectionnez les colonnes à afficher ou à masquer dans la vue.
- **Réinitialiser la vue (Reset View)** : cliquez dessus pour rétablir les paramètres par défaut de la vue.
- **Actualiser (Refresh)** : cliquez dessus pour actualiser les détails affichés avec les données les plus récentes.
- **CSV** : cliquez dessus pour exporter toutes les données dans un fichier au format CSV.

Vous pouvez également afficher les événements d'opérateur à l'aide de la nouvelle interface utilisateur d'Orchestrator.

- Dans le portail opérateur, cliquez sur l'option **Ouvrir la nouvelle interface utilisateur d'Orchestrator (Open New Orchestrator UI)** disponible en haut de la fenêtre.
- Cliquez sur **Lancer la nouvelle interface utilisateur d'Orchestrator (Launch New Orchestrator UI)** dans la fenêtre contextuelle. L'interface utilisateur s'ouvre dans un nouvel onglet affichant les options de surveillance.
- Cliquez sur **Événements d'opérateur (Operator Events)** pour afficher les événements.

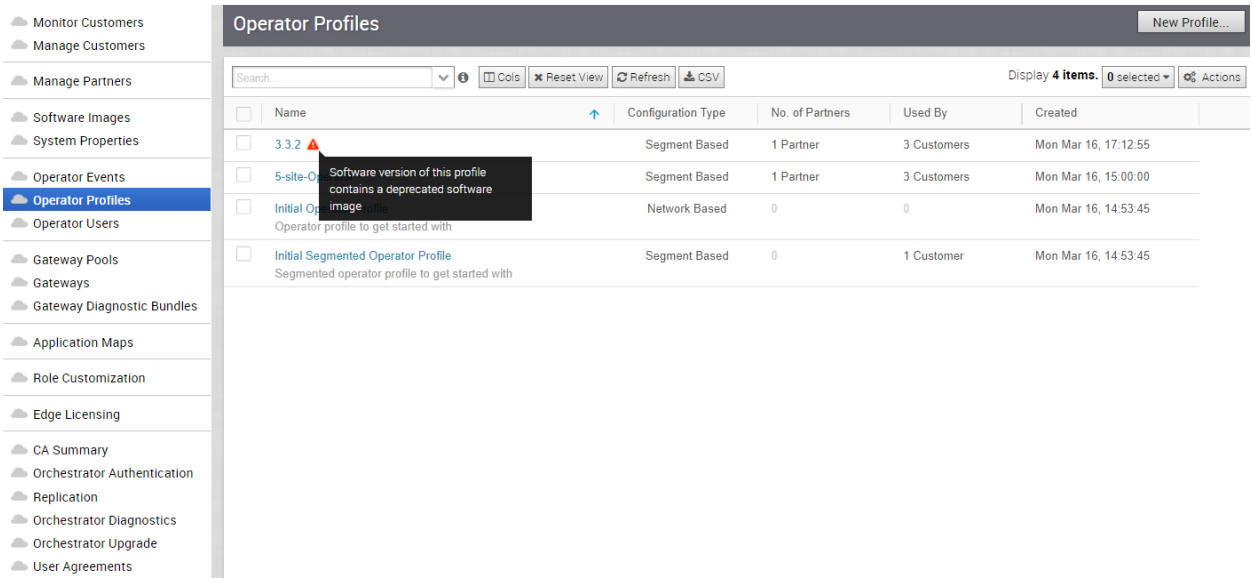


Dans le champ **Rechercher (Search)**, entrez un terme pour rechercher des détails spécifiques. Cliquez sur l'icône Filtre (Filter) pour filtrer la vue selon un critère spécifique.

Gérer les profils d'opérateur

Un profil d'opérateur permet de spécifier les paramètres réseau gérés par SD-WAN Orchestrator. Lorsque vous créez un client ou un partenaire, vous pouvez lui attribuer un profil d'opérateur.

Sur le portail opérateur, cliquez sur **Profils d'opérateurs (Operator Profiles)**. La page **Profils d'opérateurs (Operator Profiles)** affiche les profils disponibles.



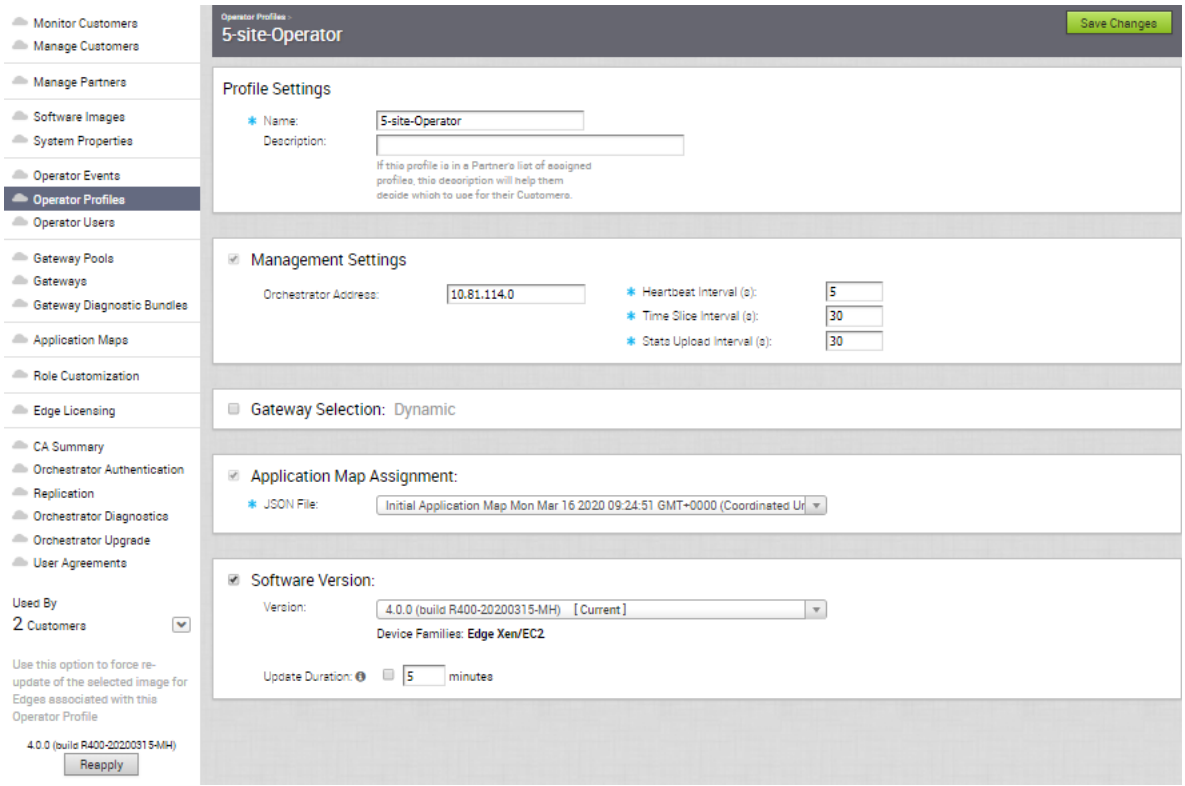
Note Les profils d'opérateurs qui contiennent une image obsolète sont signalés pour informer l'utilisateur que la version logicielle du profil contient une image logicielle obsolète.

En tant qu'utilisateur opérateur, vous pouvez créer un nouveau profil d'opérateur, dupliquer un profil existant, modifier ou supprimer un profil à l'aide du bouton **Actions** situé dans le coin supérieur droit de la page **Profils d'opérateurs (Operator Profiles)** comme suit :

- **Nouveau profil (New Profile)** : crée un profil d'opérateur. Reportez-vous à la section Créer un profil d'opérateur.
- **Dupliquer le profil (Duplicate Profile)** : crée une copie du profil d'opérateur sélectionné. Reportez-vous à la section Dupliquer un profil d'opérateur.
- **Modifier le profil (Modify Profile)** : permet de mettre à jour les paramètres réseau dans le profil d'opérateur sélectionné. Reportez-vous à la section Modifier un profil d'opérateur.
- **Retirer le profil (Remove Profile)** : retire le profil d'opérateur sélectionné de tous les partenaires et clients associés.
- **Effacer le profil (Delete Profile)** : supprime les profils sélectionnés.

  Note Vous ne pouvez pas supprimer un profil qui a déjà été attribué à un client ou à un partenaire.

Pour mettre à jour le profil d'opérateur dont l'image est obsolète avec une autre image logicielle, cliquez sur le lien d'accès au nom de ce profil d'opérateur. La page Profil d'opérateur (Operator Profile) sélectionnée s'affiche.



Sous **Version logicielle (Software Version)**, dans le menu déroulant **Version**, sélectionnez l'image logicielle et cliquez sur Enregistrer les modifications (Save Changes).

Note Le menu déroulant **Version** affiche les images logicielles qui sont obsolètes avec un indicateur, mais vous ne pourrez pas les sélectionner.

Pour le profil sélectionné, les informations d'utilisation, telles que le nombre de clients utilisant le profil et la version logicielle utilisée par le profil, s'affichent dans la partie inférieure gauche de la page.

Cliquez sur **Réappliquer (Reapply)** pour forcer la nouvelle mise à jour de l'image logicielle sélectionnée pour les dispositifs Edge associés au profil d'opérateur sélectionné.

Liens associés

- Pour attribuer un profil à un nouveau client, reportez-vous à la section Créer un client.
- Pour modifier le profil d'un client existant, reportez-vous à la section Configurer les clients.
- Pour attribuer un profil à un partenaire, reportez-vous à la section Chapitre 9 Gérer les partenaires.

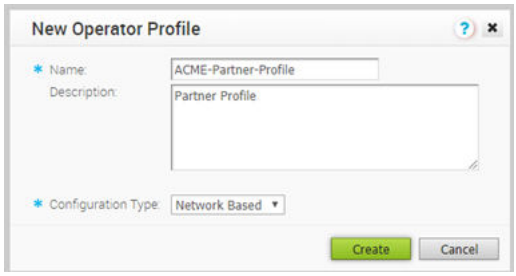
Créer un profil d'opérateur

Lorsque vous installez SD-WAN Orchestrator, un profil d'opérateur initial est disponible. Si nécessaire, vous pouvez créer des profils supplémentaires.

Sur le portail opérateur, cliquez sur **Profils d'opérateurs (Operator Profiles)**.

1 Cliquez sur **Nouveau profil (New Profile)** ou sur **Actions > Nouveau profil (New Profile)**.

2 Dans la fenêtre **Nouveau profil d'opérateur (New Operator Profile)**, entrez le nom et la description, puis choisissez le type de configuration.



3 Cliquez sur **Créer (Create)**.

Le nouveau profil s'affiche sur la page **Profils d'opérateurs (Operator Profiles)**.

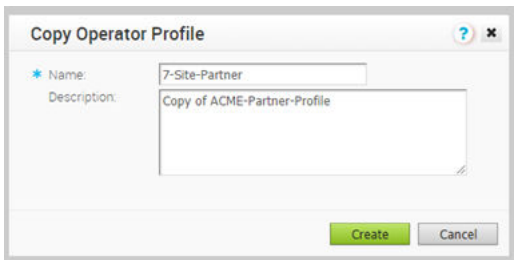
Dupliquer un profil d'opérateur

Vous pouvez dupliquer un profil d'opérateur pour en créer une copie.

Sur le portail opérateur, cliquez sur **Profils d'opérateurs (Operator Profiles)**.

1 Sélectionnez le profil à dupliquer et cliquez sur **Actions > Dupliquer le profil (Duplicate Profile)**.

2 Dans la fenêtre **Copier le profil d'opérateur (Copy Operator Profile)**, mettez à jour le nom et la description.



3 Cliquez sur **Créer (Create)**.

Une copie du profil s'affiche sur la page **Profils d'opérateurs (Operator Profiles)**.

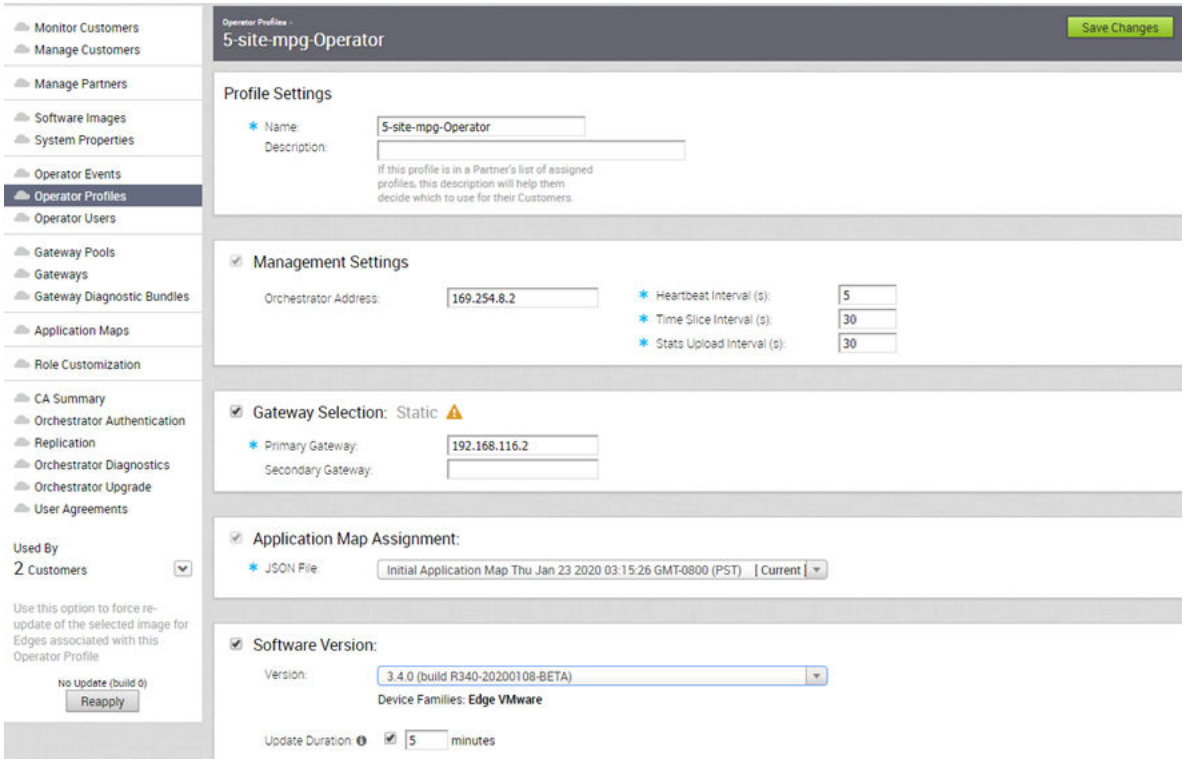
Modifier un profil d'opérateur

Vous pouvez modifier un profil d'opérateur pour mettre à jour les paramètres de profil.

Sur le portail opérateur, cliquez sur **Profils d'opérateurs (Operator Profiles)**.

Cliquez sur le lien vers un profil ou sélectionnez le profil et cliquez sur **Actions > Modifier le profil (Modify Profile)**.

Les paramètres existants du profil sélectionné s'affichent et vous pouvez configurer les éléments suivants :



Paramètres de profil (Profile Settings)

Si nécessaire, vous pouvez modifier le nom et la description du profil sélectionné.

Paramètres de gestion (Management Settings)

L'adresse IP de l'instance de SD-WAN Orchestrator s'affiche. Vous pouvez configurer les intervalles de gestion suivants :

- **Intervalle de pulsation (Heartbeat Interval)** : intervalle de temps entre les messages de pulsation envoyés depuis l'instance de SD-WAN Orchestrator aux dispositifs SD-WAN Edges. La valeur par défaut est de 30 secondes et l'intervalle minimal doit être de 10 secondes. Si un dispositif SD-WAN Edge ne reçoit pas deux pulsations en continu, le dispositif SD-WAN Edge est marqué comme étant Hors service (Down).

  Note Lorsque vous modifiez l'intervalle de pulsation, assurez-vous de mettre à jour le paramètre Délai de notification d'alerte hors ligne SD-WAN Edge (Edge Offline Alert Notification Delay) en conséquence, afin d'éviter d'envoyer des alertes inutiles.

- **Intervalle de tranche de temps (Timeslice Interval)** : intervalle de temps pendant lequel les données de surveillance sont collectées pour un flux.

- **Intervalle de chargement des statistiques (Stats Upload Interval)** : intervalle de temps pour le chargement des données de surveillance. Toutes les données de chaque tranche de temps sont collectées pendant l'intervalle de chargement des statistiques, puis chargées.

Sélection de SD-WAN Gateway

Par défaut, la sélection de SD-WAN Gateway est dynamique. Les passerelles VMware SD-WAN Gateways sont choisies dynamiquement à partir du pool de passerelles SD-WAN Gateway Pool. Assurez-vous que le pool de passerelles SD-WAN Gateway Pool comprend au moins deux passerelles VMware SD-WAN Gateways pour que la sélection de SD-WAN Gateway soit efficace. Pour plus d'informations sur les pools de passerelles SD-WAN Gateway Pools, reportez-vous à la section Chapitre 13 Gérer les pools de passerelles et les passerelles.

Cochez la case pour que la sélection de passerelle SD-WAN Gateway soit Statique. Pour la sélection de passerelle SD-WAN Gateway statique, vous devez spécifier la passerelle SD-WAN Gateway principale. Vous pouvez également entrer une passerelle SD-WAN Gateway secondaire facultative.

Note Utilisez la sélection de passerelle SD-WAN Gateway statique uniquement à des fins de test ou de débogage. N'utilisez pas cette option pour les configurations de transfert de VPN SD-WAN Edge à SD-WAN Edge ou de partenaires.

Attribution de mappage d'application (Application Map Assignment)

Par défaut, le mappage d'application initial est attribué au profil d'opérateur. Vous pouvez choisir un autre mappage d'application disponible dans la liste déroulante. Reportez-vous également à la section Chapitre 14 Mappages d'applications.

Version logicielle

Vous pouvez choisir de transférer la dernière image logicielle vers les dispositifs SD-WAN Edges. Par défaut, aucune mise à jour n'est appliquée aux terminaux. Cochez la case et choisissez l'image logicielle dans la liste déroulante **Version**. Pour plus d'informations sur les images logicielles, reportez-vous à la section Chapitre 10 Images logicielles.

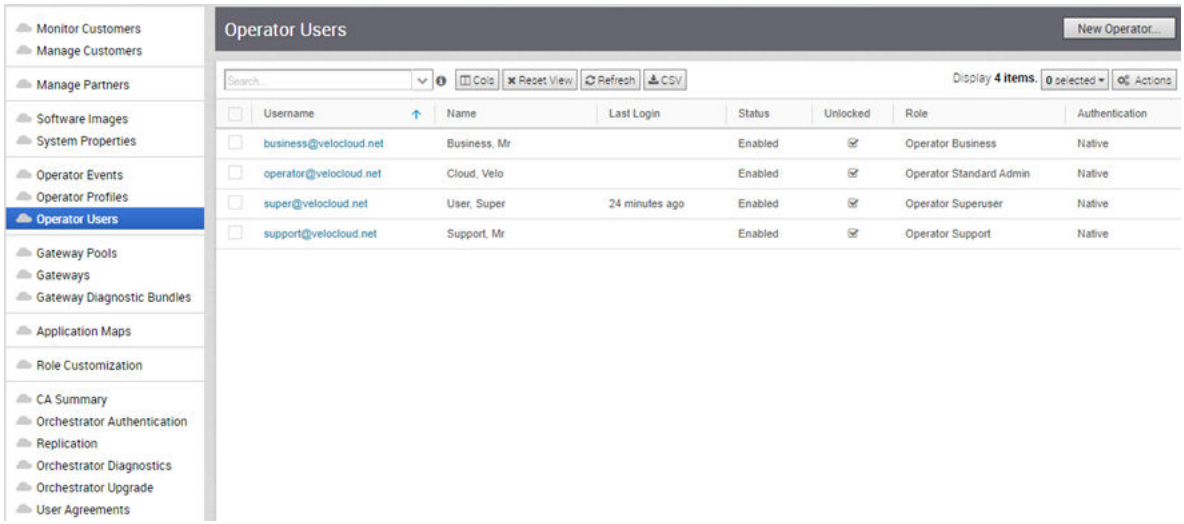
Cochez la case **Mettre à jour la durée (Update Duration)** et entrez la durée en minutes. Lorsque vous activez cette option, SD-WAN Orchestrator met à jour tous les terminaux associés au client d'entreprise dans la période spécifiée.

Après la mise à jour des paramètres ci-dessus, cliquez sur **Enregistrer les modifications (Save Changes)**.

Gérer les utilisateurs opérateurs

La page **Utilisateurs opérateurs (Operator Users)** affiche les utilisateurs opérateurs existants. Un super utilisateur opérateur peut créer des utilisateurs opérateurs dotés de privilèges de rôle différents et configurer des jetons d'API pour chacun d'entre eux.

Dans le portail de l'opérateur, cliquez sur **Utilisateurs opérateurs (Operator Users)** et configurez les éléments suivants.



Cliquez sur **Actions** pour effectuer les activités suivantes :

- **Nouvel opérateur (New Operator)** : crée des utilisateurs opérateurs. Reportez-vous à la section Créer un utilisateur opérateur.
- **Modifier l'opérateur (Modify Operator)** : modifie les propriétés de l'utilisateur opérateur sélectionné. Vous pouvez également cliquer sur le lien vers le nom d'utilisateur pour modifier les propriétés. Reportez-vous à la section Configurer les utilisateurs opérateurs.
- **Réinitialisation du mot de passe (Password Reset)** : envoie à l'utilisateur sélectionné un e-mail contenant un lien pour réinitialiser le mot de passe.
- **Supprimer l'opérateur (Delete Operator)** : supprime les utilisateurs sélectionnés.

Créer un utilisateur opérateur

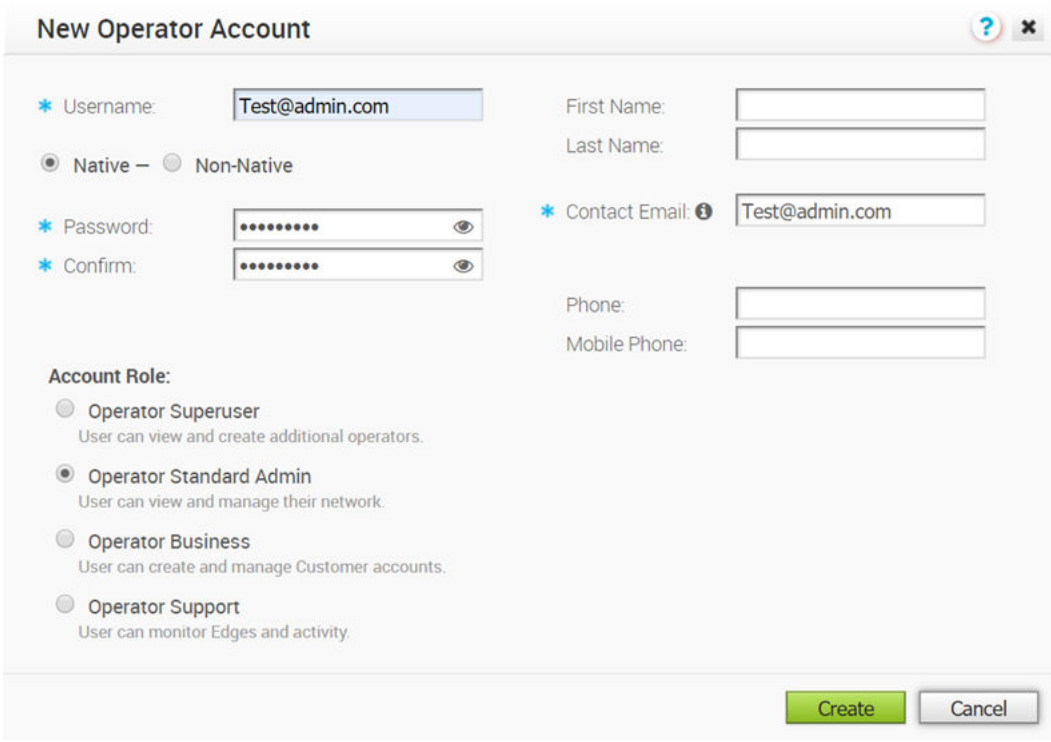
Les super utilisateurs opérateurs peuvent créer des utilisateurs opérateurs.

Sur le portail opérateur, cliquez sur **Utilisateurs opérateurs (Operator Users)**.

Procédure

1 Vous pouvez créer des utilisateurs opérateurs en cliquant sur **Nouvel opérateur (New Operator)** ou sur **Actions > Nouvel opérateur (New Operator)**.

2 Dans la fenêtre **Compte du nouvel opérateur (New Operator Account)**, entrez les informations suivantes :



a Entrez les informations de l'utilisateur, comme le nom d'utilisateur, le mot de passe, le nom, l'e-mail et les numéros de téléphone.

b Si vous avez choisi le mode d'authentification comme mode Natif (Native) dans la section Chapitre 17 Authentification d'Orchestrator, le type de l'utilisateur est sélectionné comme étant Natif (Native). Si vous avez choisi un autre mode d'authentification, vous pouvez choisir le type de l'utilisateur. Si vous décidez que l'utilisateur ne doit pas être natif, l'option Mot de passe (Password) n'est pas disponible, car il est hérité du mode d'authentification.

c **Rôle de compte (Account Role)** : choisissez le rôle d'utilisateur dans les options disponibles.

3 Cliquez sur **Créer (Create)**.

Résultats

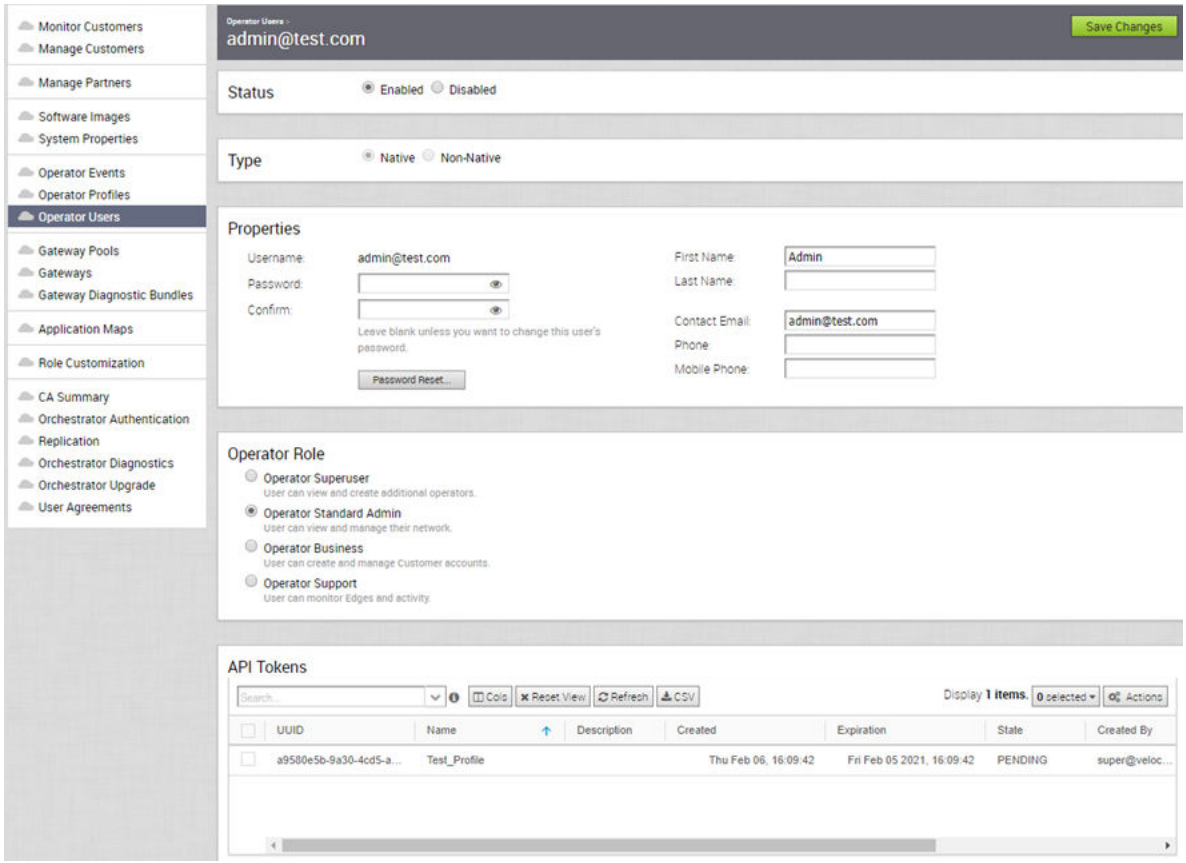
Les informations de l'utilisateur s'affichent sur la page **Utilisateurs opérateurs (Operator Users)**.

Configurer les utilisateurs opérateurs

Vous pouvez configurer des propriétés supplémentaires et créer des jetons d'API pour un utilisateur opérateur.

Sur le portail opérateur, cliquez sur **Utilisateurs opérateurs (Operator Users)**. Pour configurer un utilisateur opérateur, cliquez sur le lien vers un nom d'utilisateur ou sélectionnez l'utilisateur et cliquez sur **Actions > Modifier l'opérateur (Modify Operator)**.

Les propriétés existantes de l'utilisateur sélectionné s'affichent et, si nécessaire, vous pouvez ajouter ou modifier les éléments suivants :



État

Par défaut, l'état est **Activé (Enabled)**. Si vous choisissez **Désactivé (Disabled)**, l'utilisateur est déconnecté de toutes les sessions actives.

Type

Si vous avez choisi le mode d'authentification de l'opérateur **Natif (Native)** dans Chapitre 17 Authentification d'Orchestrator, le type d'utilisateur **Natif (Native)** est sélectionné. Si vous avez choisi un autre mode d'authentification, vous pouvez choisir le type de l'utilisateur. Si vous choisissez l'utilisateur **Non natif (Non-Native)**, vous ne pouvez pas réinitialiser le mot de passe ni modifier le rôle d'utilisateur.

Propriétés

Les informations de contact existantes de l'utilisateur s'affichent. Si nécessaire, vous pouvez modifier ces informations et choisir de réinitialiser le mot de passe. Si vous cliquez sur **Réinitialisation du mot de passe (Password Reset)**, un e-mail contenant un lien est envoyé à l'utilisateur pour réinitialiser le mot de passe.

Rôle

Le type existant du rôle d'utilisateur s'affiche. Si nécessaire, vous pouvez choisir un autre rôle pour l'utilisateur. Les privilèges du rôle sont modifiés en conséquence.

Jetons d'API

Les utilisateurs peuvent accéder aux API Orchestrator à l'aide de jetons au lieu d'une authentification basée sur une session. En tant que super utilisateur opérateur, vous pouvez gérer les jetons d'API pour les clients. Vous pouvez créer plusieurs jetons d'API pour un utilisateur.

Pour les utilisateurs en lecture seule d'entreprise et les utilisateurs experts commerciaux MSP, l'authentification par jeton n'est pas activée.

Par défaut, les jetons d'API sont activés. Pour les désactiver, accédez à **Propriétés système (System Properties)** sur le portail opérateur, puis définissez la valeur de la propriété système `session.options.enableApiTokenAuth` sur **Faux (False)**.

Configurer des jetons d'API :

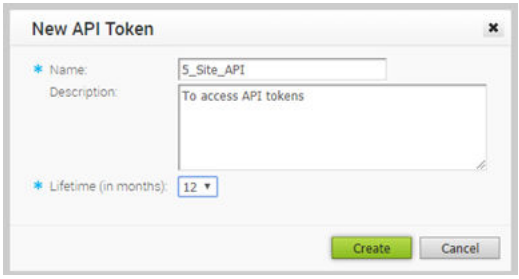
Tout utilisateur peut créer des jetons en fonction des privilèges auxquels ils ont été attribués à leurs rôles d'utilisateur, à l'exception des utilisateurs en lecture seule d'entreprise et les utilisateurs experts commerciaux MSP.

Les utilisateurs peuvent effectuer les actions suivantes, en fonction de leurs rôles :

- Les utilisateurs d'entreprise peuvent créer, télécharger et révoquer des jetons pour eux-mêmes.
- Les super utilisateurs opérateurs peuvent gérer des jetons d'autres utilisateurs opérateurs et des utilisateurs d'entreprise, si l'utilisateur d'entreprise a délégué des autorisations d'utilisateur à l'opérateur.
- Les super utilisateurs d'entreprise peuvent gérer les jetons de tous les utilisateurs de cette entreprise.
- Les utilisateurs ne peuvent télécharger que leurs propres jetons.
- Les super utilisateurs ne peuvent créer et révoquer que les jetons pour d'autres utilisateurs.

Pour gérer les jetons d'API :

- Dans la section **Jetons d'API (API Tokens)**, cliquez sur **Actions > Nouveau jeton d'API (New API Token)**, pour créer un jeton.
- Dans la fenêtre **Nouveau jeton d'API (New API Token)**, entrez un **Nom (Name)** et une **Description** pour le jeton, puis choisissez **Durée de vie (Lifetime)** dans le menu déroulant.



- Cliquez sur **Créer (Create)** et le nouveau jeton s'affiche dans la grille **Jetons d'API (API Tokens)**.
- Initialement, l'état du jeton affiché est **En attente (Pending)**. Pour télécharger le jeton, sélectionnez-le, puis cliquez sur **Actions > Télécharger le jeton d'API (Download API Token)**. L'état passe à **Activé (Enabled)**, ce qui signifie que le jeton d'API peut être utilisé pour l'accès à l'API.
- Pour désactiver un jeton, sélectionnez-le, puis cliquez sur **Actions > Révoquer le jeton d'API (Revoke API Token)**. L'état du jeton affiché est **Révoqué (Revoked)**.
- Lorsque la durée de vie du jeton est écoulée, l'état passe à **Expiré (Expired)**.

Seul l'utilisateur associé à un jeton peut le télécharger et ensuite, seul l'ID du jeton s'affiche. Vous ne pouvez télécharger un jeton qu'une seule fois.

Après le téléchargement du jeton, l'utilisateur peut l'envoyer comme partie intégrante de l'en-tête d'autorisation de la demande pour accéder à l'API Orchestrator.

L'exemple suivant montre un exemple d'extrait de code permettant d'accéder à une API.

```
curl -k -H "Authorization: Token <Token>"
  -X POST https://vco/portal/
  -d '{ "id": 1, "jsonrpc": "2.0", "method": "enterprise/getEnterpriseUsers", "params":
{ "enterpriseId": 1 }}'
```

Après avoir modifié les paramètres et les jetons d'API, cliquez sur **Enregistrer les modifications (Save Changes)**.

Gérer les pools de passerelles et les passerelles

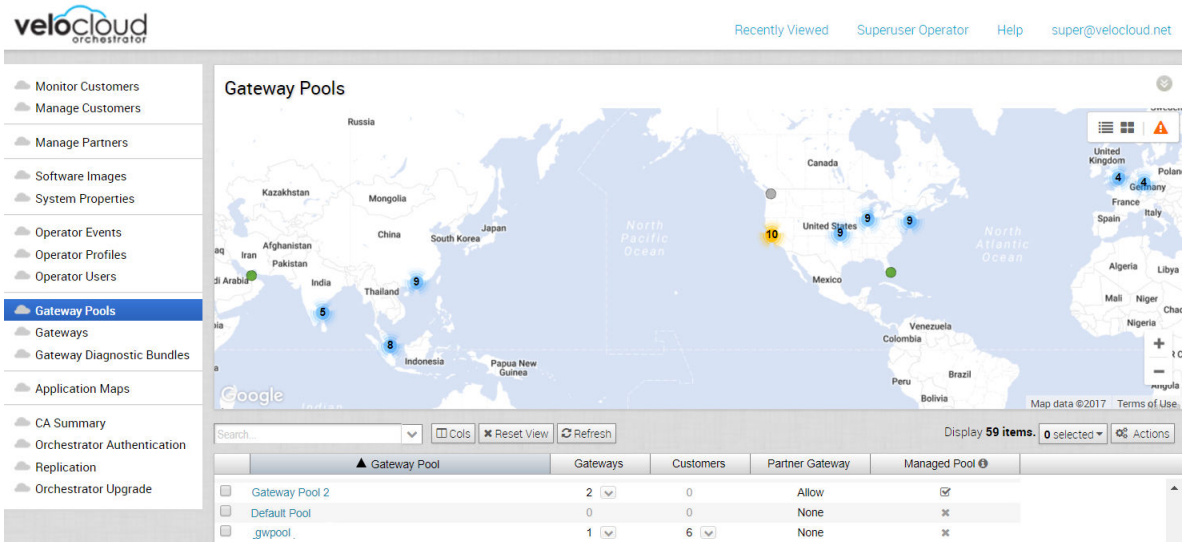
13

Un réseau VMware se compose de plusieurs passerelles de service déployées sur un réseau de niveau supérieur et de centres de données cloud. Les instances de SD-WAN Gateway apportent les avantages des services distribués sur le cloud et des chemins optimisés pour toutes les applications, succursales et centres de données. Les fournisseurs de services peuvent également déployer leurs propres passerelles partenaires dans leur infrastructure de cloud privé.

Ce chapitre contient les rubriques suivantes :

Pools de passerelles

Vous pouvez organiser les passerelles en pools qui sont ensuite attribués à un réseau. Il existe un pool par défaut non renseigné après l'installation d'une entité de SD-WAN Orchestrator. Vous pouvez créer des pools de passerelles supplémentaires.



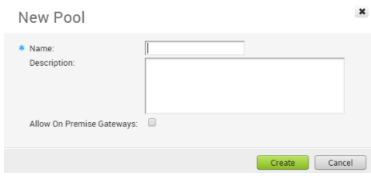
Colonne Pool géré

Les cases à cocher de la colonne **Pool géré (Managed Pool)** qui sont associées à des pools de passerelles représentent les pools de passerelles que les partenaires peuvent modifier et gérer. Si un pool de passerelles est associé à un « x », les partenaires disposent uniquement d'un accès en lecture à ce pool.

Note Si un opérateur coche la case **Autoriser l'accès à la gestion des passerelles (Grant Gateway Management Access)**, les pools de passerelles attribués à un partenaire s'affichent dans la colonne **Pool géré (Managed Pool)** avec une coche en regard.

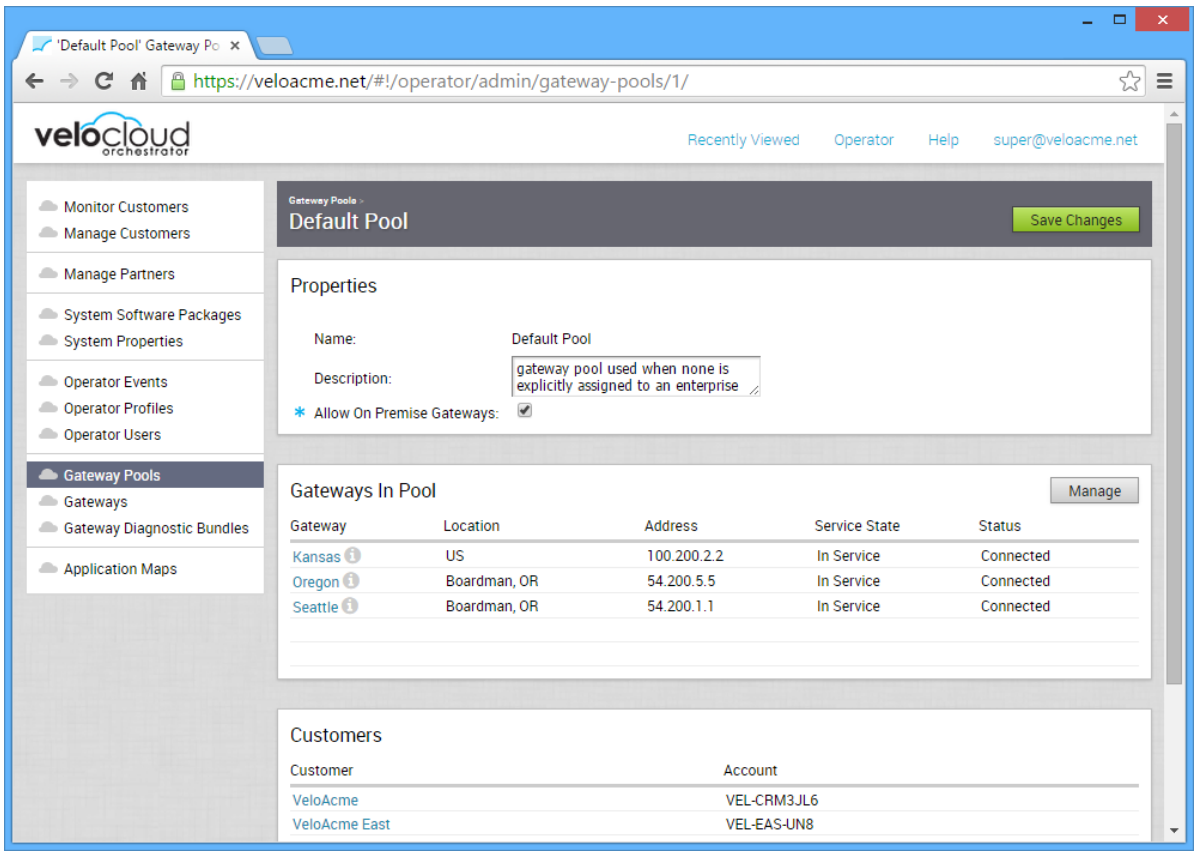
Créer un pool de passerelles

Si vous cliquez sur **Nouveau pool (New Pool)**, la boîte de dialogue suivante vous invite à entrer un nom pour un nouveau pool de passerelles. Vous pouvez également indiquer si les passerelles de partenaires seront autorisées dans le nouveau pool.



Si vous cliquez sur un pool de passerelles, les propriétés du pool, les passerelles à l'intérieur du pool et les clients qui utilisent le pool s'affichent. Notez que l'une des propriétés indique si le pool autorise ou non l'inclusion des passerelles sur site dans le pool.

Note Une instance de VMware SD-WAN Gateway peut fonctionner en tant que passerelle standard qui fournit des services réseau de VMware ou en tant que passerelle de partenaires qui permet l'acheminement du trafic réseau vers le réseau d'un fournisseur de services. Vous ne pouvez pas utiliser une passerelle pour les deux fonctions. Un pool de passerelles peut contenir des passerelles configurées en tant que passerelles de partenaires ou passerelles standard. Toutefois, si une passerelle de partenaires est placée dans un pool de passerelles dans lequel l'option **Autoriser les passerelles de partenaires (Allow Partner Gateways)** n'est pas sélectionnée, la passerelle fonctionne comme une passerelle standard.



Création de pools de passerelles spécifiques à un partenaire

Cette section décrit comment créer des passerelles et des pools de passerelles pour un partenaire. Les passerelles et les pools de passerelle que vous créez ne seront utilisés que par le partenaire.

Pour créer une passerelle ou un pool de passerelles sur le portail partenaire de SD-WAN Orchestrator :

1 Dans le panneau de navigation de SD-WAN Orchestrator, cliquez sur le lien **Gérer les partenaires (Manage Partners)**. La fenêtre **Gérer les partenaires (Manage Partners)** s'affiche.

2 Dans la fenêtre **Gérer les partenaires (Manage Partners)**, cliquez sur l'un des partenaires disponibles affichés dans la colonne **Partenaire (Partner)**. La fenêtre **Gérer les clients partenaires (Manage Partner Customers)** s'affiche.

3 Dans le panneau de navigation, cliquez sur le lien **Pool de passerelles (Gateway Pool)** pour créer un pool de passerelles ou cliquez sur le lien **Passerelle (Gateway)** pour créer une passerelle.

4 Dans le bouton **Actions** (situé au-dessus de la grille de la table dans le coin supérieur droit), cliquez sur **Nouveau pool de passerelles (New Gateway Pool)** (ou **Nouvelle passerelle [New Gateway]** Si vous avez sélectionné le lien **Passerelle [Gateway]**).

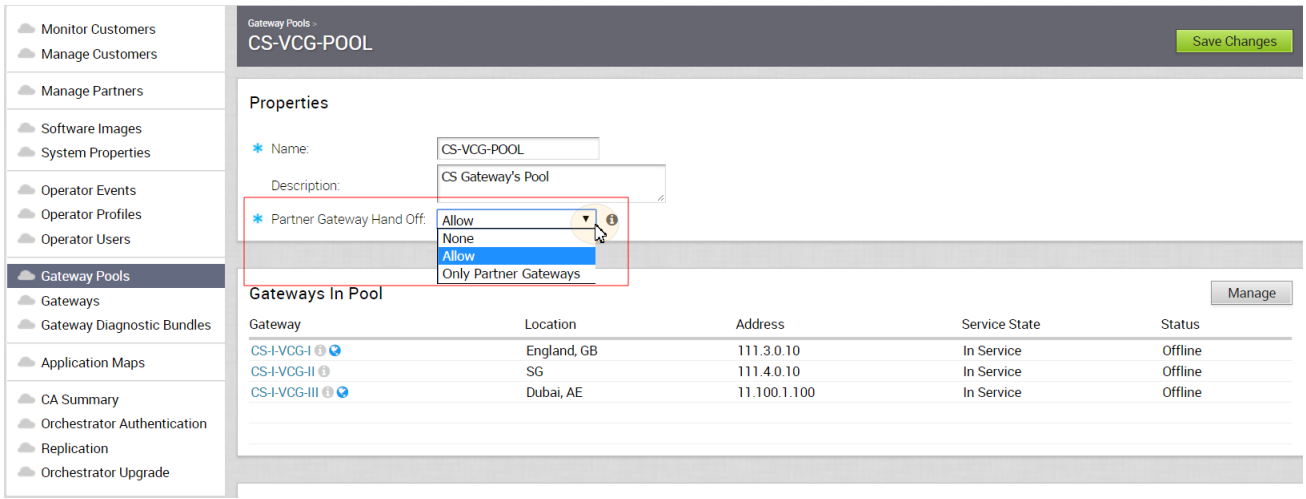
Note Dans les étapes ci-dessus, vous créez des passerelles spécifiques aux partenaires. Par conséquent, les passerelles ou les pools de passerelles que vous créez ne seront associés qu'à ce partenaire.

Supprimer un pool de passerelles

Pour supprimer des passerelles et des pools de passerelle appartenant à un partenaire, les opérateurs doivent supprimer les passerelles du portail partenaire. En outre, si la passerelle est utilisée par un partenaire, l'opérateur ne peut pas la supprimer. L'opérateur doit attendre que la passerelle soit disponible avant de pouvoir la supprimer.

Transfert de la passerelle de partenaires

Cette section décrit le menu déroulant **Transfert de passerelle de partenaires (Partner Gateway Hand Off)**



La zone **Propriétés (Properties)** des pools de passerelles affiche la zone de texte **Nom (Name)**, la zone de texte **Description** et un menu déroulant **Transfert de passerelle de partenaires (Partner Gateway Hand Off)**.

Le menu déroulant **Transfert de passerelle de partenaires (Partner Gateway Hand Off)** se compose des trois options suivantes :

Option	Description
Aucun (None)	À utiliser lorsque les entreprises attribuées à ce pool de passerelles ne requièrent pas de transferts de passerelle de partenaires.
Autoriser (Allow)	À utiliser lorsque le pool doit prendre en charge la combinaison de la passerelle de partenaires et de passerelles cloud.
Passerelles de partenaires uniquement (Only Partner Gateways)	À utiliser lorsque des dispositifs Edge dans les entreprises ne doivent pas se voir attribués des passerelles cloud à partir du pool et doivent se voir attribués uniquement les passerelles 1 et 2 qui sont définies pour le dispositif Edge individuel.

Si vous cliquez sur une passerelle spécifique, des détails supplémentaires s'affichent pour cette passerelle. Les détails sont notamment les propriétés, les informations de contact et d'emplacement, les clients qui utilisent la passerelle et tous les pools dont la passerelle est membre.

Passerelles de partenaires

Une passerelle peut être configurée en tant que passerelle de partenaires et peut fonctionner comme telle si elle fait partie d'un pool de passerelles qui autorise les passerelles de partenaires.

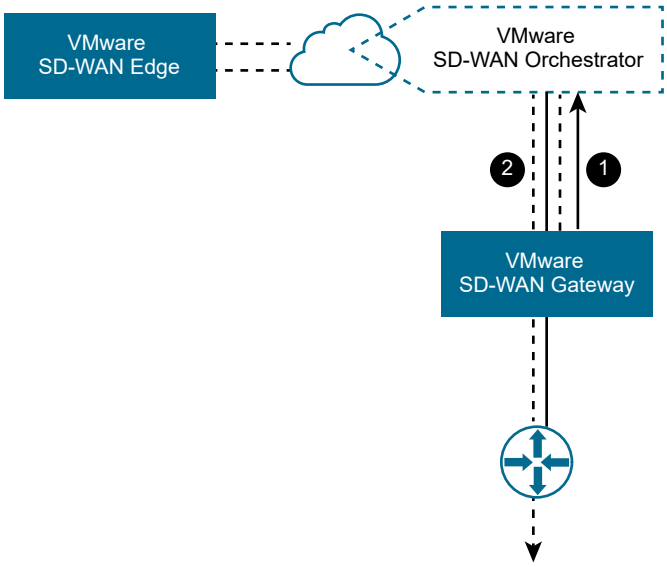
Passerelles de partenaires

Les passerelles SD-WAN Gateway de partenaires peuvent être configurées avec plusieurs sous-réseaux, chacun d'eux pouvant être défini avec un transfert de NAT ou de VLAN. Chaque sous-réseau peut également être configuré avec un coût relatif et pour le chiffrement du trafic.

Les exemples ci-dessous illustrent deux cas d'utilisation de la configuration des passerelles SD-WAN Gateways de partenaires.

Configuration de passerelle - Cas d'utilisation n°1

Dans l'illustration suivante, une passerelle SD-WAN Gateway est connectée en mode VLAN/VRF à un VRF qui ne dispose d'aucun accès à l'Internet public. Toutefois, la passerelle SD-WAN Gateway de partenaires doit être en mesure de contacter SD-WAN Orchestrator dans le cloud public et il doit exister un chemin d'accès pour atteindre le cloud. L'instance de SD-WAN Gateway peut acheminer un trafic spécifique vers la NAT de manière sélective (par exemple, l'adresse IP d'une instance de SD-WAN Orchestrator ou les sous-réseaux utilisés pour atteindre des serveurs DNS publics), même si elle fonctionne en mode VLAN/VRF.

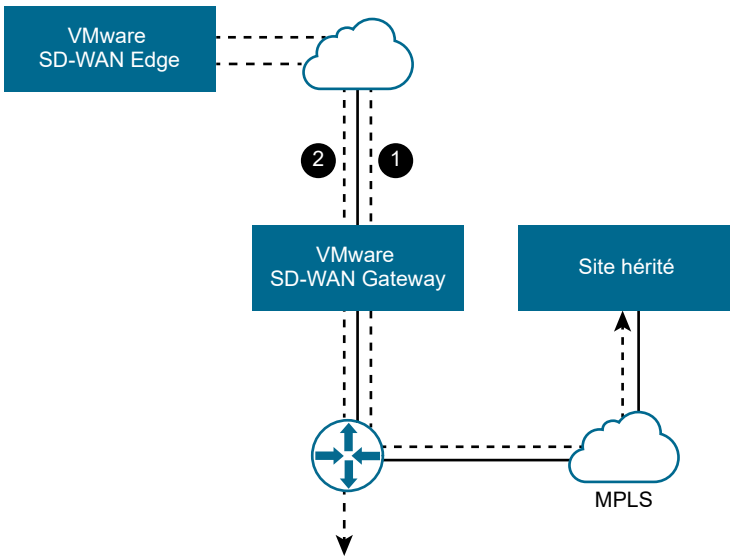


- Cas n°1 : le trafic de SD-WAN Orchestrator est acheminé via une ou plusieurs adresses IP vers la NAT.
- Cas n°2 : le trafic d'entreprise est acheminé via des sous-réseaux vers le VLAN/VRF.

Configuration de passerelle SD-WAN Gateway - Cas d'utilisation n°2

Il est courant qu'une passerelle SD-WAN Gateway de partenaires soit associée à un réseau d'entreprise afin de fournir la connectivité aux sites hérités. Cette nécessité peut survenir même si les sites d'entreprise n'ont pas tous été convertis en réseau VMware. Pour ce cas d'utilisation, il est nécessaire d'indiquer le trafic par sous-réseau sur la passerelle SD-WAN Gateway partenaire. Chaque sous-réseau peut également être configuré pour chiffrer le trafic réseau.

L'illustration suivante montre un exemple dans lequel seul le trafic vers des sites hérités est chiffré. Si l'instance de SD-WAN Gateway est déjà configurée avec un sous-réseau 0.0.0.0/0 pour autoriser l'intégralité du trafic (ce qui est une configuration courante), il suffit d'ajouter le sous-réseau privé pour vos sites hérités et de le marquer comme étant chiffré.

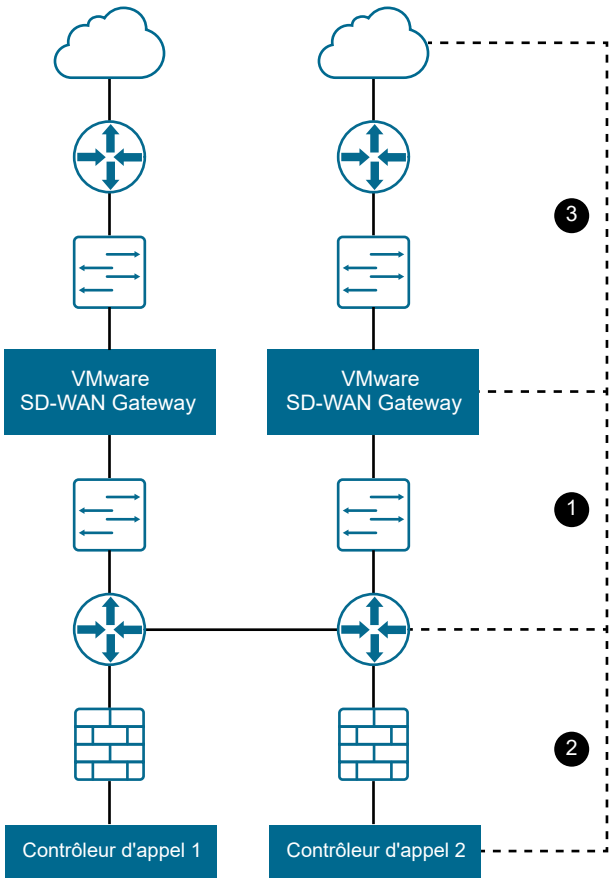


- Cas n°1 : le sous-réseau (par exemple, 10.0.0.0/8) est défini pour les sites hérités et marqué pour le chiffrement. Le trafic est transmis entre SD-WAN Edge et SD-WAN Gateway sur le tunnel IPsec.
- Cas n°2 : le trafic restant est envoyé non chiffré à SD-WAN Edge, puis à sa destination finale.

Résilience de la passerelle de partenaires

La passerelle SD-WAN Gateway de partenaires assure la résilience en détectant les pannes et en basculant vers une autre passerelle SD-WAN Gateway de partenaires. Cela inclut la capacité d'une passerelle SD-WAN Gateway de partenaires à détecter les conditions de panne et, pour l'infrastructure environnante, à détecter les pannes de la passerelle SD-WAN Gateway elle-même.

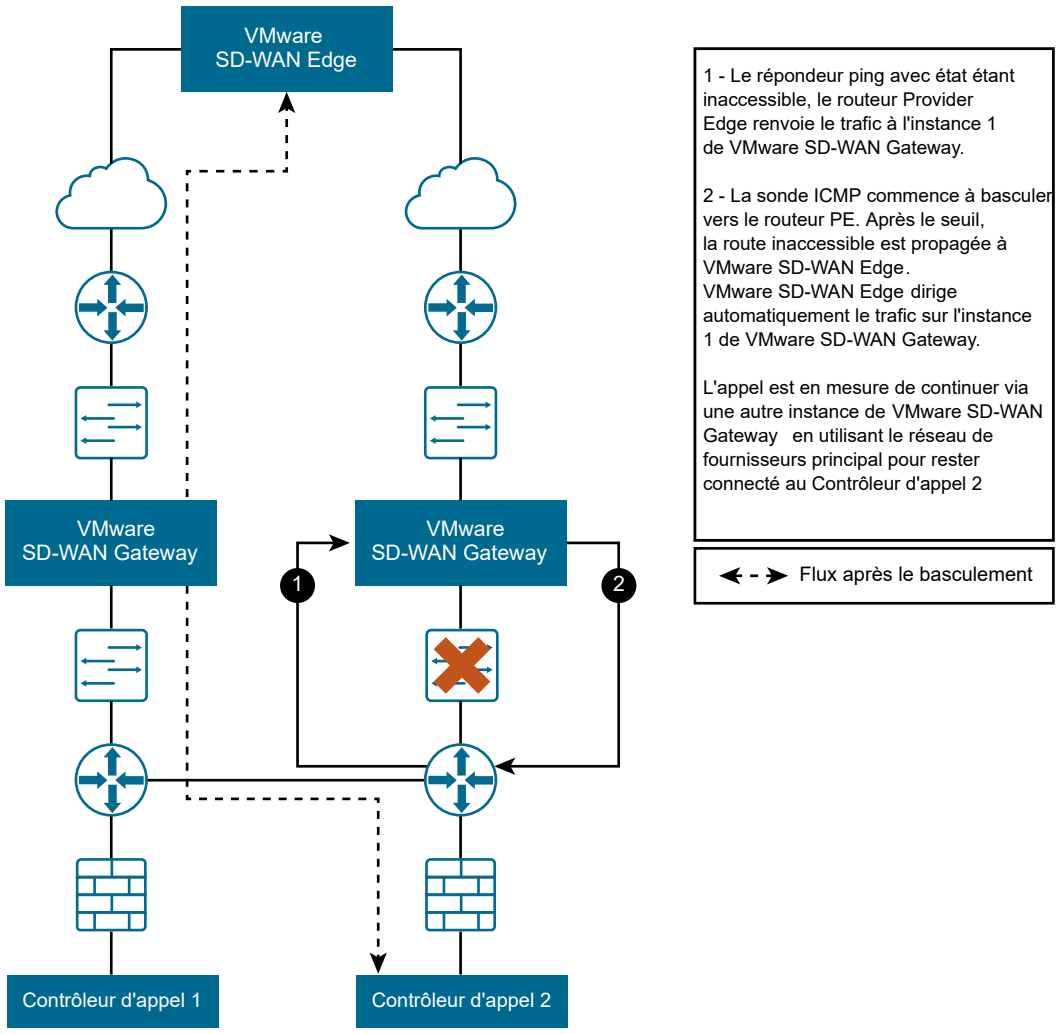
Examinez la topologie de passerelle SD-WAN Gateway suivante :



Cette figure illustre trois zones de panne distinctes :

Zone de panne	Composant	Description
1	Provider Edge	Provider Edge (PE) est une instance dans laquelle une panne peut être détectée soit par le routeur Provider Edge envoyant un ping à l'instance de SD-WAN Gateway, soit par l'instance de SD-WAN Gateway envoyant un ping au routeur Provider Edge.
2	Contrôleur d'appel (Call Controller)	L'instance de SD-WAN Gateway doit être en mesure d'envoyer un ping au routeur Provider Edge ou au contrôleur d'appel pour vérifier la connectivité.
3	Réseau WAN	L'instance de SD-WAN Gateway doit disposer d'un répondeur ping avec état qui répond uniquement si la zone WAN est disponible.

La figure suivante présente un scénario de panne typique qui se produit entre l'instance de SD-WAN Gateway et le routeur Provider Edge et décrit l'activité qui en découle.



La passerelle SD-WAN Gateway de partenaires prend également en charge les coûts de route configurables pour permettre des scénarios de panne plus flexibles. Enfin, un type de transfert supplémentaire est requis lorsque les balises NAT ou VLAN ne sont pas appliquées aux paquets et qu'elles sont simplement transmises au routeur Provider Edge.

Sondes de basculement ICMP

Cette section décrit les sondes de basculement ICMP.

Pour résoudre une panne dans les zones #1 ou #2 du diagramme de topologie SD-WAN Gateway, SD-WAN Gateway prend en charge la capacité facultative d'envoi de sondes de basculement. Ces sondes effectuent un ping sur une adresse IP de destination unique à la fréquence spécifiée. Si le seuil des réponses manquées successives au ping est dépassé, la passerelle marque les routes de SD-WAN Gateway comme étant inaccessibles. Bien que les routes soient marquées comme étant inaccessibles en raison de l'état d'échec de cette sonde, l'envoi de sondes se poursuit. Si le même seuil est dépassé pour les réponses réussies successives au ping, SD-WAN Gateway marque les routes comme étant de nouveau accessibles.

Exemple de scénario

Par exemple, prenez le cas où un utilisateur a configuré une fréquence de deux secondes et un seuil de trois.

1 Les dispositifs VMware SD-WAN Edges se connectent à l'instance principale de SD-WAN Gateway. L'instance principale de SD-WAN Gateway marque les routes comme étant accessibles.

2 L'instance principale de SD-WAN Gateway ne peut recevoir aucune réponse pour trois sondes successives (environ 6 secondes).

3 L'instance principale de SD-WAN Gateway marque les routes comme étant inaccessibles et communique cela à tous les dispositifs Edge connectés.

4 Les dispositifs Edge commencent à acheminer le trafic SD-WAN Gateway via l'instance secondaire de SD-WAN Gateway.

5 La connectivité est restaurée et l'instance principale de SD-WAN Gateway reçoit trois réponses successives des sondes.

6 L'instance principale de SD-WAN Gateway marque les routes comme étant accessibles et communique cela à tous les dispositifs Edge connectés.

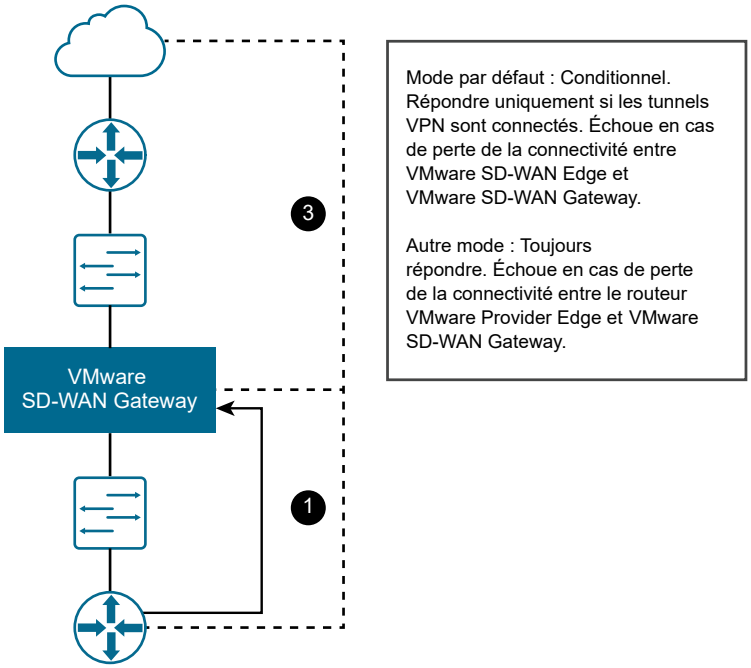
7 Les dispositifs Edge réacheminent le trafic via l'instance principale de SD-WAN Gateway.

Cela peut être utilisé dans le scénario de panne #1 pour effectuer un ping sur une adresse IP du routeur Provider Edge. Cela peut être utilisé dans le scénario de panne #2 pour effectuer un ping sur le contrôleur d'appels réel.

Répondeur ping avec état

Pour résoudre une panne dans la zone #2 ou #3 du diagramme de topologie de la passerelle de partenaires, SD-WAN Gateway prend en charge un répondeur ping avec état facultatif. Cela permet la configuration d'une adresse IP virtuelle (qui doit être différente de l'adresse IP de l'interface) dans SD-WAN Gateway qui, en fonction de la configuration, répond toujours aux commandes ping (le service de passerelle est en cours d'exécution) ou sur la base conditionnelle de la connectivité WAN (des tunnels VPN sont connectés à la passerelle).

Cela peut être utilisé dans le scénario de panne #1 en faisant en sorte que le routeur Provider Edge effectue un ping sur le répondeur ping, car l'inaccessibilité de SD-WAN Gateway risque d'entraîner l'échec d'IP SLA sur le routeur Provider Edge. Cela peut également être utilisé dans le scénario de panne #3 en faisant en sorte que SD-WAN Gateway ne réponde que si des tunnels VPN sont connectés. Ce comportement est semblable à celui de BGP (aucun client connecté indique aucune route client).



La passerelle de partenaires répond à la demande ICMP du routeur Provider Edge (PE) en fonction de la valeur IP SLA configurée dans le routeur PE. Le routeur PE du répondeur ping avec état doit être configuré, comme indiqué ci-dessous avec des informations de la balise VLAN appropriées.

```
!IP-SLA configuration to send ICMP request to gateway virtual IP
ip sla 1
icmp-echo 192.168.10.10 source-ip 192.168.10.1
vrf CUSTOMER1
threshold 1000
timeout 1000
frequency 2
ip sla schedule 1 life forever start-time now

!tracking the IP SLA for its reachability
track 1 ip sla 1 reachability

!all the routes will reachable only when SLA probe succeeds
ip route vrf CUSTOMER1 0.0.0.0 0.0.0.0 192.168.11.101 track 1
ip route vrf CUSTOMER2 0.0.0.0 0.0.0.0 192.168.12.101 track 1
ip route vrf CUSTOMER1 10.0.0.0 255.0.0.0 192.168.10.10 track 1
ip route vrf CUSTOMER2 10.0.0.0 255.0.0.0 192.168.10.10 track 1
ip route vrf CUSTOMER1 192.168.100.0 255.255.255.0 192.168.10.10 track 1
```

Mises en garde lors de l'utilisation du mode de transfert NAT

Lors de l'utilisation du mode de transfert NAT, prenez en compte les mises en garde suivantes :

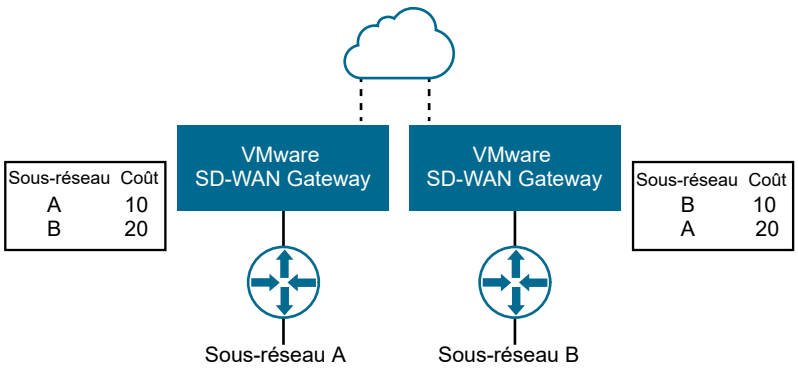
- Pour le mode de transfert VLAN, la passerelle de partenaires peut écouter sur n'importe quelle adresse IP si elle est accessible au routeur PE (y compris son adresse IP d'interface). Pour le mode de transfert NAT, la passerelle de partenaires ne répond pas si la demande ICMP est envoyée à sa propre adresse IP d'interface (WAN).
- Le flux inverse n'est pas pris en charge dans le mode de transfert NAT.

Sous-réseaux actifs/de secours

Cette section décrit comment configurer des sous-réseaux actifs et de secours pour une passerelle de partenaires.

Sous-réseaux sur une passerelle de partenaires

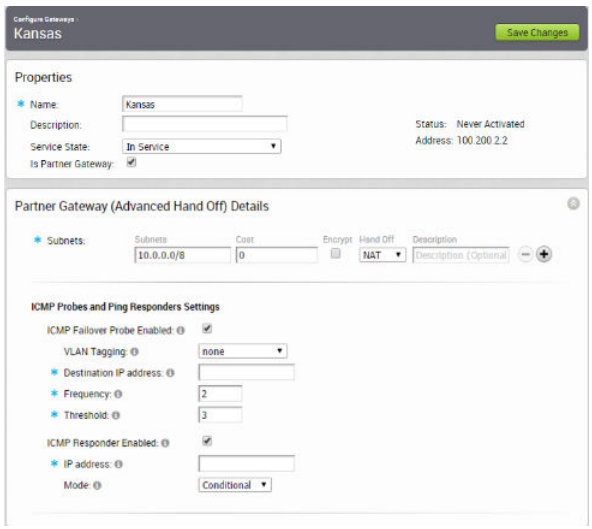
Les sous-réseaux configurés sur une passerelle de partenaires sont entrés sous forme de sous-réseaux et de descriptions facultatives. Un champ `Cost` est inclus pour permettre la pondération entre les routes. Les routes peu coûteuses sont préférées à celles qui sont très coûteuses. La figure suivante illustre les paramètres `Cost` par sous-réseau.



Configuration et utilisation de la passerelle de partenaires

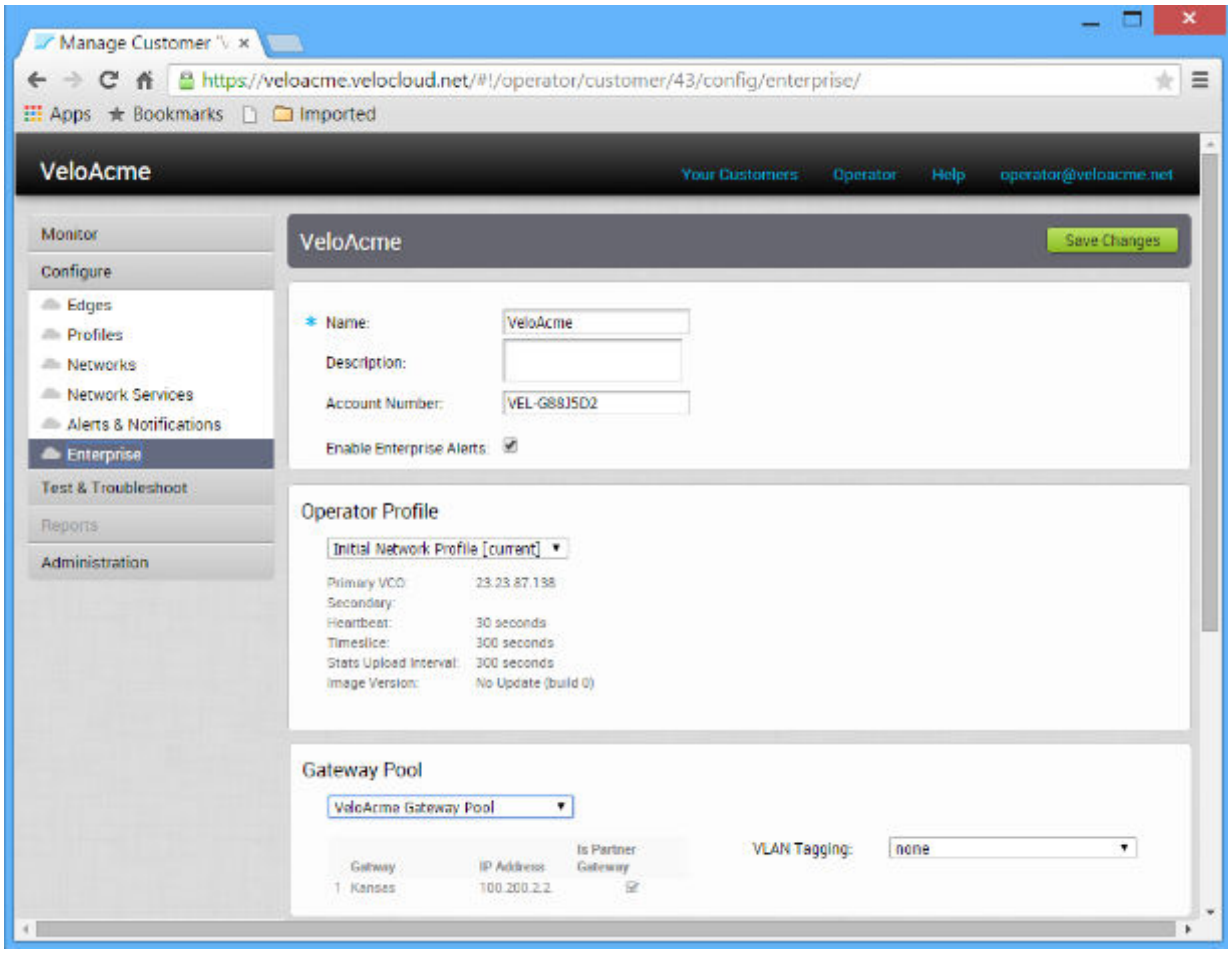
Si l'option **Est la passerelle de partenaires (Is Partner Gateway)** est sélectionnée pour une passerelle, une configuration supplémentaire est requise :

1 Sélectionnez la passerelle qui sera une passerelle de partenaires, puis cochez la case **Est la passerelle de partenaires (Is Partner Gateway)**. Une section **Informations sur la passerelle de partenaires (transfert avancé) [Partner Gateway (Advanced Hand Off) Details]** s'affiche pour la passerelle.



Cette section permet de configurer un ou plusieurs sous-réseaux qui acheminent le trafic vers la passerelle de partenaires. Pour chaque sous-réseau, vous pouvez sélectionner un type de **transfert (Hand Off)** (VLAN ou NAT) et indiquer si le trafic doit être chiffré ou non. Vous pouvez également entrer les paramètres Sondes ICMP (ICMP Probes) et Répondeurs ping (Ping Responders), et les informations de contact et d'emplacement de la passerelle.

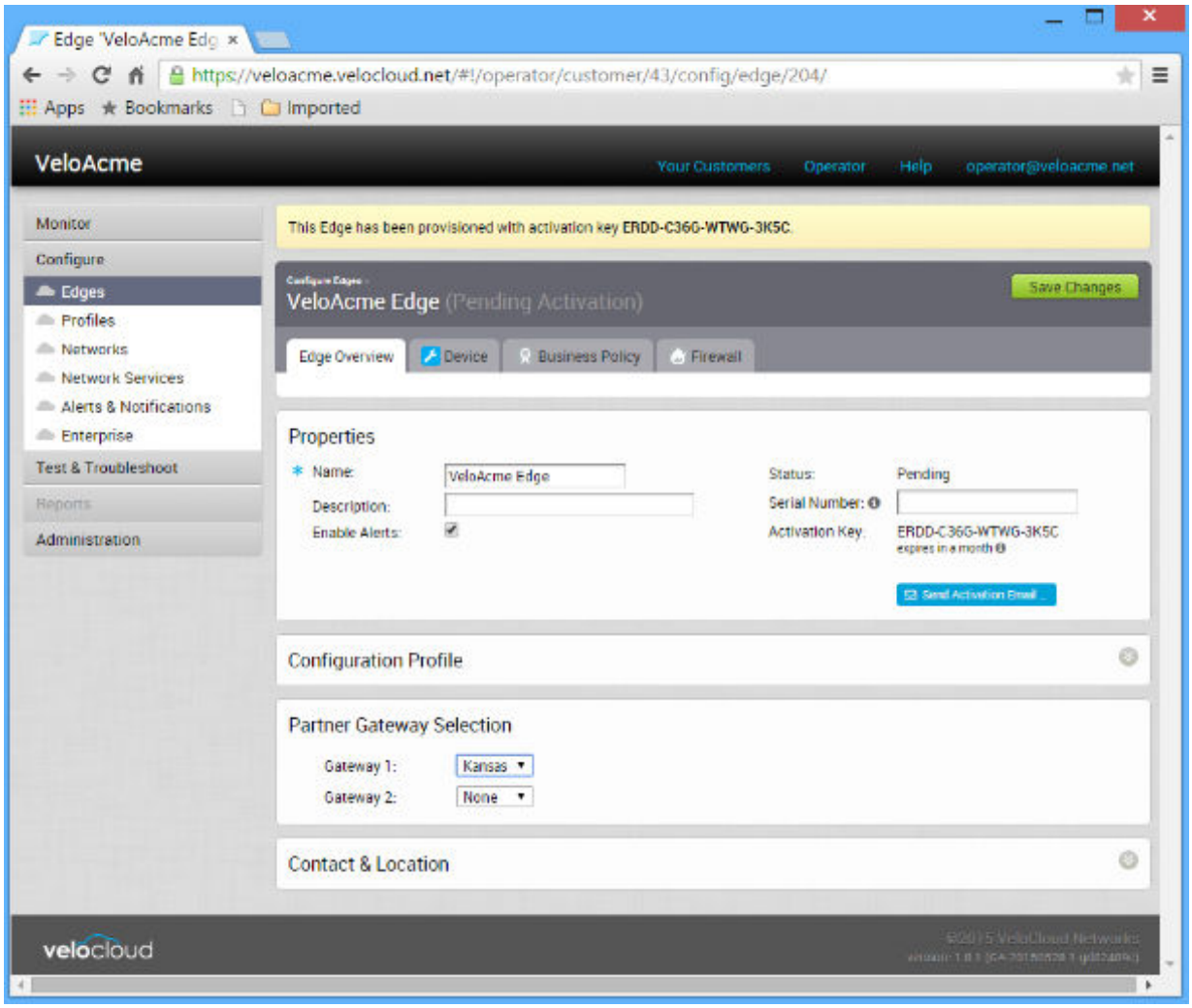
2 Pour chaque client qui utilise des passerelles de partenaires, sélectionnez un pool de passerelles qui contient la passerelle de partenaires en sélectionnant un client, puis en choisissant **Configurer (Configure) -> Entreprise (Enterprise)**.



Vous pouvez également choisir le balisage VLAN pour le pool.

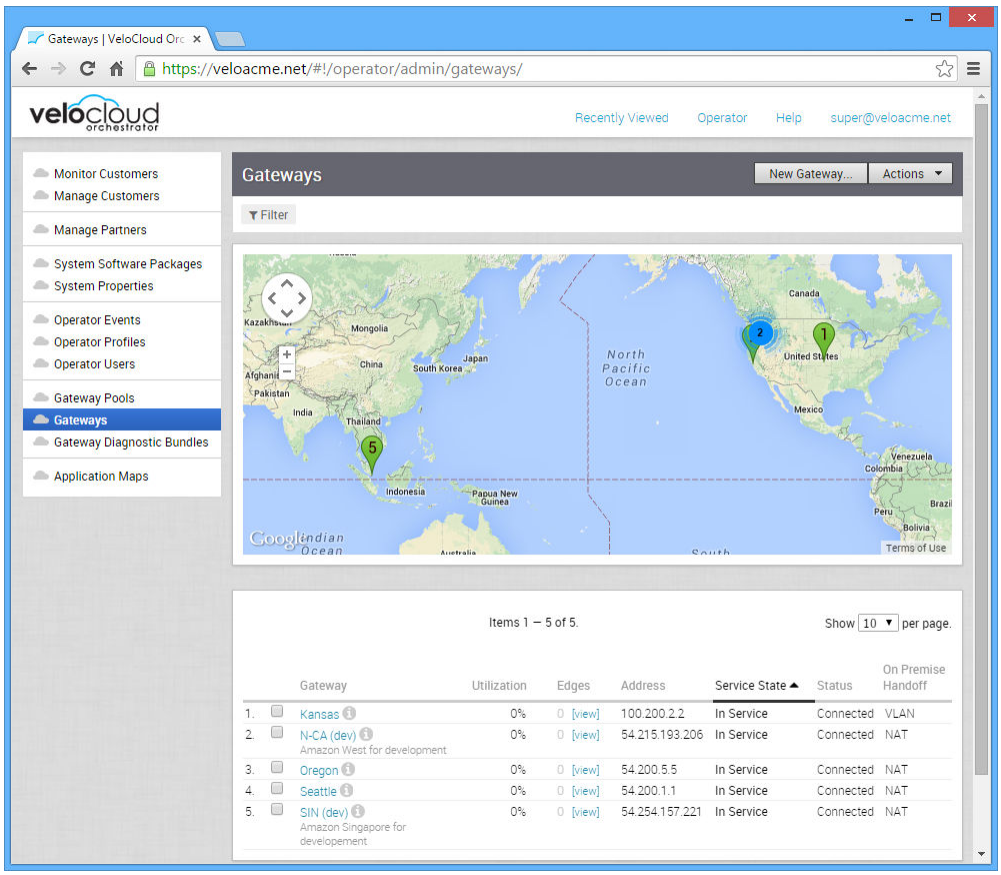
3 Pour que le VRF de la passerelle de partenaires reconnaisse et active BGP, accédez à **Configurer (Configure) > Client (Customer)** dans l'écran **Pool de passerelles (Gateway Pool)**. Pour plus d'informations sur la configuration, reportez-vous à la section Configurer le protocole BGP de passerelle.

4 Pour chaque dispositif Edge client qui utilise une passerelle de partenaires, configurez la sélection de passerelles de partenaires pour choisir les **Passerelles (Gateways)**. Choisissez d'abord un client, sélectionnez **Configurer (Configure) -> Dispositifs Edge (Edges) ->**, puis **Edge**.



Page Passerelles

Si vous cliquez sur le lien **Passerelles (Gateways)**, toutes les passerelles gérées par SD-WAN Orchestrator s'affichent sous la forme d'une liste contenant des informations sur les passerelles et en tant qu'emplacement sur une carte. Cliquez sur une passerelle pour afficher les informations sur la passerelle.

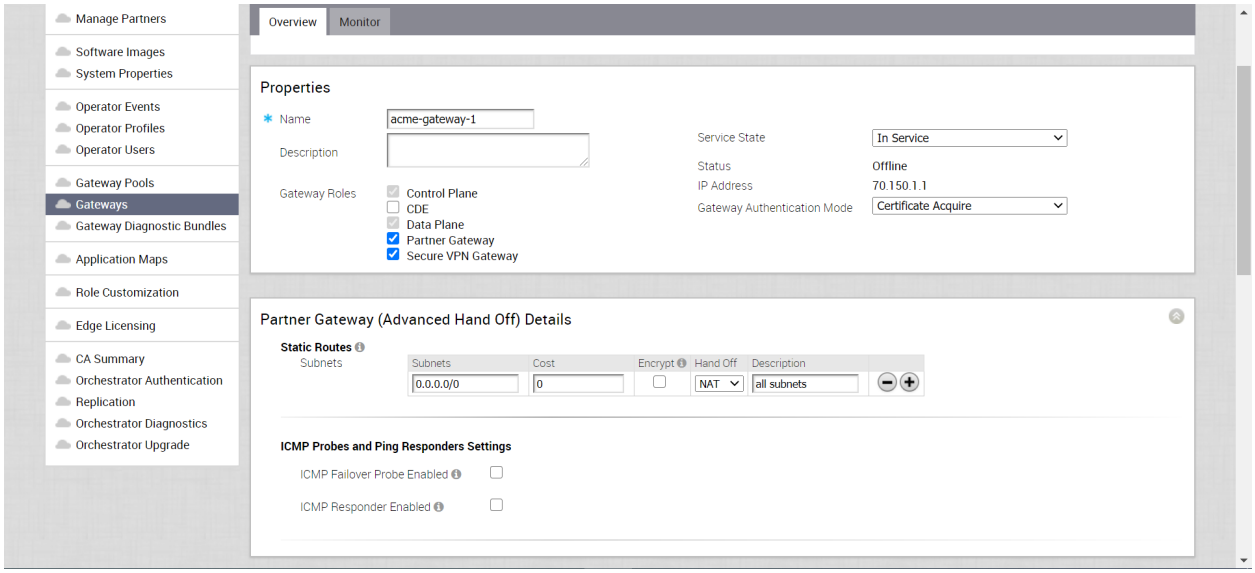


Activer le mode de passerelle de partenaires

Sur la même page **Passerelle (Gateway)** (**Opérateur (Operator) > Passerelles (Gateways)**), activez le mode de passerelle de partenaires en cochant la case **Passerelle partenaire (Partner Gateway)**. Décochez la case **Passerelle VPN sécurisée (Secure VPN Gateway)** (qui n'est nécessaire que si vous prévoyez d'utiliser cette instance de SD-WAN Gateway pour établir un tunnel IPSec vers un Non VMware SD-WAN Site).

Onglet **Présentation (Overview)**

L'écran **Passerelles (Gateways)** comprend les sections suivantes : Propriétés (Properties), Détails de la passerelle partenaire (transfert avancé) [Partner Gateway (Advanced Handoff) Details], Contact et emplacement (Contact & Location), Utilisation du client (Customer Usage), Appartenance au pool (Pool Membership). Pour plus d'informations sur ces sections, reportez-vous-y.



Zone **Propriétés (Properties)**

Outre les zones de texte Nom (Name) et Description, la zone **Propriétés (Properties)** comprend les options suivantes :

- État du service (Service State)
- État (Status) :
- Adresse IP (IP Address)
- Mode d'authentification de la passerelle (Gateway Authentication Mode) :
  - **Certificat désactivé (Certificate Disabled)** : Edge utilise un mode d'authentification par clé prépartagée.
  - **Acquisition de certificat (Certificate Acquire)** : cette option est sélectionnée par défaut et demande au dispositif Edge d'obtenir un certificat auprès de l'autorité de certification de SD-WAN Orchestrator, en générant une paire de clés et en envoyant une demande de signature de certificat à Orchestrator. Une fois le certificat acquis, le dispositif Edge l'utilise pour l'authentification auprès de SD-WAN Orchestrator et pour l'établissement de tunnels VCMP.

    Note Après l'acquisition du certificat, l'option peut être mise à jour sur **Certificat requis (Certificate Required)**.

  - **Certificat requis (Certificate Required)** : le dispositif Edge utilise le certificat PKI. (Les opérateurs peuvent modifier la fenêtre de temps de renouvellement du certificat pour les passerelles via les propriétés système. Pour plus d'informations, reportez-vous à la section Tableau 11-3. Autorité de certification).
- Rôles de passerelle (Gateway Roles) :
  - Plan de contrôle (Control Plane) :
  - CDE :

- Plan de données (Data Plane) :
- Passerelle partenaire (Partner Gateway) :
- Passerelle VPN sécurisée (Secure VPN Gateway) :

Zone **Détails de la passerelle partenaire (transfert avancé) [Partner Gateway (Advanced Handoff) Details]**

- Routes statiques : spécifiez les sous-réseaux ou les routes que SD-WAN Gateway doit annoncer à SD-WAN Edge, ainsi que le mode de transfert et si le trafic doit être chiffré ou non. Cela s'applique globalement par SD-WAN Gateway et à TOUS les clients. Avec BGP, cette section n'est généralement utilisée que s'il existe un sous-réseau partagé auquel tous les clients doivent accéder et si le transfert NAT est requis.

  Supprimez les sous-réseaux inutilisés de la liste des routes statiques ci-dessus si aucun sous-réseau ne doit être annoncé à SD-WAN Edge et si le transfert est de type NAT.

  Les paramètres de la sonde ICMP sont facultatifs et recommandés uniquement s'il est souhaitable qu'ICMP vérifie la santé de SD-WAN Gateway. Avec la prise en charge de BGP sur la passerelle de partenaires, il n'est plus nécessaire d'utiliser la sonde ICMP pour le basculement et la convergence des routes.
- Sonde de basculement ICMP : SD-WAN Gateway peut utiliser la sonde ICMP pour vérifier l'accessibilité d'une adresse IP particulière. Il peut informer SD-WAN Edge de basculer vers la passerelle secondaire si SD-WAN Gateway détecte l'inaccessibilité de l'adresse IP particulière.
- Répondeur ICMP activé : cela permet à SD-WAN Gateway de répondre à la sonde ICMP à partir du prochain routeur de tronçon lorsque ses tunnels sont actifs.
- Mode = Conditionnel : SD-WAN Gateway répond à la demande ICMP uniquement lorsque son service est actif et lorsqu'au moins un tunnel est actif.
- Mode = Toujours : SD-WAN Gateway répond toujours à la demande ICMP de son homologue.

Configurer le protocole BGP de passerelle

Cette section décrit la configuration du protocole BGP de la passerelle.

Configurer BGP

Cette section décrit comment configurer BGP sur des passerelles de partenaires. Par défaut, BGP est activé sur les passerelles de partenaires.

Pour plus d'informations sur BGP pour SD-WAN Edge, reportez-vous à la section *Configurer le routage dynamique avec OSPF ou BGP (Configure Dynamic Routing with OSPF or BGP)* dans le Guide de l'administrateur.

Note Nous prenons en charge le protocole BGP du numéro de système autonome (ASN, Autonomous System Number) 4 octets :

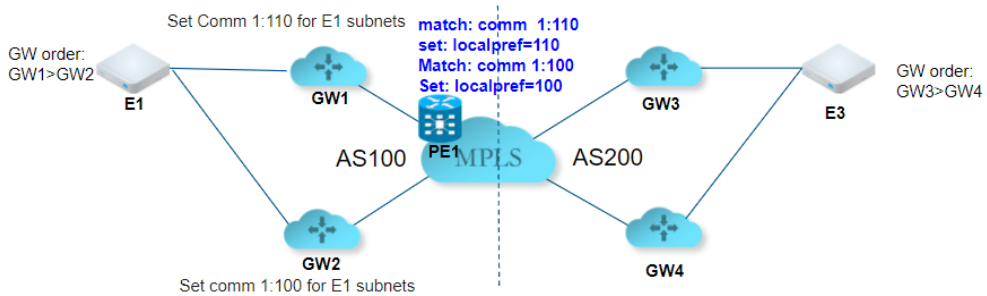
- En tant qu'ASN de SD-WAN Edge lui-même
- Effectuer une liaison avec un voisin ayant un ASN 4 octets
- Accepter les ASN 4 octets dans les annonces de route

Priorité BGP du client (communauté automatique)

La zone **Priorité BGP du client (Customer BGP Priority)** comprend la case **Activer le mappage de la communauté (Enable Community Mapping)**. Lorsque cette option est cochée, deux modes de mappage sont disponibles pour configurer les communautés, **Tous les segments (All Segments)** et **Par segment (Per Segment)**. La communauté comporte deux parties : **Communauté (Community)** et **Communauté 2 (Community 2)**.

Pour les fournisseurs de services qui déploient un client sur plusieurs instances de BGP AS et qui préfèrent utiliser des valeurs de communauté BGP pour contrôler la symétrie des chemins, il est possible d'attribuer automatiquement des valeurs de communauté BGP aux préfixes de branche en fonction des ordres de préférence des passerelles de partenaires pour cette branche. Par défaut, VMware attribue automatiquement les valeurs BGP MED au préfixe de la branche pour influencer le chemin BGP et obtenir la symétrie des chemins, qui s'applique à un seul scénario AS.

La topologie suivante fournit un exemple de ce cas d'utilisation.



Dans la topologie ci-dessus, plusieurs instances de MPLS BGP AS, valeurs de communauté BGP et valeurs de préférence locale sont utilisées sur les routeurs PE pour obtenir la symétrie des chemins. Pour la branche E1, l'ordre des passerelles de partenaires est GW1>GW2, ce qui implique que pour le trafic sortant, GW1 est préféré. Pour conserver la symétrie des chemins, GW1 doit attribuer une valeur de communauté de 1:110 pour faire correspondre la valeur PE BGP route-map configurée, de sorte que le chemin de retour préfère également GW1.

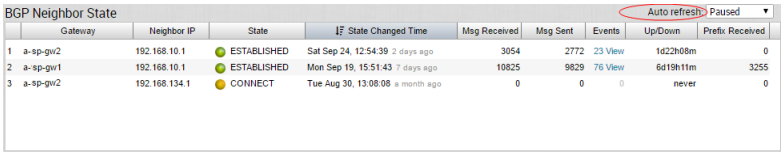
De même, GW2 doit attribuer une valeur de communauté de 1:00 pour faire correspondre la valeur PE BGP route-map configurée, ce qui la rend moins souhaitable. Cette opération sera automatisée via la fonctionnalité de communauté automatique (introduite dans la version 2.5). En attribuant des valeurs de communauté aux priorités GW, les passerelles de partenaires attribuent dynamiquement les valeurs de communauté correspondantes aux préfixes de la branche. Cette configuration s'applique au niveau du client.

Surveillance

Pour afficher les passerelles configurées :

1 Accédez à **Surveiller (Monitor) > Services réseau (Network Services)**.

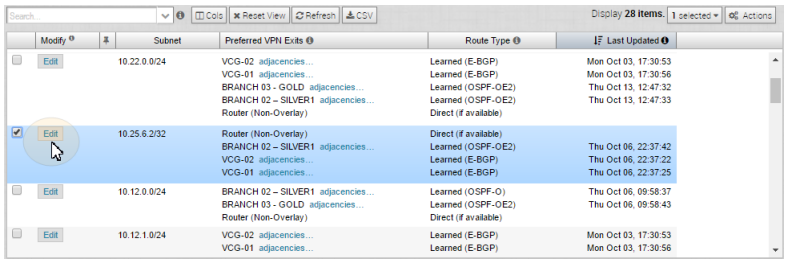
2 Dans l'écran **Services réseau (Network Services)**, faites défiler jusqu'à la zone **État du voisin BGP (BGP Neighbor State)** pour afficher vos passerelles configurées.



Note Dans le menu déroulant **Actualisation automatique (Auto refresh)**, vous pouvez définir la fréquence à laquelle la zone **État du voisin BGP (BGP Neighbor State)** est actualisée automatiquement (5, 30 ou 60 secondes), ou arrêter la fonctionnalité **Actualisation automatique (Auto refresh)** en choisissant **En pause (Paused)** dans le menu déroulant.

Contrôle des flux de superposition

Toutes les routes sont affichées dans la table **Contrôle de flux de superposition (Overlay Flow Control)**. Vous pouvez modifier l'ordre des sorties VPN préférées pour un sous-réseau particulier en cliquant sur le bouton **Modifier (Edit)** dans la colonne **Modifier (Modify)**.



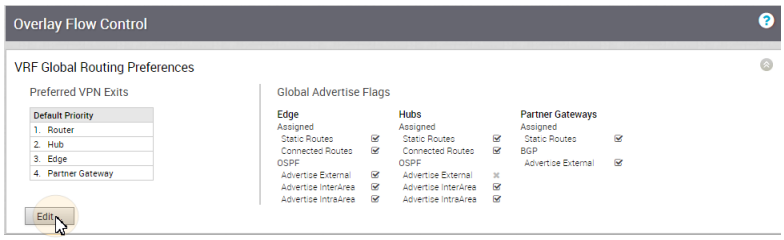
Nom de la colonne (Column Name)	Description
Modifier (Modify)	Accès pour modifier les configurations globales.
Sous-réseau (Subnet)	Réseau auquel cette route correspond, ainsi qu'une liste des dispositifs Edge ayant appris cette route.
Type de route (Route Type)	Les types sont les suivants : BGP, OSPF-O, OSPF-OE2, Statique (Static) et Connecté (Connected).

Nom de la colonne (Column Name)	Description
Sorties VPN préférées (Preferred VPN Exits)	Ordre de la sortie VPN.
Dernière mise à jour (Last Updated)	Date et l'heure auxquelles les routes sont apprises.

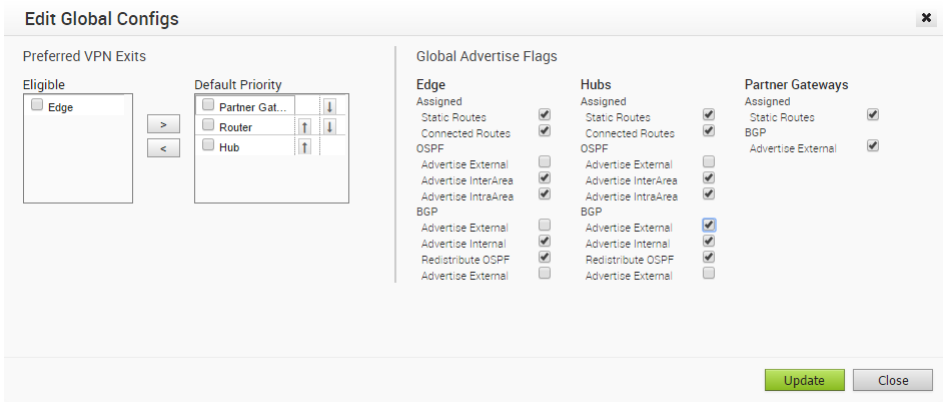
Modifier les configurations globales

Pour modifier les configurations globales :

1 Cliquez sur le bouton **Modifier (Edit)** au bas de la zone **Préférences de routage global (Global Routing Preferences)** du VRF pour ouvrir la boîte de dialogue **Modifier les configurations globales (Edit Global Configs)**.



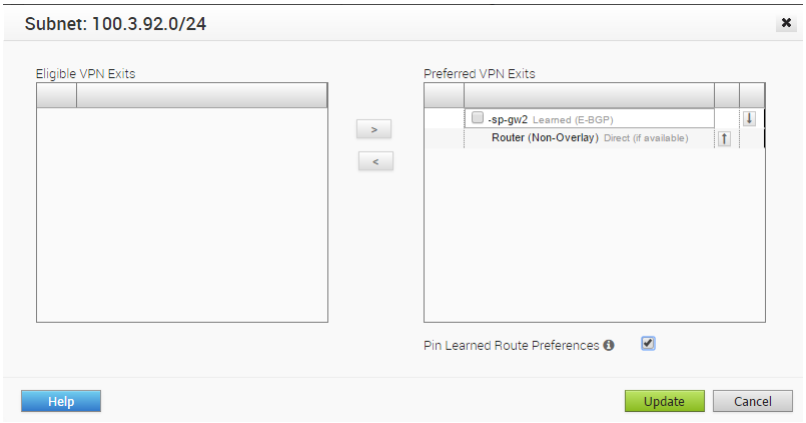
2 Dans la boîte de dialogue **Modifier les configurations globales (Edit Global Configs)**, modifiez la zone **Indicateurs d'annonce globale (Global Advertise Flags)** area.



Modifier le sous-réseau

En tant qu'option supplémentaire, vous pouvez modifier l'ordre de sortie de VPN en modifiant le sous-réseau.

Pour accéder à cette boîte de dialogue, cliquez sur le lien **Modifier (Edit)** dans la colonne **Modifier (Modify)** de la table **Contrôle de superposition (Overlay Control)**.



Exécuter des diagnostics pour les passerelles

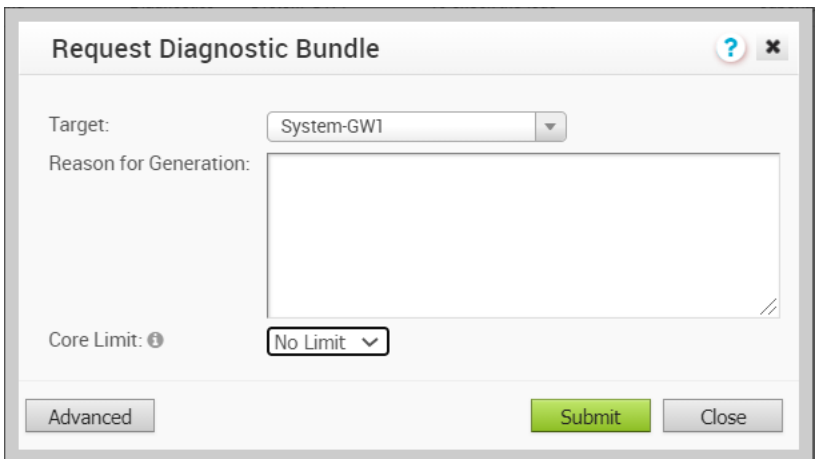
Les bundles de diagnostics permettent aux utilisateurs de collecter tous les fichiers de configuration et les fichiers journaux depuis une passerelle VMware SD-WAN Gateway spécifique dans un fichier compressé consolidé. Les données disponibles dans les bundles de diagnostics peuvent être utilisées par les ingénieurs de support VMware pour le dépannage des passerelles SD-WAN Gateways.

Dans le portail opérateur, cliquez sur **Bundles de diagnostics de la passerelle (Gateway Diagnostic Bundles)**.

Pour générer un bundle de diagnostics :

1 Cliquez sur **Demander le bundle de diagnostics (Request Diagnostic Bundle)**.

2 Dans la fenêtre **Demander le bundle de diagnostics (Request Diagnostic Bundle)**, configurez les paramètres suivants :

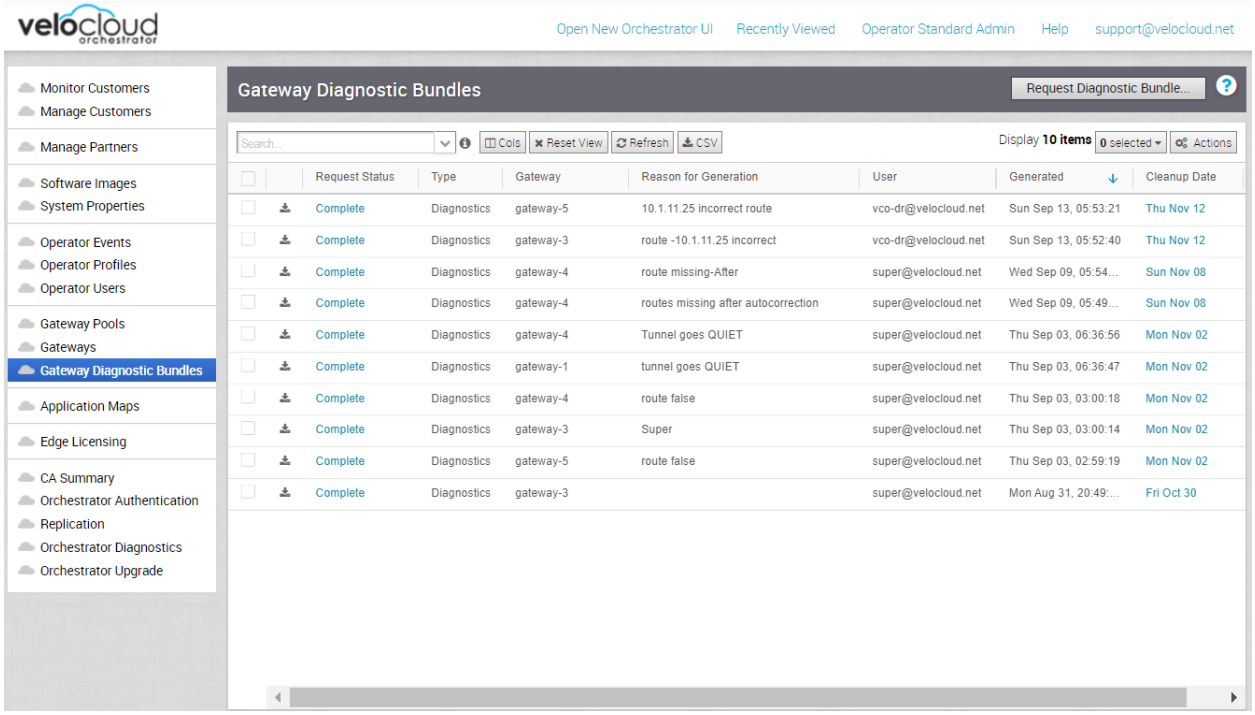


- **Cible (Target)** : sélectionnez la passerelle VMware SD-WAN Gateway cible dans la liste déroulante. Les données sont collectées à partir de la passerelle VMware SD-WAN Gateway sélectionnée.

- **Motif de la génération (Reason for Generation)** : vous pouvez éventuellement entrer la raison pour laquelle vous générez le bundle.
- Si nécessaire, cliquez sur le bouton **Avancé (Advanced)** et choisissez une valeur dans la liste déroulante **Limite de cœurs (Core Limit)**. La limite de cœurs est utilisée pour réduire la taille du bundle chargé lorsque la connectivité Internet rencontre des problèmes.

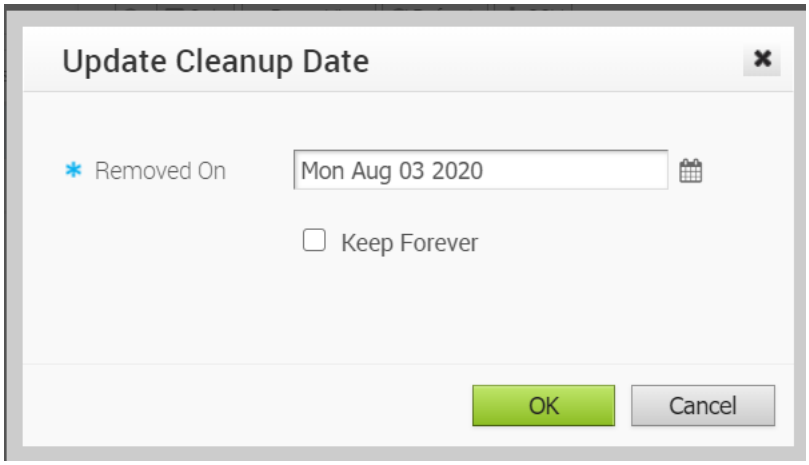
3 Cliquez sur **Envoyer (Submit)**.

La fenêtre **Bundles de diagnostics de la passerelle (Gateway Diagnostic Bundles)** affiche les détails des bundles générés, ainsi que l'état.



Pour télécharger un bundle généré, cliquez sur le lien **Terminé (Complete)** ou sélectionnez le bundle et cliquez sur **Actions > Télécharger le bundle de diagnostics (Download Diagnostic Bundle)**. Le bundle est téléchargé sous la forme d'un fichier ZIP.

Les bundles terminés sont supprimés automatiquement à la date affichée dans la colonne **Date de nettoyage (Cleanup Date)**. Vous pouvez cliquer sur le lien d'accès à la date de nettoyage pour modifier celle-ci.



Dans la fenêtre **Mettre à jour la date de nettoyage (Update Cleanup Date)**, choisissez la date de suppression du bundle sélectionné.

Si vous souhaitez conserver le bundle, cochez la case **Conserver indéfiniment (Keep Forever)** afin de ne pas supprimer automatiquement le bundle.

Pour supprimer un bundle manuellement, sélectionnez le bundle et cliquez sur **Actions > Supprimer (Delete)**.

Surveiller les passerelles

Vous pouvez surveiller l'état et les données d'utilisation des passerelles disponibles dans le portail opérateur.

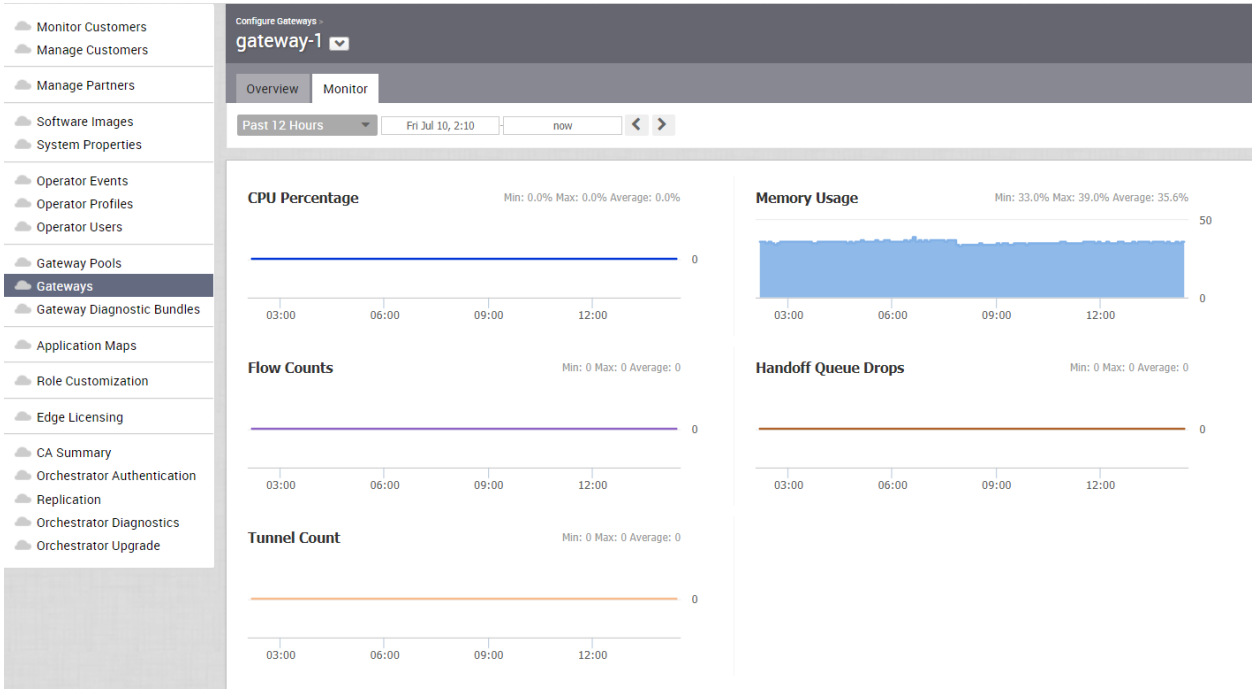
Pour surveiller les passerelles :

Procédure

1. Dans le portail de l'opérateur, cliquez sur **Passerelles (Gateways)**.
2. La page **Passerelles (Gateways)** affiche la liste des passerelles disponibles.
3. Cliquez sur le lien d'accès à une passerelle. Les détails de la passerelle sélectionnée s'affichent.
4. Cliquez sur l'onglet **Surveiller (Monitor)** pour afficher les données d'utilisation de la passerelle sélectionnée.

Résultats

L'onglet **Surveiller (Monitor)** de la passerelle sélectionnée affiche les détails suivants :



En haut de la page, vous pouvez choisir une période spécifique pour afficher les détails de la passerelle pour la durée sélectionnée.

Cette page affiche la représentation graphique des détails d'utilisation des paramètres suivants pendant la durée de la période sélectionnée, ainsi que les valeurs minimale, maximale et moyenne.

- **Pourcentage du CPU (CPU Percentage)** : pourcentage d'utilisation du CPU.
- **Utilisation de la mémoire (Memory Usage)** : pourcentage d'utilisation de la mémoire.
- **Nombre de flux (Flow Counts)** : nombre de flux de trafic.
- **Abandons des files d'attente de transfert (Handoff Queue Drops)** : nombre de paquets abandonnés en raison du transfert en file d'attente.
- **Nombre de tunnels (Tunnel Count)** : nombre de sessions du tunnel.

Pour afficher plus de détails, passez la souris sur les graphiques.

Vous pouvez également afficher les détails à l'aide de la nouvelle UI d'Orchestrator. Reportez-vous à la section Surveiller les passerelles à l'aide d'une nouvelle interface utilisateur d'Orchestrator.

Surveiller les passerelles à l'aide d'une nouvelle interface utilisateur d'Orchestrator

Vous pouvez surveiller l'état et les données d'utilisation du réseau des passerelles disponibles dans le portail opérateur.

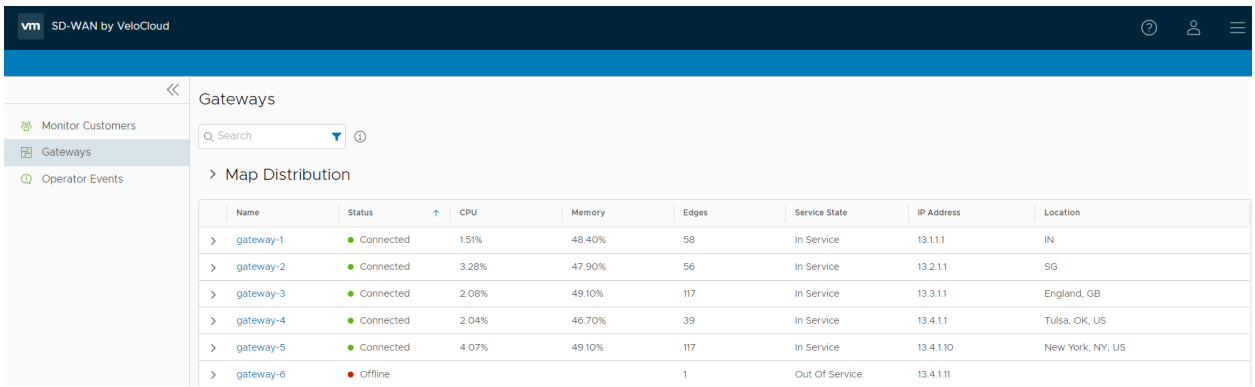
Pour surveiller les passerelles :

Procédure

1. Dans le portail opérateur, cliquez sur l'option **Ouvrir la nouvelle interface utilisateur d'Orchestrator (Open New Orchestrator UI)** disponible en haut de la fenêtre.
2. Cliquez sur **Lancer la nouvelle interface utilisateur d'Orchestrator (Launch New Orchestrator UI)** dans la fenêtre contextuelle. L'interface utilisateur s'ouvre dans un nouvel onglet affichant les options de surveillance.
3. Cliquez sur **Passerelles (Gateways)**.

Résultats

La page **Passerelles (Gateways)** affiche la liste des passerelles disponibles.



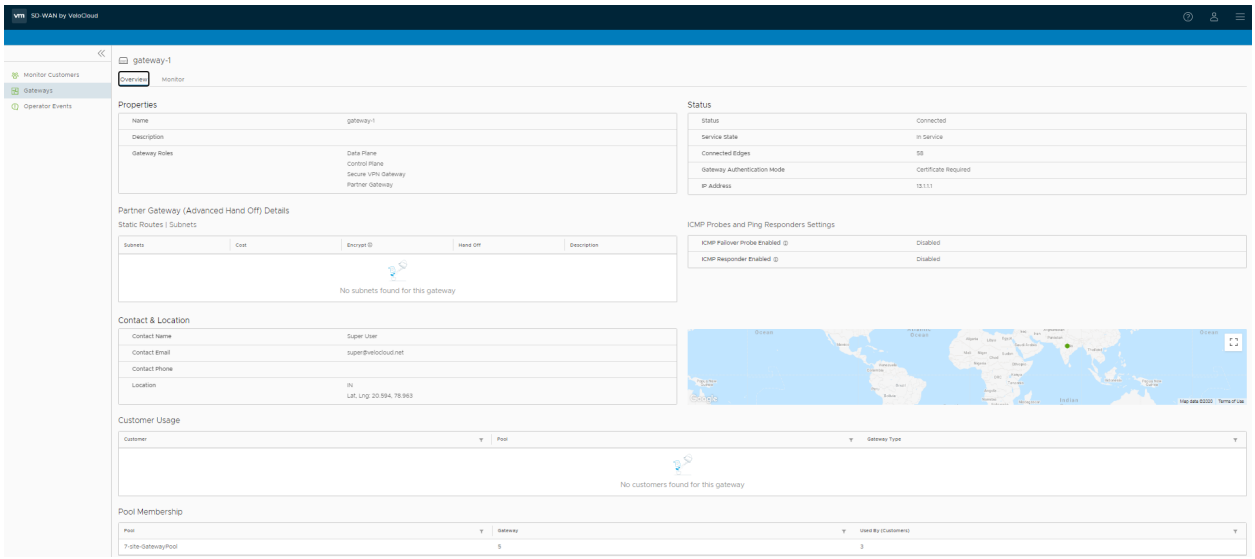
Cliquez sur **Distribution de la carte (Map Distribution)** pour développer et afficher les emplacements des passerelles sur la carte. Par défaut, cette vue est réduite.

Vous pouvez également cliquer sur les flèches avant chaque nom de passerelle pour afficher plus de détails.

La page affiche les détails suivants :

- **Nom (Name)** : nom de la passerelle.
- **État (Status)** : état actuel de la passerelle. L'état peut être l'un des suivants : Connecté (Connected), Dégradé (Degraded), Désactivé (Disabled), Jamais activé (Never Activated), Hors ligne (Offline), Hors service (Out of Service) ou Suspendu (Quiesced).
- **CPU** : pourcentage d'utilisation du CPU par la passerelle.
- **Mémoire (Memory)** : pourcentage d'utilisation de la mémoire par la passerelle.
- **Dispositifs Edge (Edges)** : nombre de dispositifs Edge connectés à la passerelle.
- **État du service (Service State)** : état du service de la passerelle. L'état peut être l'un des suivants : Historique (Historical), En service (In Service), Hors service (Out of Service), Service en attente (Pending Service) ou Suspendu (Quiesced).
- **Adresse IP (IP Address)** : adresse IP de la passerelle.
- **Emplacement (Location)** : emplacement de la passerelle.

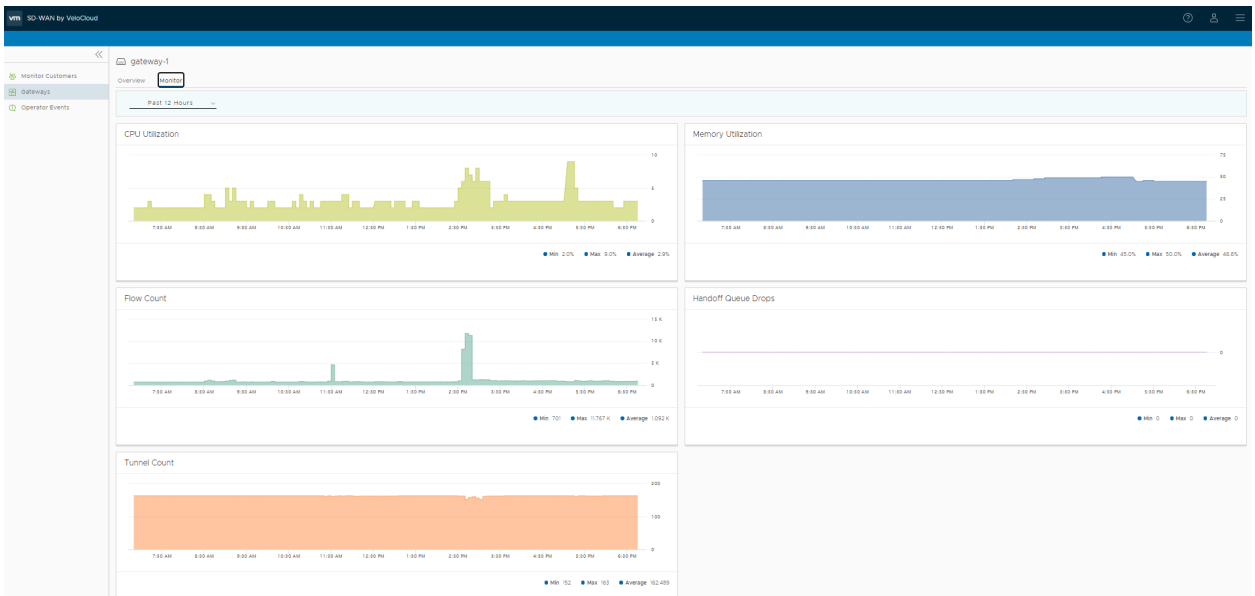
Cliquez sur le lien d'accès à une passerelle pour afficher les détails de la passerelle sélectionnée.



L'onglet **Présentation (Overview)** affiche les propriétés, l'état, l'emplacement, l'utilisation du client et le pool de passerelles de la passerelle sélectionnée.

Note Cet onglet permet uniquement d'afficher les détails de la passerelle. Pour configurer les informations sur la passerelle, accédez à la page **Passerelles (Gateways)** dans le portail opérateur.

Cliquez sur l'onglet **Surveiller (Monitor)** pour afficher les détails de l'utilisation de la passerelle sélectionnée.

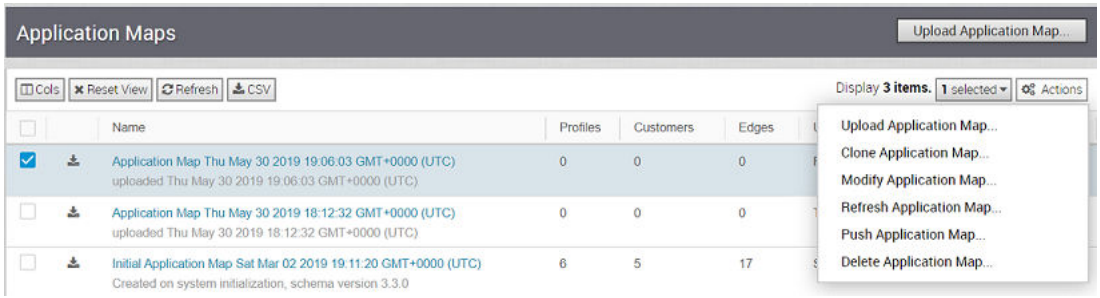


Pour plus d'informations sur les données affichées, reportez-vous à la section Surveiller les passerelles.

Mappages d'applications 14

Les **Mappages d'applications (Application Maps)** sont des fichiers JSON constitués de plusieurs applications contenant des définitions, qui peuvent être utilisés lors de la création de stratégies commerciales.

Dans le panneau de l'opérateur, cliquez sur **Mappages d'applications (Application Maps) > Actions** pour effectuer les activités suivantes.



- **Charger le mappage d'applications (Upload Application Map)** : autorise le chargement du fichier JSON avec les applications et les définitions. Reportez-vous à la section Charger la carte d'application.
- **Cloner un mappage d'applications (Clone Application Map)** : crée un mappage d'applications en clonant un fichier de mappage d'applications existant. Reportez-vous à la section Cloner une carte d'application.
- **Modifier le mappage d'applications (Modify Application Map)** : permet d'ajouter ou de mettre à jour les informations des applications disponibles dans le mappage d'applications sélectionné. Reportez-vous à la section Modifier la carte d'application.
- **Actualiser le mappage d'applications (Refresh Application Map)** : met à jour les définitions d'applications répertoriées dans les mappages d'applications sélectionnés. Reportez-vous à la section Actualiser le mappage d'application.
- **Transférer le mappage d'applications (Push Application Map)** : transfère les dernières mises à jour des définitions d'applications disponibles dans les mappages d'applications vers les dispositifs SD-WAN Edges associés. Reportez-vous à la section Transférer le mappage d'application.

- **Supprimer le mappage d'applications (Delete Application Map)** : supprime les mappages d'applications sélectionnés. Vous ne pouvez pas supprimer un mappage qui a été attribué à un profil d'opérateur.

Ce chapitre contient les rubriques suivantes :

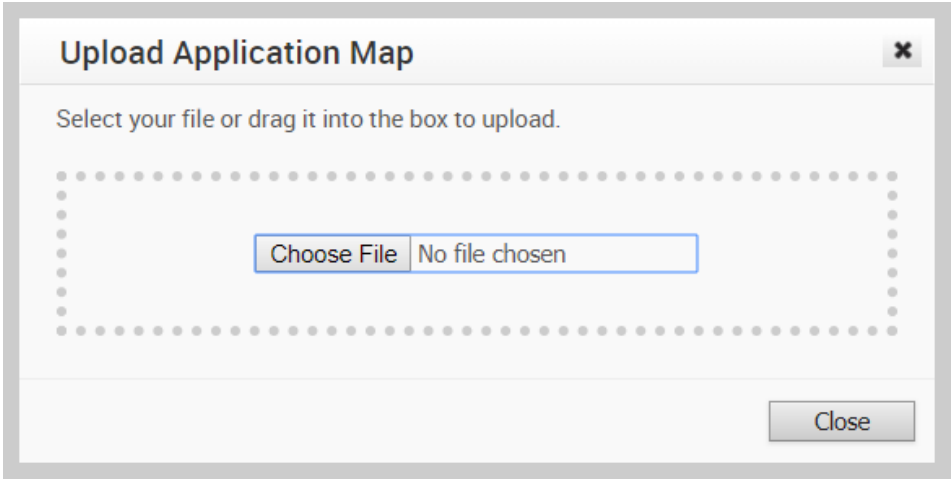
Charger la carte d'application

VMware SD-WAN fournit une carte d'application initiale avec les applications possibles. Vous pouvez également charger votre fichier JSON avec les applications à utiliser dans les business policies.

Sur le portail opérateur, cliquez sur **Cartes d'applications (Application Maps)**.

1 Pour charger un fichier de mappage, cliquez sur **Charger la carte d'application (Upload Application Map)** ou sur **Actions > Charger la carte d'application (Upload Application Map)**.

2 Dans la fenêtre **Charger la carte d'application (Upload Application Map)**, choisissez votre fichier de carte d'application.



Après la validation du contenu, le fichier est chargé.

Celui-ci est au format JSON et vous pouvez personnaliser les applications selon vos besoins. L'exemple suivant illustre un fichier JSON personnalisé pour l'application `bittorrent`.

```
{
            "id": 15,
            "name": "APP_BITTORRENT",
            "displayName": "bittorrent",
```

```
            "class": 14,
            "description": "BitTorrent is a peer-to-peer protocol. [Note: bittorrent is also
known as kadmelia.]",
            "knownIpPortMapping": {},
            "protocolPortMapping": {},
            "doNotSlowLearn": 1,
            "mustNotUseGateway": 1
        }
```


Vous pouvez afficher les fichiers chargés dans la fenêtre **Cartes d'applications (Application Maps)** et, si nécessaire, télécharger le fichier.

Pour attribuer une carte d'application à un profil d'opérateur, reportez-vous à la section Gérer les profils d'opérateur.

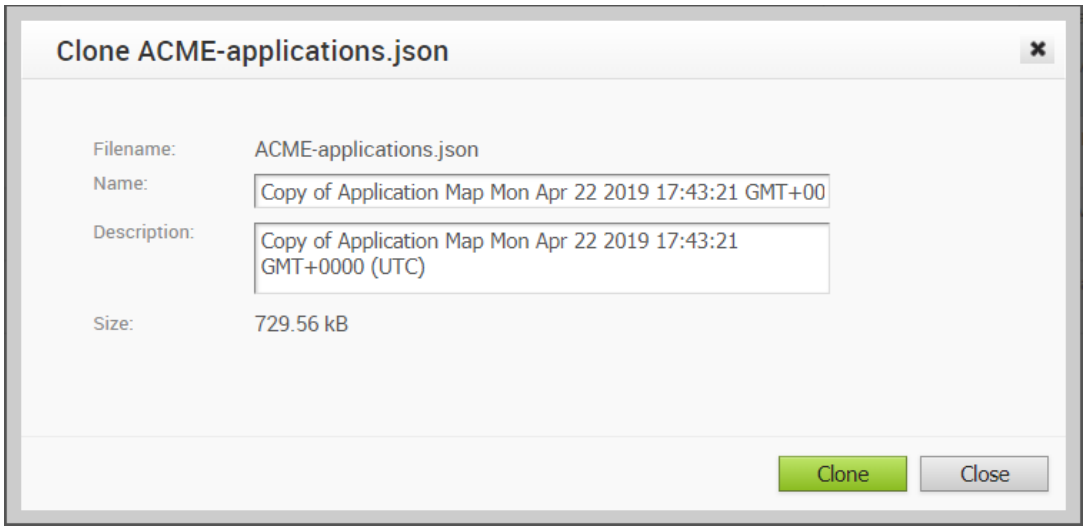
Cloner une carte d'application

Vous pouvez créer une carte d'application en clonant une carte dl'application existante.

Sur le portail opérateur, cliquez sur **Cartes d'applications (Application Maps)**.

1 Sélectionnez la carte d'application à cloner, puis cliquez sur **Actions > Cloner une carte d'application (Clone Application Map)**.

2 Dans la fenêtre **Cloner une carte d'application (Clone Application Map)**, entrez un nouveau nom et une description pour la carte d'application.



3 Cliquez sur **Cloner (Clone)**.

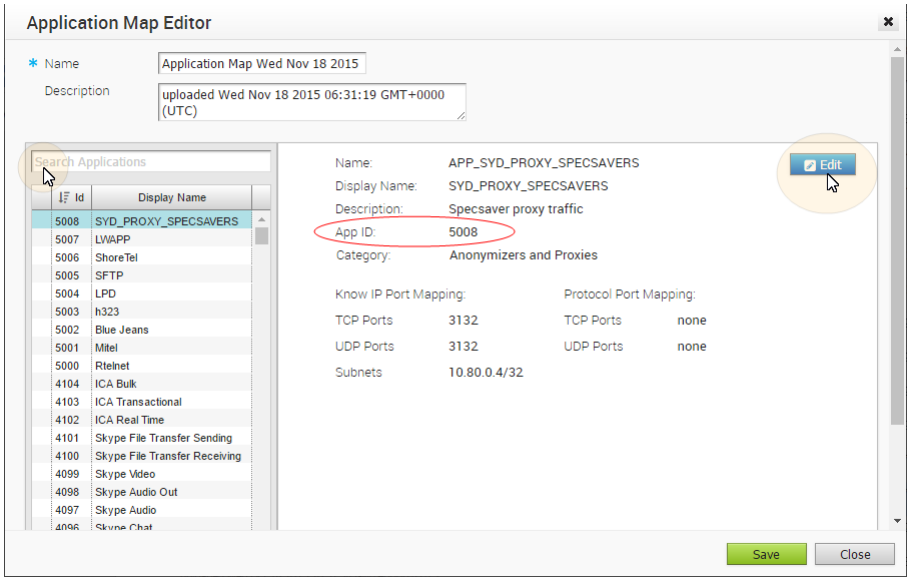
Modifier la carte d'application

Vous pouvez ajouter ou mettre à jour les détails d'application disponibles dans les cartes d'applications existantes.

Sur le portail opérateur, cliquez sur **Cartes d'applications (Application Maps)**.

1 Sélectionnez la carte d'application à mettre à jour et cliquez sur **Actions > Modifier la carte d'application (Modify Application Map)** ou cliquez sur le lien vers la carte d'application.

2 L'**éditeur de carte d'application (Application Map Editor)** affiche la liste des définitions d'applications disponibles dans le fichier de mappage.

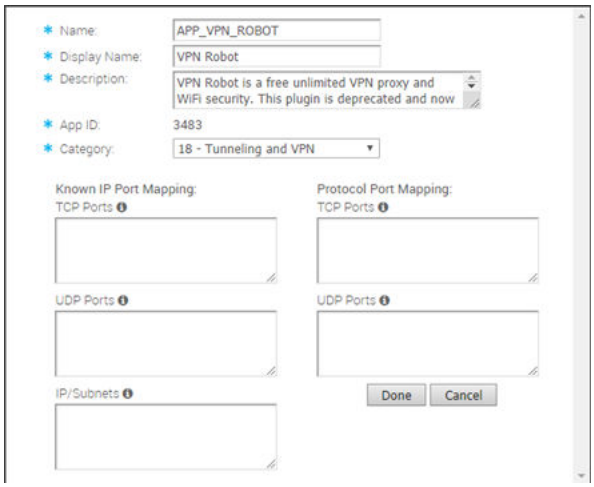


Sélectionnez une définition d'application et affichez les informations détaillées relatives la définition sélectionnée. Vous pouvez également rechercher une définition d'application, trier les définitions par ID d'application nom d'affichage, créer une définition d'application ou supprimer une définition existante.

3 Pour ajouter une définition à la liste, cliquez sur **Ajouter nouvelle (Add New)**.

4 Pour supprimer une définition de la liste, cliquez sur **Supprimer (Remove)**.

5 Pour modifier les détails de la définition sélectionnée, cliquez sur **Modifier (Edit)**.



Mettez à jour les détails tels que le nom, le nom d'affichage, la description, la catégorie, les ports et cliquez sur **Terminé (Done)**.

Lorsque vous créez une définition, l'ID d'application est attribué automatiquement.

Vous pouvez télécharger la carte d'application sous la forme d'un fichier JSON pour attribuer des indicateurs supplémentaires aux définitions d'applications. Vous pouvez également modifier l'ID d'application. Il est alors recommandé de définir les ID comme suit :

Pour les versions antérieures à la version 3.3.2 :

- 0-4999 pour les applications DPI
- 5000-5999 pour les applications VMware SD-WAN
- 6000-6999 pour les applications définies par l'utilisateur

Pour les versions 3.3.2 et ultérieures :

- 0-4999 pour les applications DPI
- 5000-5999 pour les applications VMware SD-WAN
- 6000-9999 pour les applications définies par l'utilisateur

6 Dans l'**éditeur de carte d'application (Application Map Editor)**, cliquez sur **Enregistrer (Save)**.

Pour charger une carte d'application personnalisé, reportez-vous à la section Charger la carte d'application.

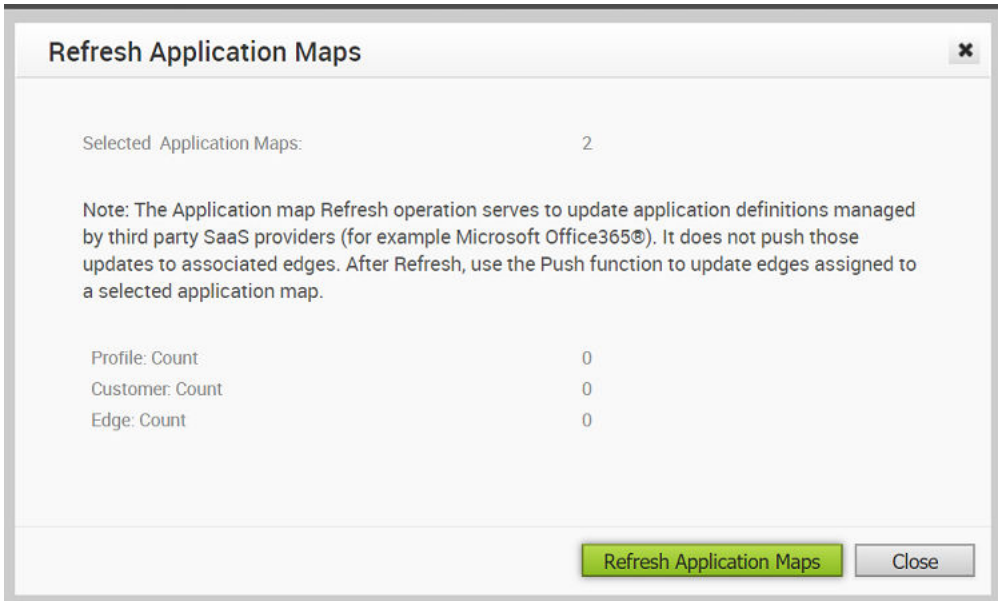
Actualiser le mappage d'application

Vous pouvez mettre à jour les définitions d'applications, gérées par des fournisseurs SaaS tiers, qui sont répertoriées dans le mappage d'application.

Sur le portail opérateur, cliquez sur **Mappages d'applications (Application Maps)**.

1 Sélectionnez les mappages d'applications à actualiser et cliquez sur **Actions > Actualiser le mappage d'applications (Refresh Application Map)**.

2 La page **Actualiser les mappages d'applications (Refresh Application Maps)** s'ouvre. Cette page répertorie le nombre de profils d'opérateur, de clients et de dispositifs SD-WAN Edges associés aux mappages d'applications sélectionnés.



3 Cliquez sur **Actualiser les mappages d'applications (Refresh Application Maps)** pour actualiser les mappages d'applications sélectionnés.

Note Vous pouvez uniquement mettre à jour les définitions d'applications dans les mappages d'applications à l'aide de l'option Actualiser (Refresh). Si vous souhaitez mettre à jour les dispositifs SD-WAN Edges associés avec les définitions les plus récentes, utilisez l'option Transférer le mappage d'application.

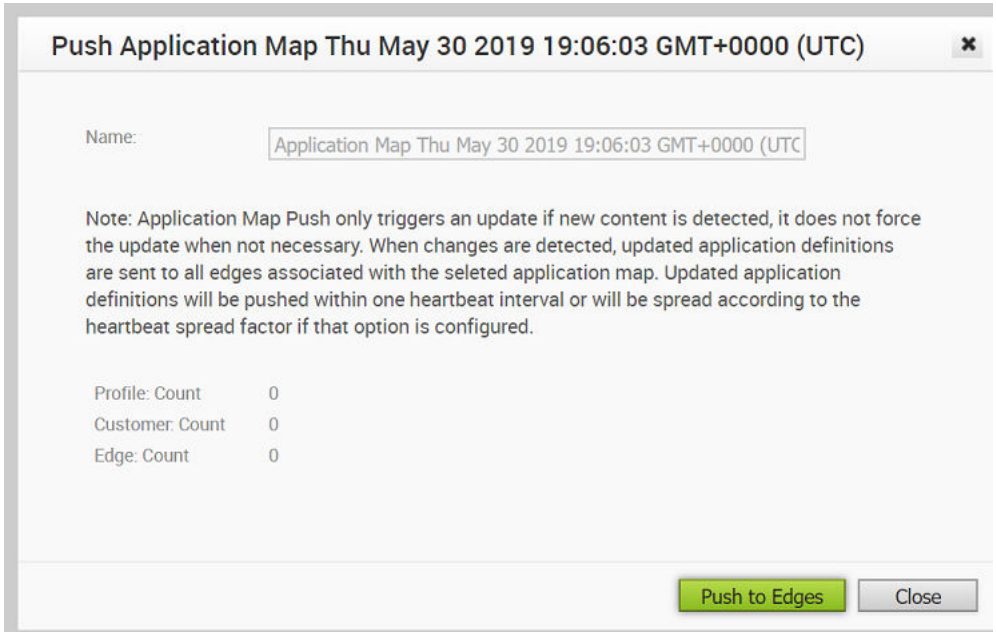
Transférer le mappage d'application

Vous pouvez transférer les dernières mises à jour des définitions d'applications disponibles dans les mappages d'applications vers les dispositifs SD-WAN Edges associés.

Sur le portail opérateur, cliquez sur **Mappages d'applications (Application Maps)**.

1 Sélectionnez le mappage d'application que vous souhaitez transférer vers les dispositifs SD-WAN Edges associés et cliquez sur **Actions > Transférer le mappage d'applications (Push Application Map)**.

2 La page **Transférer le mappage d'applications (Push Application Map)** s'ouvre. Cette page répertorie le nombre de profils d'opérateur, de clients et de dispositifs SD-WAN Edges associés au mappage d'application sélectionné.



3 Cliquez sur **Transférer vers les dispositifs Edge (Push to Edges)** pour mettre à jour les dispositifs SD-WAN Edges avec les dernières définitions d'applications disponibles dans le mappage d'application sélectionné.

Note Cette option permet de transférer les définitions d'applications uniquement lorsque des mises à jour sont disponibles.

Personnalisation des rôles

15

SD-WAN Orchestrator se compose de rôles d'utilisateur disposant d'un ensemble de privilèges différent. En tant que super utilisateur opérateur, vous pouvez attribuer un rôle prédéfini à un utilisateur. La personnalisation des rôles vous permet de personnaliser l'ensemble de privilèges existant pour les rôles d'utilisateur.

Pour activer ou de désactiver un super utilisateur partenaire afin de personnaliser les privilèges de rôle des autres utilisateurs partenaires et des utilisateurs d'entreprise du partenaire, reportez-vous à la section Configurer les informations sur les partenaires.

Pour activer ou désactiver un super utilisateur d'entreprise afin de personnaliser les privilèges de rôle des autres utilisateurs d'entreprise, reportez-vous à la section Configurer les clients.

La personnalisation des rôles s'applique aux rôles d'utilisateur de la manière suivante :

- Les personnalisations effectuées au niveau de l'entreprise remplacent les personnalisations effectuées au niveau du partenaire ou de l'opérateur.
- Les personnalisations effectuées au niveau du partenaire remplacent les personnalisations effectuées au niveau de l'opérateur.
- Les personnalisations effectuées par l'opérateur s'appliquent à tous les utilisateurs globalement dans SD-WAN Orchestrator uniquement lorsqu'aucune personnalisation n'est effectuée au niveau du partenaire ou de l'entreprise.

Dans le portail de l'opérateur, cliquez sur **Personnalisation des rôles (Role Customization)**.

Vous pouvez effectuer les opérations suivantes :

- **Afficher les privilèges actuels (Show Current Privileges)** : affiche les privilèges de rôle d'utilisateur actuels. Vous pouvez afficher les privilèges de tous les rôles d'utilisateur et les télécharger au format CSV.
- **Nouveau module (New Package)** : permet de créer un module avec des privilèges de rôle personnalisés. Reportez-vous à la section Créer un module personnalisé.
- **Rétablir les valeurs système par défaut (Reset to System Default)** : permet de réinitialiser les privilèges de rôle actuels aux paramètres par défaut. Seuls les privilèges personnalisés appliqués aux rôles d'utilisateur dans le portail de l'opérateur sont réinitialisés aux paramètres par défaut. Si vos partenaires ou vos clients ont personnalisé leurs privilèges de rôle utilisateur dans le portail partenaire ou d'entreprise, ces paramètres restent identiques.

Cliquez sur **Actions** pour effectuer les activités suivantes :

- **Charger le module (Upload Package)** : permet de charger un module personnalisé. Reportez-vous à la section Télécharger un module personnalisé.
- **Cloner le module (Clone Package)** : permet de créer une copie du module sélectionné.
- **Modifier le module (Modify Package)** : permet de modifier les paramètres de personnalisation du module sélectionné. Vous pouvez également cliquer sur le lien d'accès au module pour modifier les paramètres.
- **Supprimer le module (Delete Package)** : supprime le module sélectionné. Vous ne pouvez pas supprimer un module s'il est déjà utilisé.
- **Appliquer le module (Apply Package)** : applique la personnalisation disponible dans le module sélectionné aux rôles d'utilisateur existants. Cette option modifie les privilèges de rôle uniquement au niveau actuel. Si des personnalisations sont disponibles au niveau de l'opérateur ou à un niveau inférieur pour le même rôle, le niveau inférieur est prioritaire.

Vous pouvez également cliquer sur l'icône de téléchargement, située devant le nom du module, pour télécharger le module sous la forme d'un fichier JSON.

Note Les modules de personnalisation des rôles dépendent de la version. Un module créé sur une instance d'Orchestrator à l'aide d'une version logicielle antérieure ne sera alors pas compatible avec une instance d'Orchestrator utilisant une version ultérieure. Par exemple, un module de personnalisation des rôles créé sur un dispositif Orchestrator exécutant la version 3.4.x ne fonctionne pas correctement si Orchestrator est mis à niveau vers une version 4.x. En outre, un module de personnalisation des rôles créé sur un dispositif Orchestrator exécutant la version 3.4.x ne fonctionne pas correctement lorsqu'Orchestrator est mis à niveau vers une version 4.x.x. Dans ce cas, l'utilisateur doit vérifier et recréer le module de personnalisation des rôles pour la nouvelle version afin de garantir une application appropriée de tous les rôles.

Ce chapitre contient les rubriques suivantes :

- Créer un module personnalisé
- Télécharger un module personnalisé

Créer un module personnalisé

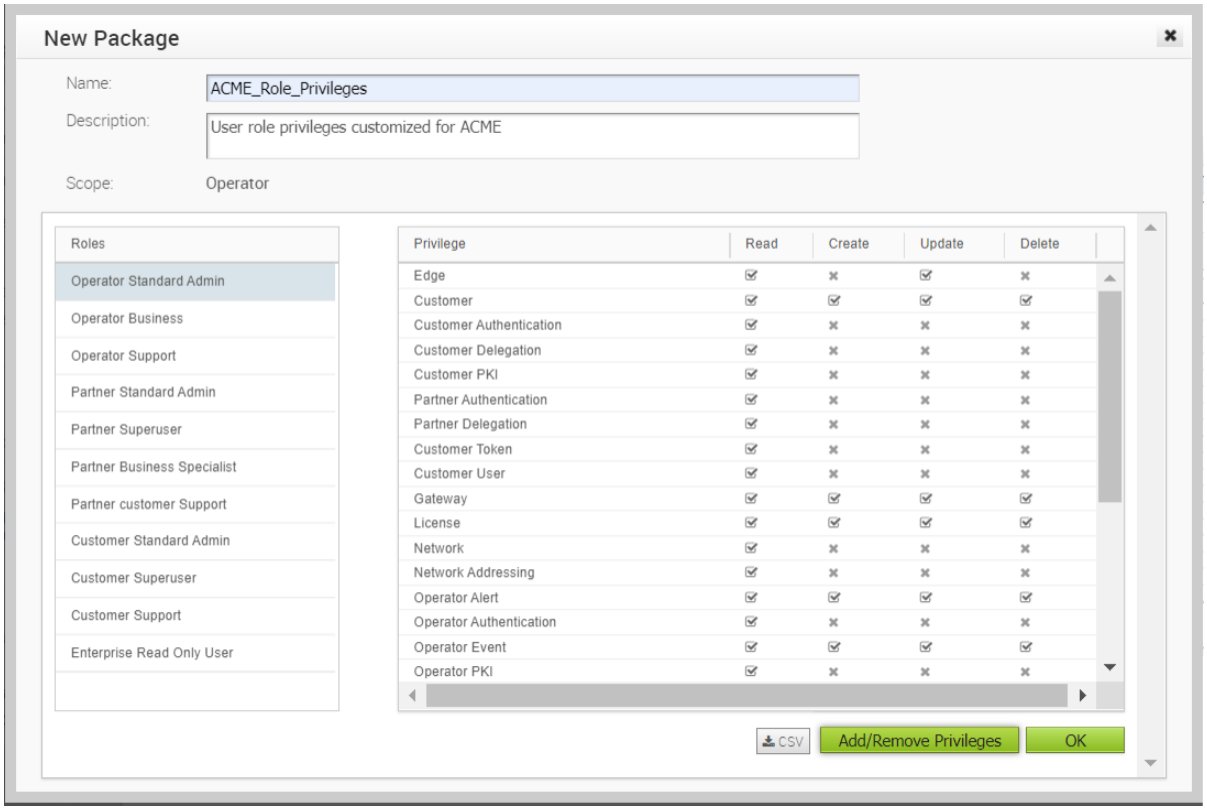
Vous pouvez créer un module personnalisé et l'appliquer aux rôles d'utilisateur existants dans SD-WAN Orchestrator.

Procédure

1 Dans le portail de l'opérateur, cliquez sur **Personnalisation des rôles (Role Customization)**.

2 Cliquez sur **Nouveau module (New Package)**.

3 Dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)**, entrez les informations suivantes :

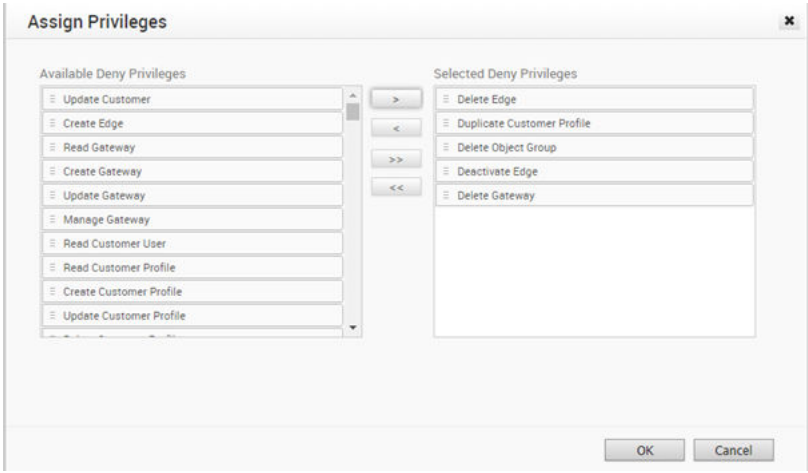


a Remplissez les champs **Nom (Name)** et **Description** pour le nouveau module personnalisé.

b Dans le volet **Rôles (Roles)**, sélectionnez un rôle d'utilisateur et cliquez sur **Ajouter/Supprimer des privilèges (Add/Remove Privileges)** pour personnaliser les privilèges du rôle sélectionné.

Note Vous pouvez uniquement ajouter ou supprimer les privilèges de refus, c'est-à-dire retirer les privilèges de la valeur par défaut système. Vous ne pouvez pas accorder de privilèges supplémentaires à un rôle à l'aide de cette option.

Dans la fenêtre **Attribuer des privilèges (Assign Privileges)**, sélectionnez des fonctionnalités dans le volet **Privilèges de refus disponibles (Available Deny Privileges)** et déplacez-les vers le volet **Privilèges de refus sélectionnés (Selected Deny Privileges)**.

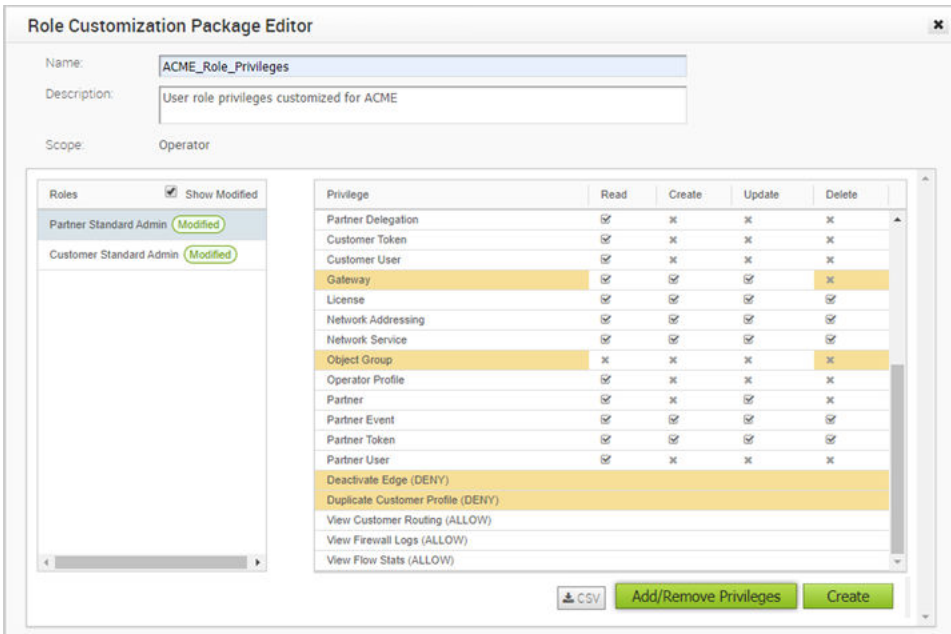


Note Vous pouvez attribuer uniquement des privilèges **Refuser (Deny)** aux rôles d'utilisateur.

Cliquez sur **OK**.

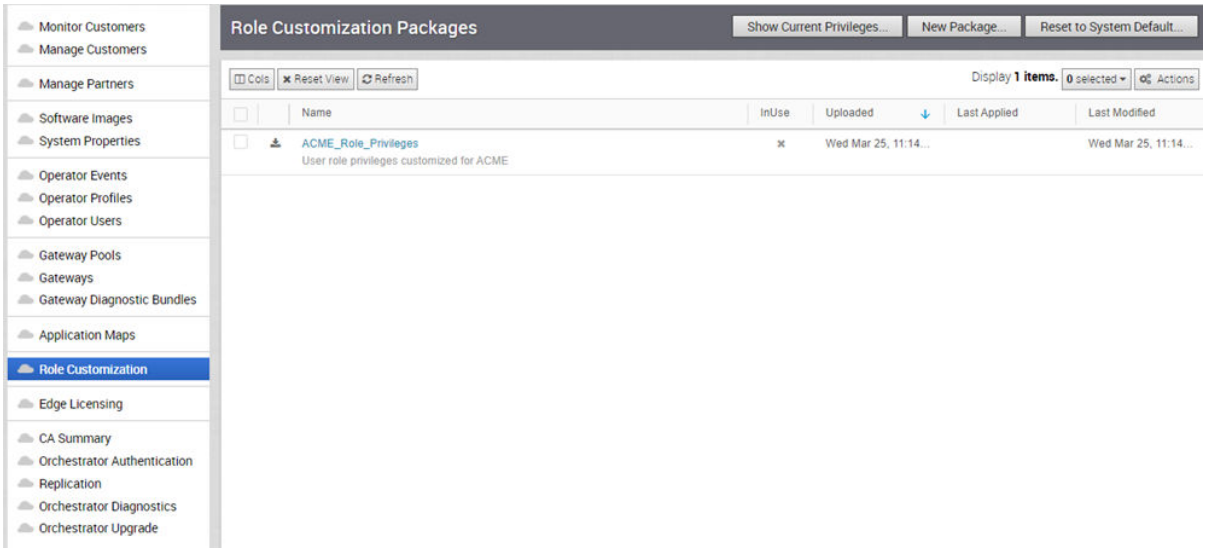
4 Dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)**, continuez à attribuer des privilèges aux rôles d'utilisateur.

5 Cochez la case **Afficher les modifications (Show Modified)** pour filtrer et afficher les privilèges personnalisés. Les modifications apportées aux privilèges sont mises en surbrillance dans une couleur différente.



6 Cliquez sur **Créer (Create)**. Vous pouvez cliquer sur **CSV** pour télécharger les privilèges du rôle d'utilisateur sélectionné au format CSV.

7 Les informations sur le nouveau module s'affichent dans la fenêtre **Modules de personnalisation des rôles (Role Customization Packages)**.



8 Pour modifier les privilèges, cliquez sur le lien d'accès au module ou sélectionnez ce dernier et cliquez sur **Actions > Modifier le module (Modify Package)**. Dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)** qui s'affiche, ajoutez ou supprimez des privilèges de refus aux rôles d'utilisateur du module, puis cliquez sur **OK**.

Étape suivante

Sélectionnez le module personnalisé et cliquez sur **Actions > Appliquer le module (Apply Package)** pour appliquer la personnalisation disponible dans le module sélectionné aux rôles d'utilisateur existants dans l'ensemble de SD-WAN Orchestrator.

Si nécessaire, vous pouvez modifier les privilèges de refus dans un module appliqué. Après avoir modifié les privilèges dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)**, cliquez sur **OK** pour enregistrer les modifications et les appliquer aux rôles d'utilisateur.

Note Vous pouvez télécharger les privilèges de rôle d'utilisateur personnalisés en tant que fichier JSON et télécharger le module personnalisé vers une autre instance d'Orchestrator. Pour plus d'informations, reportez-vous à la section Télécharger un module personnalisé.

Télécharger un module personnalisé

Vous pouvez télécharger un module avec des privilèges de rôle personnalisés attribués à différents ensembles de rôles d'utilisateur dans SD-WAN Orchestrator.

Vous pouvez télécharger les privilèges de rôle d'utilisateur déjà personnalisés en tant que module et télécharger le module dans un autre dispositif Orchestrator.

Procédure

1 Dans le portail de l'opérateur, cliquez sur **Personnalisation des rôles (Role Customization)**.

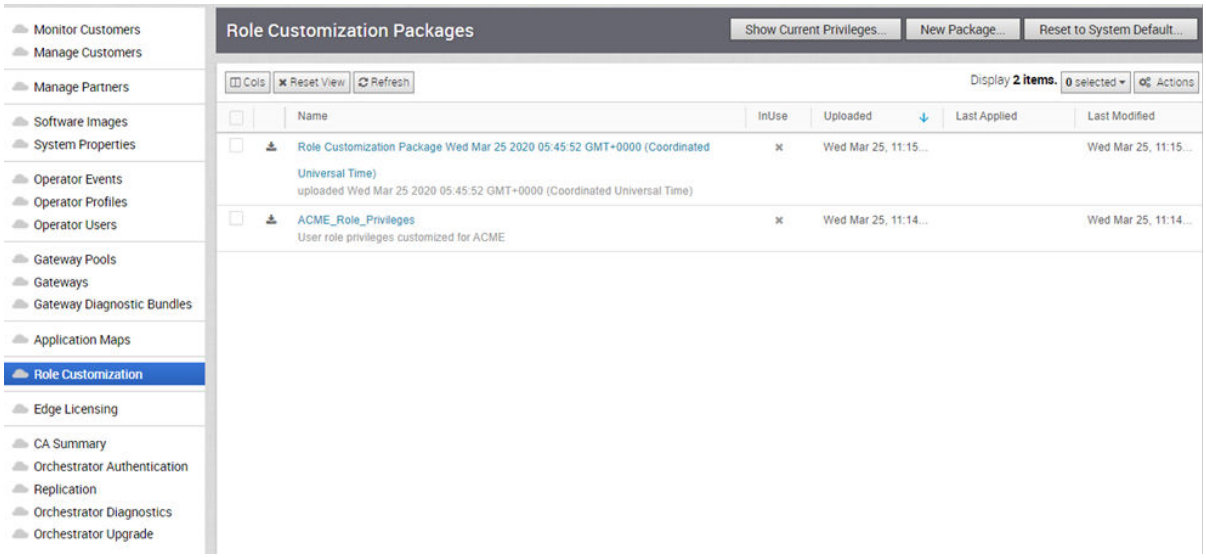
2 Cliquez sur l'icône Télécharger (Download), située devant le nom d'un module, pour télécharger le module sous la forme d'un fichier JSON.

3 Accédez au dispositif Orchestrator vers lequel vous souhaitez charger le module personnalisé.

4 Cliquez sur **Actions > Charger le module (Upload Package)**.

5 Choisissez le fichier JSON que vous avez téléchargé ; le module est alors téléchargé automatiquement.

6 Le module chargé s'affiche dans la fenêtre **Modules de personnalisation des rôles (Role Customization Packages)**.



7 Vous pouvez afficher les privilèges du module chargé et ajouter d'autres privilèges de refus. Cliquez sur le lien vers le module ou sélectionnez le module et cliquez sur **Actions > Modifier le module (Modify Package)**. Dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)** qui s'affiche, ajoutez ou supprimez des privilèges de refus aux rôles d'utilisateur du module, puis cliquez sur **OK**. Pour plus d'informations sur l'**Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)**, reportez-vous à la section Créer un module personnalisé.

Étape suivante

Sélectionnez le module personnalisé et cliquez sur **Actions > Appliquer le module (Apply Package)** pour appliquer la personnalisation disponible dans le module sélectionné aux rôles d'utilisateur existants dans l'ensemble de SD-WAN Orchestrator.

Si nécessaire, vous pouvez modifier les privilèges de refus dans un module appliqué. Après avoir modifié les privilèges dans la fenêtre **Éditeur de modules de personnalisation des rôles (Role Customization Package Editor)**, cliquez sur **OK** pour enregistrer les modifications et les appliquer aux rôles d'utilisateur.

Gestion des licences Edge

16

SD-WAN Orchestrator fournit différents types de licences pour les dispositifs SD-WAN Edges. Un opérateur peut gérer et attribuer des licences Edge aux partenaires et aux clients d'entreprise. Les partenaires peuvent attribuer des types de licences Edge à leurs clients d'entreprise.

La gestion des licences Edge est activée par défaut.

Pour désactiver la gestion des licences Edge, définissez la valeur de la propriété système **session.options.enableEdgeLicensing** sur **Faux (False)**. Sur le portail opérateur, cliquez sur **Propriétés système (System Properties)** pour mettre à jour la valeur de la propriété.

Les licences Edge sont disponibles avec les composants suivants :

Composant	Attributs pris en charge
Bande passante	10 M, 30 M, 50 M, 100 M, 200 M, 350 M, 500 M, 750 M, 1 G, 2 G, 5 G, 10 G
Éditions	Standard, Entreprise, Premium
Région	Amérique du Nord, Amérique latine, Asie-Pacifique, Europe Moyen-Orient et Afrique (EMEA)
Terme	12 mois, 36 mois, 60 mois

Un opérateur peut attribuer différents types de licences Edge à partir des 324 types de licences disponibles avec diverses combinaisons.

Outre la liste ci-dessus, VMware propose une version d'évaluation de licence avec les attributs suivants :

Composant	Attributs pris en charge
Bande passante	10 Gbits/s
Édition	POC
Région	Amérique du Nord, Europe Moyen-Orient et Afrique (EMEA), Asie-Pacifique et Amérique latine
Terme	60 mois

Note Vous pouvez attribuer la licence **Validation technique (POC)** à un client à titre de licence d'évaluation. Si nécessaire, vous pouvez mettre à niveau la licence vers toute autre édition souhaitée.

Pour attribuer des licences Edge à de nouveaux partenaires, reportez-vous à la section Créer un partenaire.

Pour gérer et attribuer des licences Edge à des partenaires existants, reportez-vous à la section Gérer les licences Edge pour des partenaires.

Pour attribuer des licences Edge à de nouveaux clients, reportez-vous à la section Créer un client.

Pour gérer et attribuer des licences Edge à des clients existants, reportez-vous à la section Gérer les licences Edge pour des clients.

Pour afficher et générer un rapport sur les types de licences Edge disponibles, reportez-vous à la section Générer un rapport sur les licences Edge.

Ce chapitre contient les rubriques suivantes :

- Gérer les licences Edge pour des partenaires
- Gérer les licences Edge pour des clients
- Générer un rapport sur les licences Edge

Gérer les licences Edge pour des partenaires

Un opérateur peut gérer les licences Edge et les attribuer à des partenaires.

La procédure suivante consiste à gérer et à attribuer des licences Edge à des partenaires existants. Pour attribuer des licences Edge à de nouveaux partenaires, reportez-vous à la section Créer un partenaire.

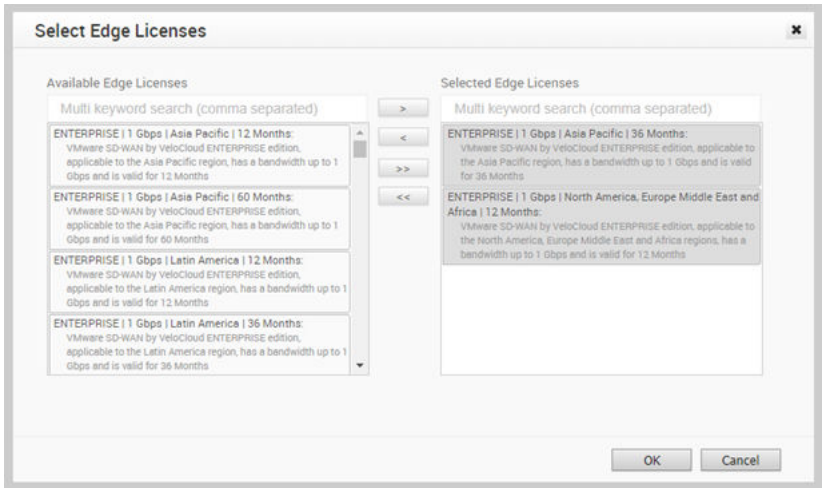
1 Dans le portail de l'opérateur, cliquez sur **Gérer les partenaires (Manage Partners)**.

2 Cliquez sur le lien vers un nom de partenaire pour accéder au portail de partenaires.

3 Dans le portail de partenaires, cliquez sur **Gestion des licences Edge (Edge Licensing)**.

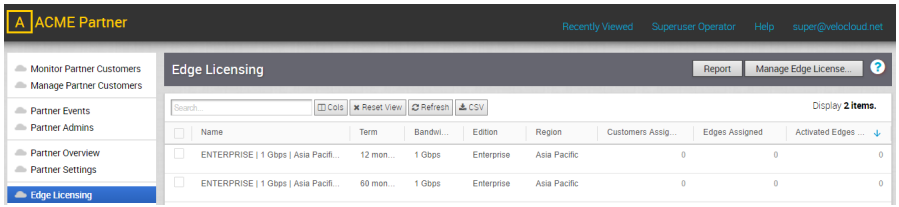
4 Cliquez sur **Gérer la licence Edge (Manage Edge License)**.

5 Dans la fenêtre **Sélectionner les licences Edge (Select Edge Licenses)**, choisissez les licences appropriées en fonction de la bande passante, de la durée, de l'édition et de la région.



6 Cliquez sur **OK**.

Les licences sélectionnées s'affichent dans la fenêtre **Gestion des licences Edge (Edge Licensing)**.

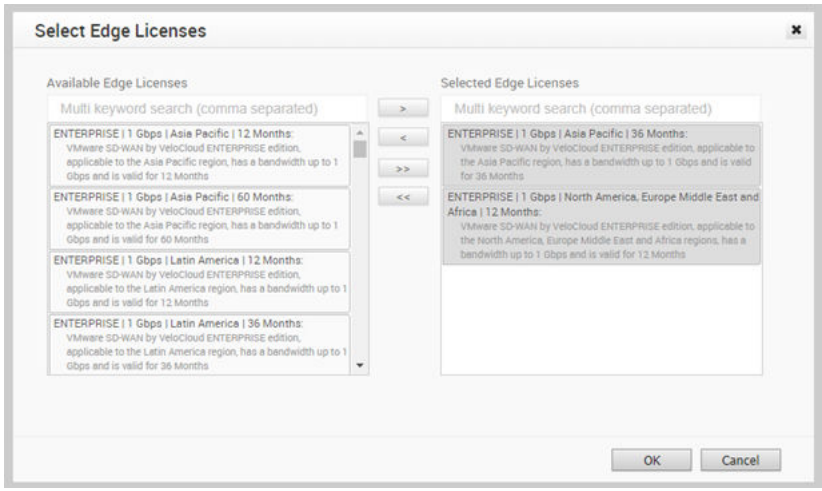


Cliquez sur **Rapport (Report)** pour générer un rapport des licences ainsi que des clients et dispositifs SD-WAN Edges associés au format CSV.

Gérer les licences Edge pour des clients

Un opérateur peut gérer les licences Edge et les attribuer à des clients.

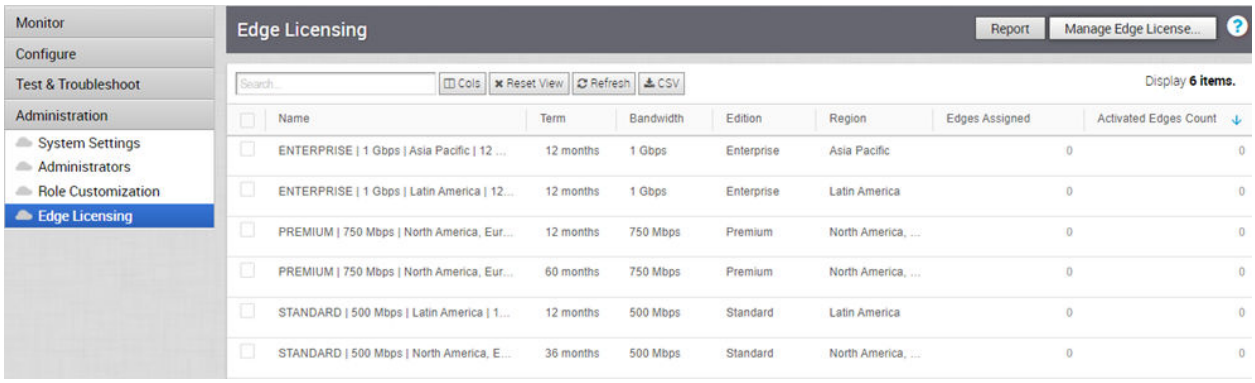
- Dans le portail de l'opérateur, cliquez sur **Gérer les clients (Manage Customers)**.
- Cliquez sur le lien vers un nom de client pour accéder au portail de l'entreprise.
- Dans le portail de l'entreprise, cliquez sur **Administration > Gestion des licences Edge (Edge Licensing)**.
- Cliquez sur **Gérer la licence Edge (Manage Edge License)**.
- Dans la fenêtre **Sélectionner les licences Edge (Select Edge Licenses)**, choisissez les licences appropriées en fonction de la bande passante, de la durée, de l'édition et de la région et déplacez-les vers le volet **Licences Edge sélectionnées (Selected Edge Licenses)**.



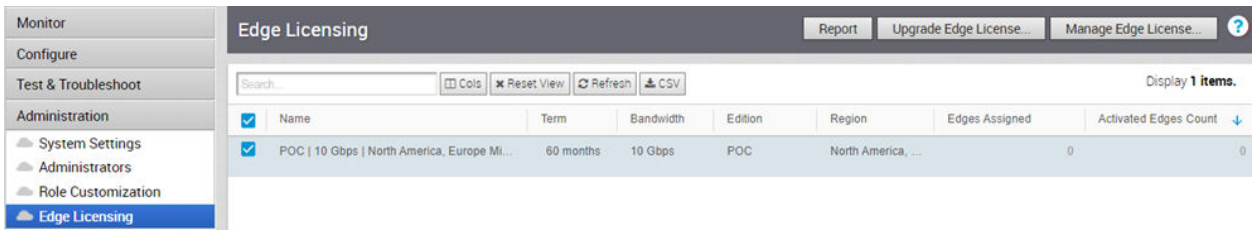
Note Outre les licences existantes, VMware propose une version d'évaluation de licence en édition **Validation technique (POC)**. Si vous sélectionnez une licence **Validation technique (POC)**, vous ne pouvez pas choisir les autres licences.

- Cliquez sur **OK**.

Les licences sélectionnées s'affichent dans la fenêtre **Gestion des licences Edge (Edge Licensing)**.



Si vous avez sélectionné la licence **Validation technique (POC)**, vous pouvez cliquer sur **Mettre à niveau la licence Edge (Upgrade Edge License)** pour passer au niveau suivant de la licence. Choisissez une édition Standard, Enterprise ou Premium dans la liste.



Note Il n'est pas possible de rétrograder un type de licence vers l'édition précédente.

Cliquez sur **Rapport (Report)** pour générer un rapport sur les licences et les dispositifs VMware SD-WAN Edges associés au format CSV.

Lorsque vous créez un dispositif SD-WAN Edge, vous pouvez choisir et attribuer une licence Edge dans la liste déroulante.

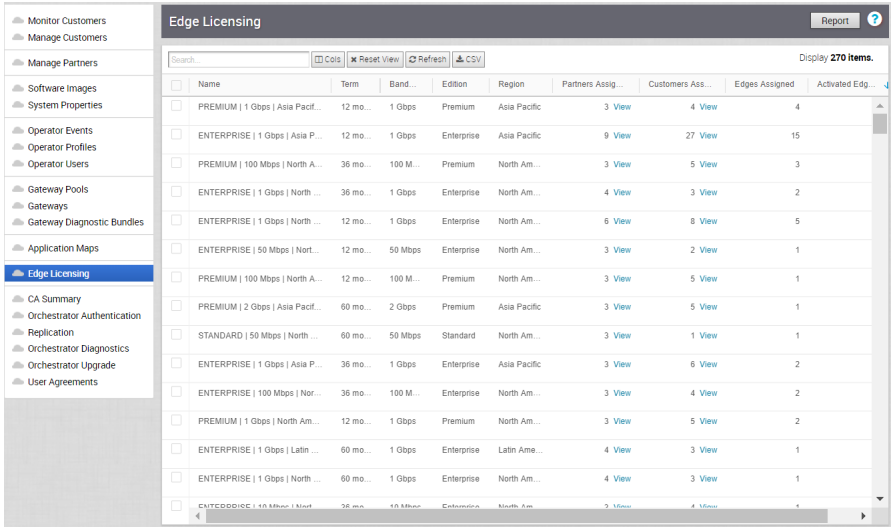
Pour attribuer une licence à un dispositif SD-WAN Edge existant :

- Dans le portail d'entreprise, cliquez sur **Configurer (Configure) > Dispositifs Edge (Edges)**.
- Pour attribuer une licence à chaque dispositif SD-WAN Edge, cliquez sur le lien vers le dispositif SD-WAN Edge et sélectionnez la licence dans la page **Présentation du dispositif Edge (Edge Overview)**. Vous pouvez également sélectionner le dispositif SD-WAN Edge et cliquer sur **Actions > Attribuer une licence Edge (Assign Edge License)** pour attribuer la licence.
- Pour attribuer une licence à plusieurs dispositifs SD-WAN Edges, sélectionnez les dispositifs SD-WAN Edges appropriés, cliquez sur **Actions > Attribuer une licence Edge (Assign Edge License)** et sélectionnez la licence.

Générer un rapport sur les licences Edge

Les super utilisateurs opérateurs, les opérateurs standard, les experts commerciaux et les opérateurs du support client peuvent générer un rapport sur les licences Edge.

Sur le portail opérateur, accédez à **Gestion des licences Edge (Edge Licensing)**.

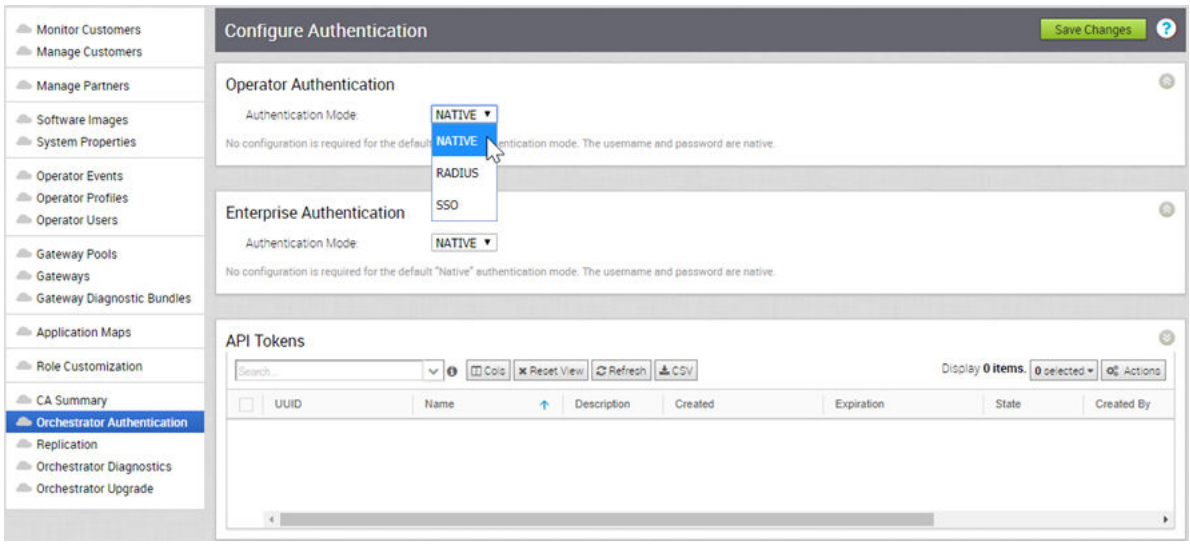


Cliquez sur **Rapport (Report)** pour générer un rapport sur les licences, les partenaires associés, les clients et les dispositifs SD-WAN Edges au format CSV.

Authentification d'Orchestrator 17

L'option Authentification d'Orchestrator (Orchestrator Authentication) vous permet de définir les modes d'authentification pour les utilisateurs d'entreprise et les opérateurs. Vous pouvez également afficher les jetons d'API existants.

Dans le portail de l'opérateur, cliquez sur **Authentification d'Orchestrator (Orchestrator Authentication)** et sélectionnez les modes d'authentification dans le menu déroulant pour les utilisateurs d'entreprise et opérateurs.



Les modes d'authentification disponibles sont les suivants : Seul un utilisateur opérateur peut activer les modes natif et RADIUS pour l'authentification d'opérateur et d'entreprise. Tout utilisateur opérateur disposant d'une autorisation de super utilisateur peut configurer et configurer le mode SSO.

- **Natif (Native)** : mode d'authentification par défaut de SD-WAN Orchestrator. Ce mode ne nécessite aucune configuration.
- **RADIUS** : RADIUS (Remote Authentication Dial-in User Service) est un protocole client-serveur qui permet aux serveurs d'accès à distance de communiquer avec un serveur central. L'authentification RADIUS fournit une gestion centralisée pour les utilisateurs. Pour plus d'informations, reportez-vous à la section Configurer l'authentification RADIUS

- **SSO** : SSO (Single Sign On) est un service d'authentification de session et d'utilisateur qui permet aux utilisateurs opérateurs de se connecter à Orchestrator avec un ensemble d'informations d'identification de connexion pour accéder à plusieurs applications. Pour plus d'informations, reportez-vous à la section Configurer l'authentification unique d'opérateur.

Jetons d'API

Vous pouvez accéder aux API Orchestrator à l'aide de l'authentification basée sur les jetons, quel que soit le mode d'authentification. Les administrateurs opérateurs disposant des autorisations appropriées peuvent afficher les jetons d'API délivrés aux utilisateurs d'Orchestrator, notamment les jetons délivrés aux utilisateurs partenaires et clients, dans cette section. Si nécessaire, un administrateur opérateur peut révoquer les jetons d'API.

Par défaut, les jetons d'API sont activés. Pour les désactiver, accédez à **Propriétés système (System Properties)** sur le portail opérateur, puis définissez la valeur de la propriété système `session.options.enableApiTokenAuth` sur **Faux (False)**.

Seul le super utilisateur opérateur ou l'utilisateur associé à un jeton d'API peut révoquer le jeton. Sélectionnez le jeton et cliquez sur **Actions > Révoquer (Revoke)**. En tant que super utilisateur d'opérateur, vous pouvez gérer les jetons d'API pour les utilisateurs d'entreprise. Pour créer et télécharger les jetons d'API, reportez-vous à la section Jetons d'API.

Ce chapitre contient les rubriques suivantes :

- Configurer l'authentification RADIUS
- Configurer l'authentification unique d'opérateur

Configurer l'authentification RADIUS

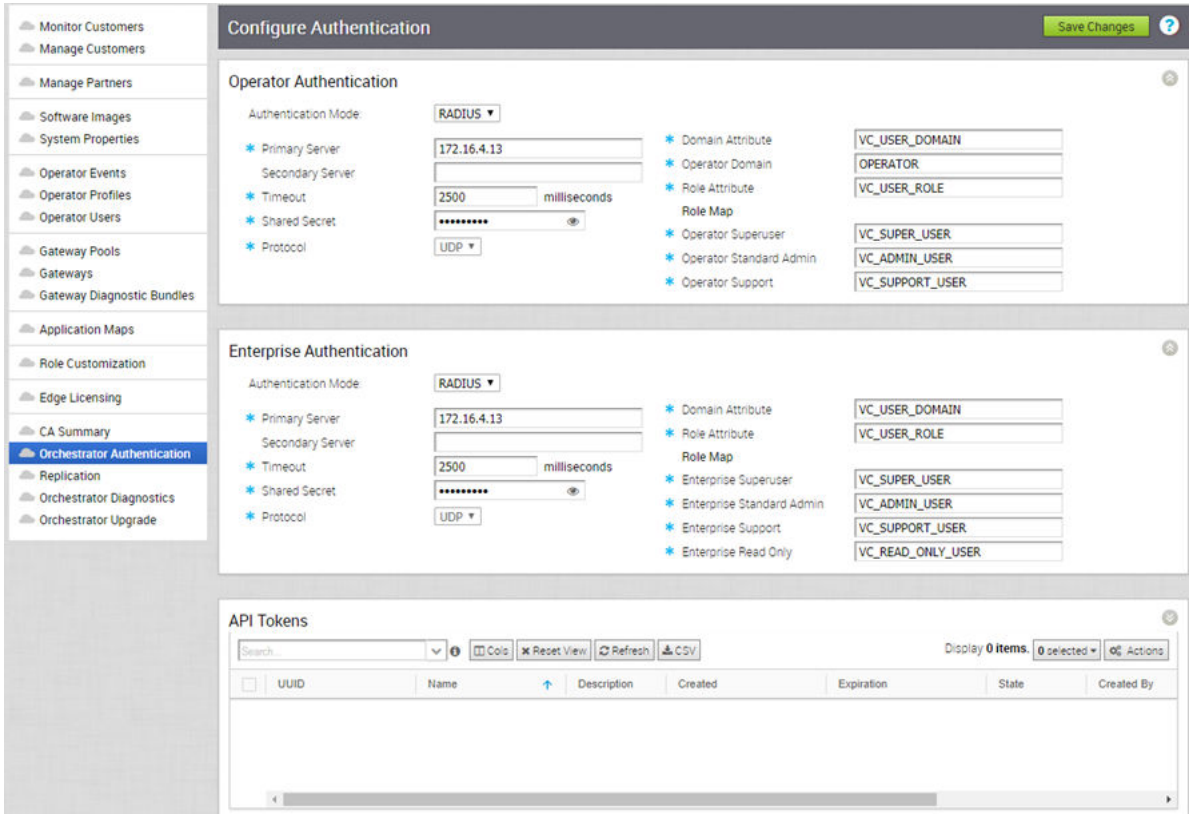
Vous pouvez configurer l'authentification Orchestrator en mode RADIUS afin que l'opérateur et les clients d'entreprise se connectent aux portails à l'aide des serveurs RADIUS.

Choisissez de déployer l'un des éléments suivants dans le mode d'authentification RADIUS :

- Serveur RADIUS unique : partagez le même serveur RADIUS entre l'opérateur et le client d'entreprise.
- Serveurs RADIUS distincts : configurez un serveur RADIUS pour l'opérateur/le fournisseur de services et un autre pour tous les clients d'entreprise.

Pour configurer le mode RADIUS, cliquez sur **Authentification d'Orchestrator (Orchestrator Authentication)** sur le portail opérateur.

Choisissez RADIUS comme **Mode d'authentification (Authentication Mode)** pour **Authentification de l'opérateur (Operator Authentication)** et **Authentification de l'entreprise (Enterprise Authentication)**. Entrez les informations appropriées.



Vous pouvez entrer ou modifier les valeurs dans les champs, à l'exception de **Protocole (Protocol)**. Vous ne pouvez modifier la valeur de protocole que dans les propriétés système. Modifiez le protocole dans les champs Valeur (Value) de `vco.operator.authentication.radius` pour l'opérateur et `vco.enterprise.authentication.radius` pour les entreprises.

Au lieu de configurer les valeurs sur la page **Configurer l'authentification (Configure Authentication)**, vous pouvez également définir les valeurs du serveur RADIUS dans les propriétés système. Sur le portail opérateur, accédez à la page **Propriétés système (System Properties)** et configurez les propriétés système suivantes :

- `vco.enterprise.authentication.mode` : entrez la valeur **RADIUS** pour activer l'authentification RADIUS des entreprises.
- `vco.enterprise.authentication.radius` : dans le champ Valeur (Value), modifiez le modèle JSON à l'aide des informations du serveur et d'autres attributs des entreprises.
- `vco.operator.authentication.mode` : entrez la valeur **RADIUS** pour activer l'authentification RADIUS des opérateurs.
- `vco.operator.authentication.radius` : dans le champ Valeur (Value), modifiez le modèle JSON à l'aide des informations du serveur et d'autres attributs des opérateurs.

Après avoir défini les propriétés système à l'aide des valeurs pertinentes, cliquez sur **Authentification d'Orchestrator (Orchestrator Authentication)**.

Le **Mode d'authentification (Authentication Mode)** passe à **RADIUS** et les champs s'affichent avec les attributs que vous avez définis dans les propriétés système.

Si nécessaire, vous pouvez modifier les valeurs dans les champs correspondants. Après la mise à jour des champs, cliquez sur **Enregistrer les modifications (Save Changes)**.

Configurer l'authentification unique d'opérateur

Le mode d'authentification unique (SSO) a été récemment ajouté à l'écran **Authentification d'Orchestrator (Orchestrator Authentication)**.

Présentation de Single Sign On

SD-WAN Orchestrator prend en charge un nouveau type d'authentification d'utilisateur appelé Single Sign On (SSO) pour tous les types d'utilisateurs Orchestrator : Opérateur, Partenaire et Entreprise.

Single Sign-On (SSO) est un service d'authentification d'utilisateur et de session qui permet aux utilisateurs SD-WAN Orchestrator de se connecter à SD-WAN Orchestrator avec un ensemble d'informations d'identification pour accéder à plusieurs applications. L'intégration du service SSO à SD-WAN Orchestrator améliore la sécurité de l'authentification des utilisateurs SD-WAN Orchestrator et permet à SD-WAN Orchestrator d'authentifier les utilisateurs à partir d'autres fournisseurs d'identité basés sur OpenID Connect (OIDC). Les fournisseurs d'identité suivants sont actuellement pris en charge :

- Okta
- OneLogin
- PingIdentity
- AzureAD
- VMwareCSP

Configurer Single Sign On pour l'utilisateur opérateur

Les utilisateurs opérateurs disposant d'une autorisation de super utilisateur peuvent installer et configurer Single Sign On (SSO) dans SD-WAN Orchestrator. Pour configurer l'authentification SSO pour l'utilisateur opérateur, suivez les étapes de cette procédure.

Pour configurer Single Sign On pour un utilisateur opérateur :

Conditions préalables

- Veillez à disposer de l'autorisation de super utilisateur opérateur.

- Avant de configurer l'authentification SSO dans SD-WAN Orchestrator, vérifiez que vous avez configuré les rôles, les utilisateurs et l'application OpenID Connect (OIDC) pour SD-WAN Orchestrator sur le site Web de votre fournisseur d'identité préféré. Pour plus d'informations, reportez-vous à la section Configurer un IDP pour l'authentification unique.

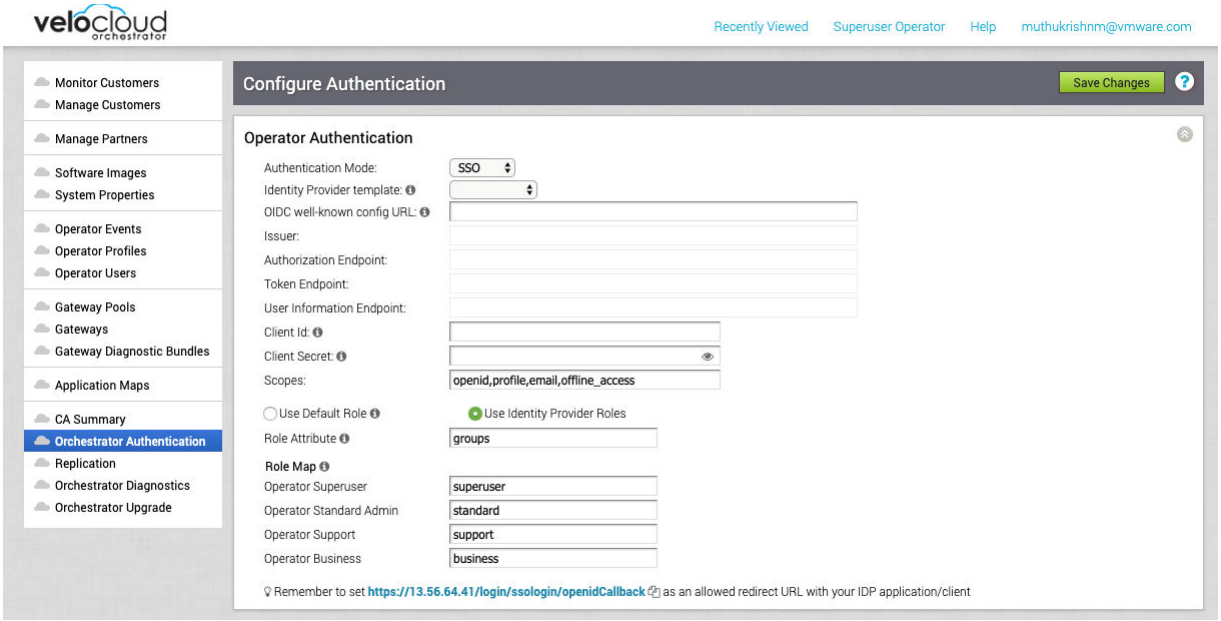
Note L'intégration SSO au niveau de la gestion des opérateurs d'une instance d'Orchestrator hébergée par VMware est réservée aux opérateurs TechOPS de VMware SD-WAN. Les partenaires disposant d'un accès au niveau de l'opérateur d'une instance d'Orchestrator hébergée n'ont pas la possibilité de s'intégrer à un service SSO.

Procédure

1 Connectez-vous à l'application SD-WAN Orchestrator en tant que super utilisateur opérateur.

2 Cliquez sur **Authentification d'Orchestrator (Orchestrator Authentication)**.

L'écran **Configurer l'authentification (Configure Authentication)** s'affiche.



3 Dans le menu déroulant **Mode d'authentification (Authentication Mode)**, sélectionnez **SSO**.

4 Dans le menu déroulant **Modèle de fournisseur d'identité (Identity Provider template)**, sélectionnez votre fournisseur d'identité (IDP) préféré que vous avez configuré pour Single Sign On.

Note Lorsque vous sélectionnez VMwareCSP comme fournisseur d'identité préféré, veillez à fournir votre ID d'organisation au format suivant : */csp/gateway/am/api/orgs/<ID d'organisation complet>.*

Lorsque vous vous connectez à la Console VMware CSP (VMware CSP console), vous pouvez afficher l'ID d'organisation avec lequel vous êtes connecté en cliquant sur votre nom d'utilisateur. Une version abrégée de l'ID s'affiche sous le nom de l'organisation. Cliquez sur l'ID pour afficher l'ID d'organisation complet.

Vous pouvez également configurer manuellement vos propres fournisseurs d'identité en sélectionnant **Autres (Others)** dans le menu déroulant **Modèle de fournisseur d'identité (Identity Provider template)**.

5 Dans la zone de texte **URL de configuration connue d'OIDC (OIDC well-known config URL)**, entrez l'URL de configuration OpenID Connect (OIDC) pour votre fournisseur d'identité. Par exemple, le format d'URL pour Okta est le suivant : `https://{oauth-provider-url}/.well-known/openid-configuration`

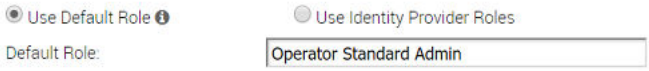
6 L'application SD-WAN Orchestrator renseigne automatiquement les informations du point de terminaison, par exemple l'émetteur, le point de terminaison d'autorisation, le point de terminaison de jeton et le point de terminaison d'informations utilisateur de votre fournisseur d'identité.

7 Dans la zone de texte **ID de client (Client Id)**, entrez l'identifiant du client fourni par votre fournisseur d'identité.

8 Dans la zone de texte **Clé secrète client (Client Secret)**, entrez le code secret client fourni par votre fournisseur d'identité, qui est utilisé par le client pour échanger un code d'autorisation pour un jeton.

9 Pour déterminer le rôle de l'utilisateur dans SD-WAN Orchestrator, sélectionnez l'une des options suivantes :

- **Utiliser le rôle par défaut (Use Default Role)** : permet à l'utilisateur de configurer un rôle statique par défaut à l'aide de la zone de texte **Rôle par défaut (Default Role)** qui s'affiche en sélectionnant cette option. Les rôles pris en charge sont les suivants : Super utilisateur opérateur, Administrateur opérateur standard, Support opérateur et Activité opérateur.



Note Dans une configuration SSO, si l'option **Utiliser le rôle par défaut (Use Default Role)** est sélectionnée et qu'un rôle d'utilisateur par défaut est défini, ce rôle par défaut est attribué à tous les utilisateurs SSO. Plutôt que d'attribuer le rôle par défaut à un utilisateur, un super utilisateur opérateur peut préenregistrer un utilisateur spécifique en tant qu'utilisateur non natif et définir un rôle d'utilisateur spécifique à l'aide de l'onglet **Utilisateurs opérateurs (Operator Users)**. Pour connaître les étapes de configuration d'un nouvel utilisateur opérateur, reportez-vous à la section Créer un utilisateur opérateur.

- **Utiliser les rôles de fournisseur d'identité (Use Identity Provider Roles)** : utilise les rôles configurés dans le fournisseur d'identité.

10 Lorsque vous sélectionnez l'option **Utiliser les rôles de fournisseur d'identité (Use Identity Provider Roles)**, dans la zone de texte **Attribut de rôle (Role Attribute)**, entrez le nom de l'attribut défini dans le fournisseur d'identité pour renvoyer les rôles.

11 Dans la zone **Mappage de rôle (Role Map)**, mappez les rôles fournis par le fournisseur d'identité à chacun des rôles de SD-WAN Orchestrator, séparés par des virgules.

Les rôles de VMware CSP suivent le format suivant : *external/<uuid de définition de service>/<nom de rôle de service mentionné lors de la création du modèle de service>.*

12 Mettez à jour les URL de redirection autorisées sur le site Web du fournisseur OIDC avec URL de SD-WAN Orchestrator (`https://<vco>/login/ssologin/openidCallback`).

13 Pour enregistrer la configuration SSO, cliquez sur **Enregistrer les modifications (Save Changes)**.

14 Cliquez sur **Tester la configuration (Test Configuration)** pour valider la configuration OpenID Connect (OIDC) spécifiée.

L'utilisateur accède au site Web du fournisseur d'identité et est autorisé à entrer les informations d'identification. Lors de la vérification du fournisseur d'identité et de la redirection réussie vers le rappel de test de SD-WAN Orchestrator, un message de validation réussi s'affiche.

Résultats

La configuration de l'authentification SSO est terminée dans SD-WAN Orchestrator.

Étape suivante

Chapitre 6 Se connecter à l'instance de SD-WAN Orchestrator à l'aide de SSO en tant qu'utilisateur opérateur

Configurer un IDP pour l'authentification unique

Pour activer l'authentification unique (Single Sign On, SSO) pour SD-WAN Orchestrator, vous devez configurer un partenaire d'identité (IDP) avec les détails de SD-WAN Orchestrator. Actuellement, les IDP suivants sont pris en charge : Okta, OneLogin, PingIdentity, AzureAD et VMware CSP.

Pour obtenir des instructions pas à pas de configuration d'une application OpenID Connect (OIDC) pour SD-WAN Orchestrator dans différents IDP, reportez-vous aux sections suivantes :

- Configurer Okta pour l'authentification unique
- Configurer OneLogin pour l'authentification unique
- Configurer PingIdentity pour l'authentification unique
- Configurer Azure Active Directory pour l'authentification unique
- Configurer VMware CSP pour l'authentification unique

Configurer Okta pour l'authentification unique

Pour prendre en charge l'authentification unique (SSO, Single Sign On) basée sur OpenID Connect (OIDC) à partir d'Okta, vous devez d'abord configurer une application dans Okta. Pour configurer une application basée sur OIDC dans Okta pour SSO, suivez les étapes de cette procédure.

Conditions préalables

Assurez-vous de disposer d'un compte Okta pour vous connecter.

Procédure

1 Connectez-vous à votre compte Okta en tant qu'utilisateur admin.

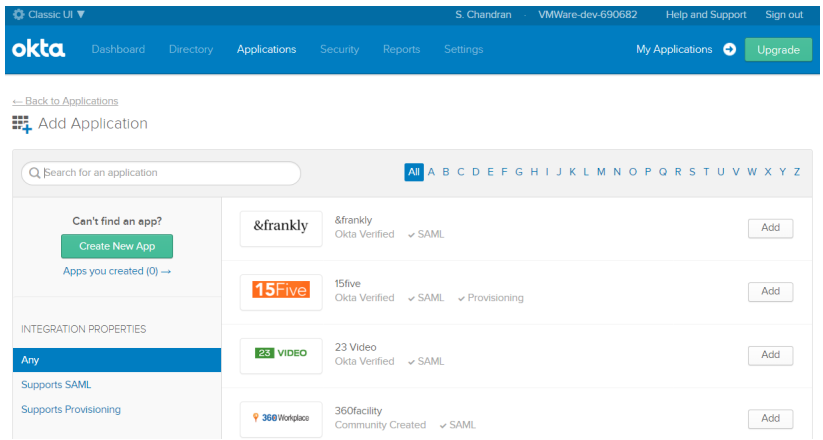
L'écran d'accueil **Okta** s'affiche.

Note Si vous vous trouvez dans la vue de la console pour les développeurs, vous devez basculer vers la vue de l'interface utilisateur classique en sélectionnant **Interface utilisateur classique (Classic UI)** dans la liste déroulante **Console pour les développeurs (Developer Console)**.

2 Pour créer une application :

a Dans la barre de navigation supérieure, cliquez sur **Applications** > **Ajouter une application (Add Application)**.

L'écran **Ajouter une application (Add Application)** s'affiche.



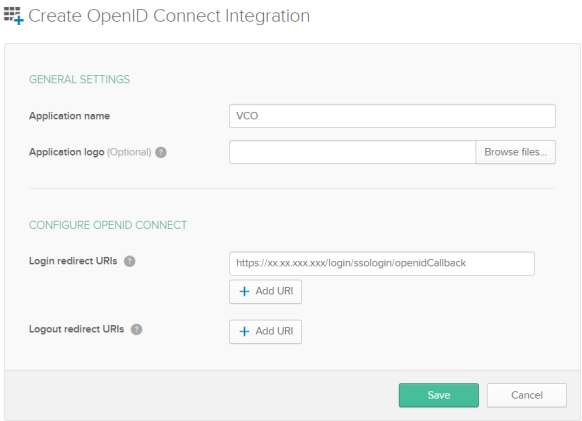
b Cliquez sur **Créer une application (Create New App)**.

La boîte de dialogue **Créer une intégration d'application (Create a New Application Integration)** s'affiche.

c Dans le menu déroulant **Plate-forme (Platform)**, sélectionnez **Web**.

d Sélectionnez **OpenID Connect** comme méthode de connexion, puis cliquez sur **Créer (Create)**.

L'écran **Créer une intégration OpenID Connect (Create OpenID Connect Integration)** s'affiche.



e Sous la zone **Paramètres généraux (General Settings)**, dans la zone de texte **Nom de l'application (Application name)**, entrez le nom de votre application.

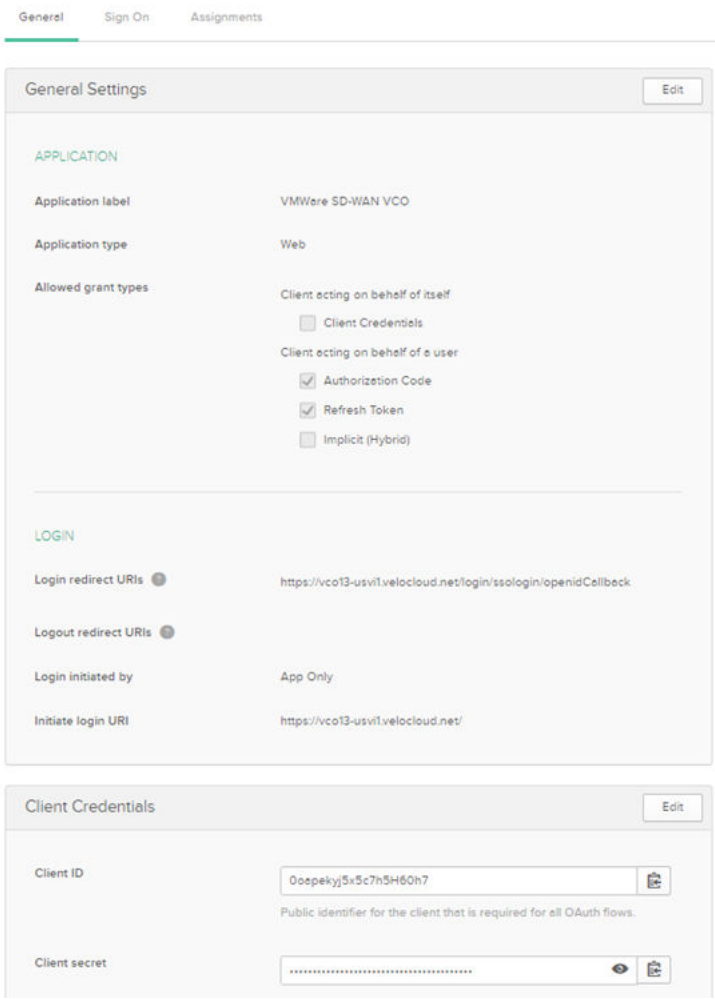
f Sous la zone de texte **CONFIGURE OPENID CONNECT**, dans la zone de texte **URI de direction de connexion (Login redirect URIs)**, entrez l'URL de redirection que votre application SD-WAN Orchestrator utilise comme point de terminaison de rappel.

Dans l'application SD-WAN Orchestrator, en bas de l'écran **Configurer l'authentification (Configure Authentication)**, vous trouverez le lien d'URL de direction. Idéalement, l'URL de direction de SD-WAN Orchestrator est au format suivant : https://<Orchestrator URL>/login/ssologin/openidCallback.

g Cliquez sur **Enregistrer (Save)**. La page de l'application qui vient d'être créée s'affiche.

h Dans l'onglet **Général (General)**, cliquez sur **Modifier (Edit)** et sélectionnez **Actualiser le jeton (Refresh Token)** pour les types d'autorisations autorisés, puis cliquez sur **Enregistrer (Save)**.

Notez les informations d'identification de client (ID de client et clé secrète de client) qui seront utilisées lors de la configuration SSO dans SD-WAN Orchestrator.



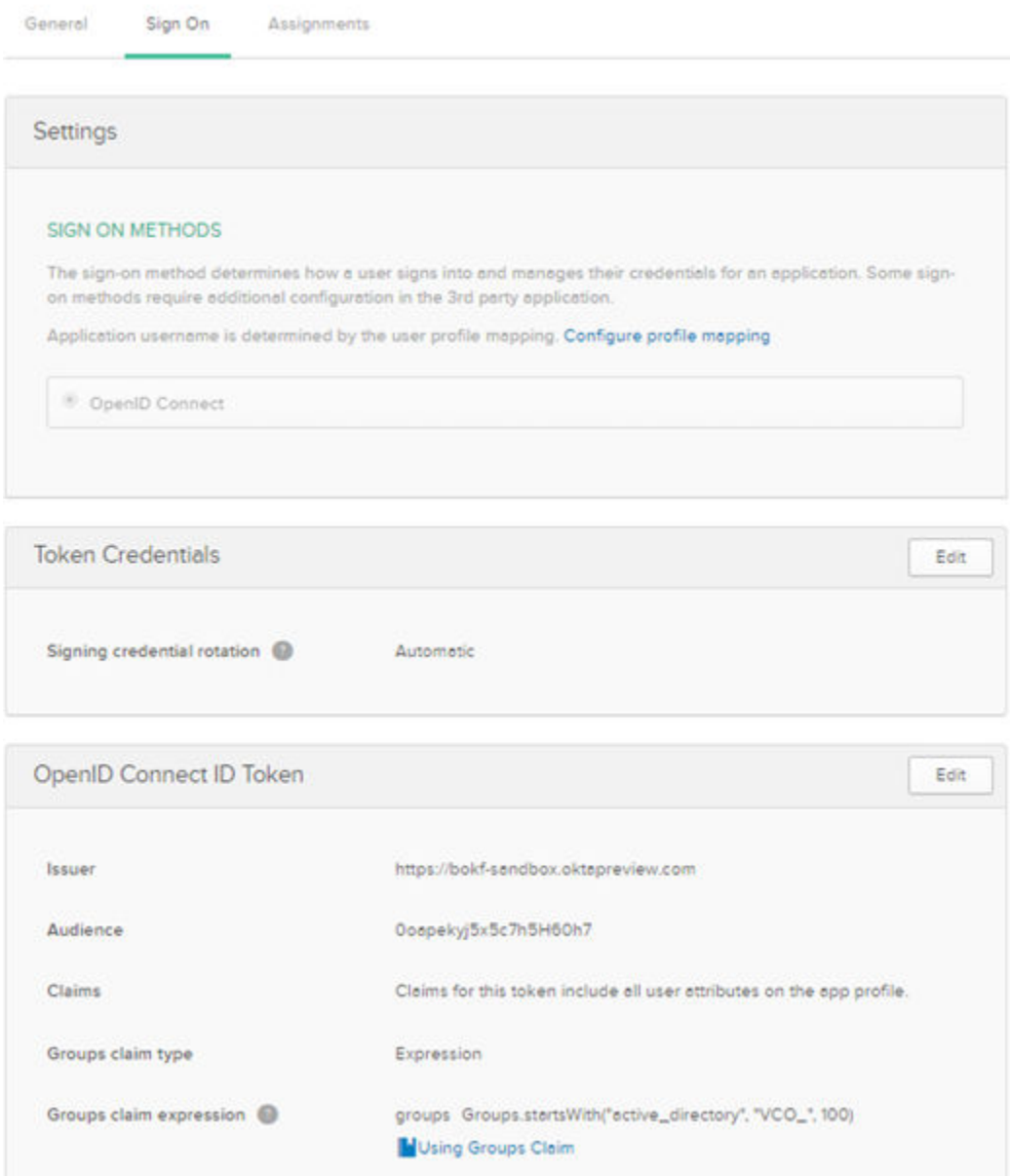
i Cliquez sur l'onglet **Connexion (Sign On)** et, dans la zone **Jeton d'identificateur OpenID Connect (OpenID Connect ID Token)**, cliquez sur **Modifier (Edit)**.

j Dans le menu déroulant **Type de réclamation des groupes (Groups claim type)**, sélectionnez **Expression**. Par défaut, le type de réclamation des groupes est défini sur **Filtre (Filter)**.

k Dans la zone de texte **Expression de réclamation des groupes (Groups claim expression)**, entrez le nom de la réclamation qui sera utilisée dans le jeton et une instruction d'expression d'entrée Okta qui évalue le jeton.

l Cliquez sur **Enregistrer (Save)**.

L'application est configurée dans l'IDP. Vous pouvez attribuer des groupes d'utilisateurs et des utilisateurs à votre application SD-WAN Orchestrator.



3 Pour attribuer des groupes et des utilisateurs à votre application SD-WAN Orchestrator :

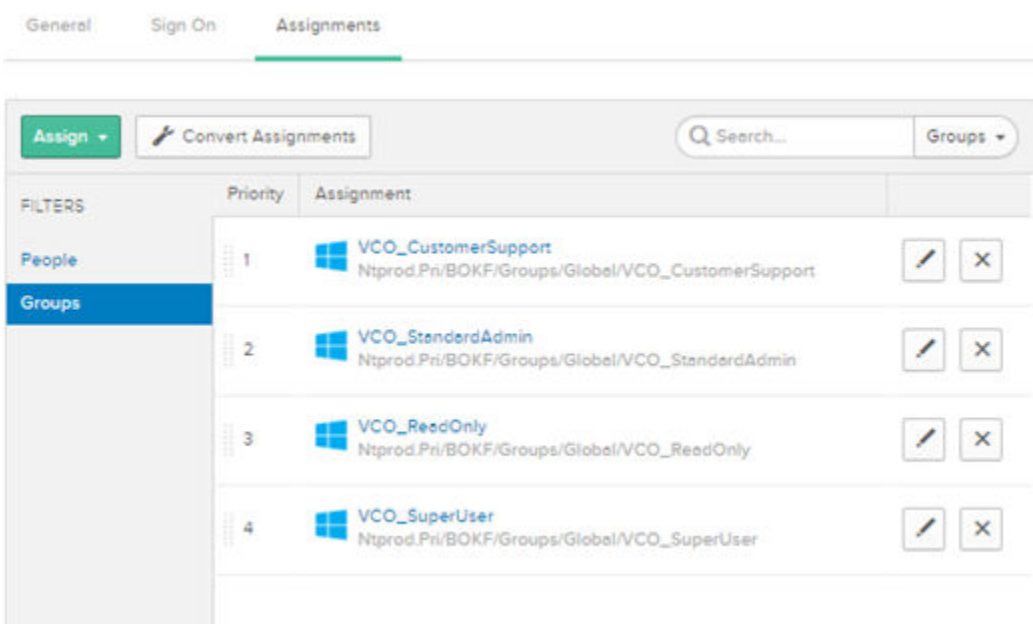
a Accédez à **Application** > **Applications** et cliquez sur le lien de votre application SD-WAN Orchestrator.

b Dans l'onglet **Attributions (Assignments)**, dans le menu déroulant **Attribuer (Assign)**, sélectionnez **Attribuer à des groupes (Assign to Groups)** ou **Attribuer à des personnes (Assign to People)**.

La boîte de dialogue **Attribuer <Application Name> à des groupes (Assign <Application Name> to Groups)** ou **Attribuer <Application Name> à des personnes (Assign <Application Name> to People)** s'affiche.

c Cliquez sur **Attribuer (Assign)** en regard des groupes d'utilisateurs ou des utilisateurs disponibles auxquels vous souhaitez attribuer l'application SD-WAN Orchestrator, puis cliquez sur **Terminé (Done)**.

Les utilisateurs ou les groupes d'utilisateurs attribués à l'application SD-WAN Orchestrator seront affichés.



Résultats

Vous avez terminé la configuration d'une application basée sur OIDC dans Okta pour SSO.

Étape suivante

Configurez l'authentification unique dans SD-WAN Orchestrator.

Créer un groupe d'utilisateurs dans Okta

Pour créer un groupe d'utilisateurs, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Annuaire (Directory)** > **Groupes (Groups)**.

2 Cliquez sur **Ajouter un groupe (Add Group)**.

La boîte de dialogue **Ajouter un groupe (Add Group)** s'affiche.

3 Entrez le nom et la description du groupe, puis cliquez sur **Enregistrer (Save)**.

Créer un utilisateur dans Okta

Pour ajouter un nouvel utilisateur, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Annuaire (Directory)** > **People**.

2 Cliquez sur **Ajouter une personne (Add Person)**.

La boîte de dialogue **Ajouter une personne (Add Person)** s'affiche.

3 Entrez toutes les informations obligatoires, telles que le prénom, le nom de famille et l'ID d'e-mail de l'utilisateur.

4 Pour définir le mot de passe, sélectionnez **Définir par utilisateur (Set by user)** dans le menu déroulant **Mot de passe (Password)** et activez **Envoyer l'e-mail d'activation de l'utilisateur maintenant (Send user activation email now)**.

5 Cliquez sur **Enregistrer (Save)**.

Un e-mail de lien d'activation sera envoyé à votre ID d'e-mail. Cliquez sur le lien de l'e-mail pour activer votre compte d'utilisateur Okta.

Configurer OneLogin pour l'authentification unique

Pour configurer une application basée sur OpenID Connect (OIDC) dans OneLogin pour l'authentification unique (SSO, Single Sign-On), suivez les étapes de cette procédure.

Conditions préalables

Assurez-vous de disposer d'un compte OneLogin pour vous connecter.

Procédure

1 Connectez-vous à votre compte OneLogin en tant qu'utilisateur admin.

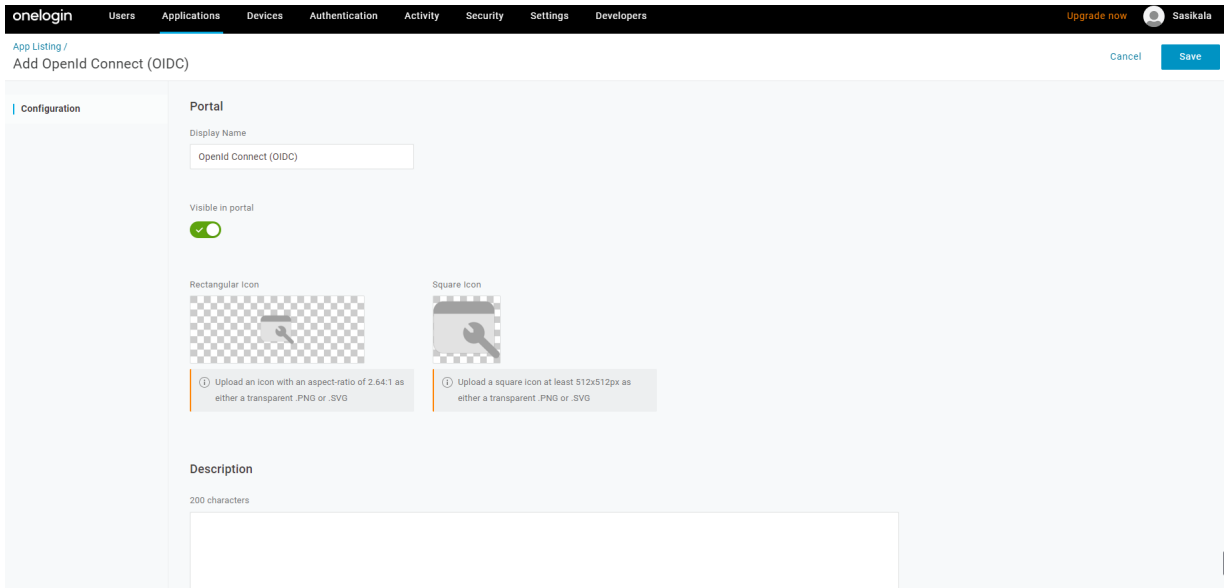
L'écran d'accueil **OneLogin** s'affiche.

2 Pour créer une application :

a Dans la barre de navigation supérieure, cliquez sur **Applications (Apps)** > **Ajouter des applications (Add Apps)**.

b Dans la zone de texte **Rechercher des applications (Find Applications)**, recherchez « OpenId Connect » ou « OIDC », puis sélectionnez l'application **OpenId Connect (OIDC)**.

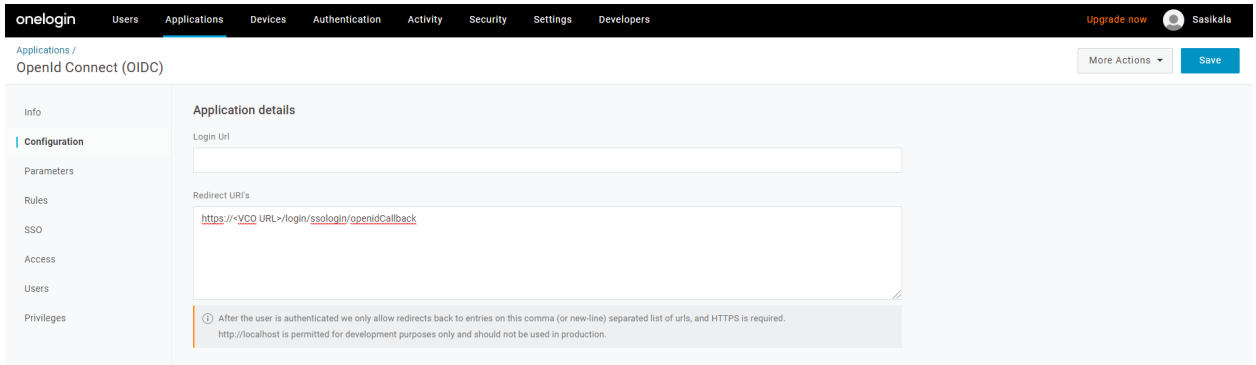
L'écran **Ajouter OpenId Connect (OIDC)** [**Add OpenId Connect (OIDC)**] s'affiche.



c Dans la zone de texte **Nom d'affichage (Display Name)**, entrez le nom de votre application et cliquez sur **Enregistrer (Save)**.

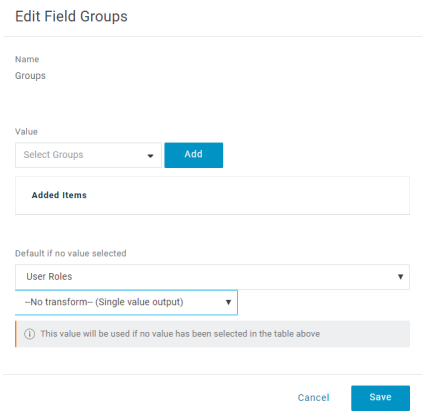
d Dans l'onglet **Configuration**, entrez l'URI de direction que SD-WAN Orchestrator utilise comme point de terminaison de rappel et cliquez sur **Enregistrer (Save)**.

Dans l'application SD-WAN Orchestrator, au bas de l'écran **Authentification (Authentication)**, se trouve le lien d'URL de direction. Idéalement, l'URL de direction de SD-WAN Orchestrator est au format suivant : https://<Orchestrator URL>/login/ssologin/openidCallback.



e Dans l'onglet **Paramètres (Parameters)**, sous **OpenId Connect (OIDC)**, double-cliquez sur **Groupes (Groups)**.

La fenêtre contextuelle **Modifier les groupes de champs (Edit Field Groups)** s'affiche.

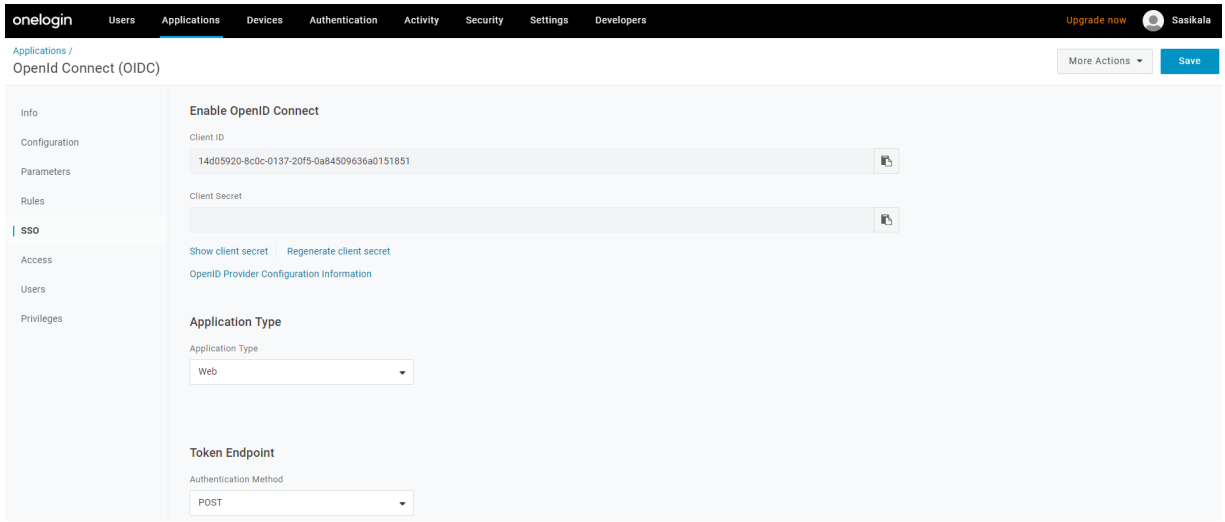


f Configurez les rôles d'utilisateur avec la valeur « --Aucune transformation--(Sortie à valeur unique) [No transform--(Single value output)] » à envoyer dans l'attribut groupes (groups), puis cliquez sur **Enregistrer (Save)**.

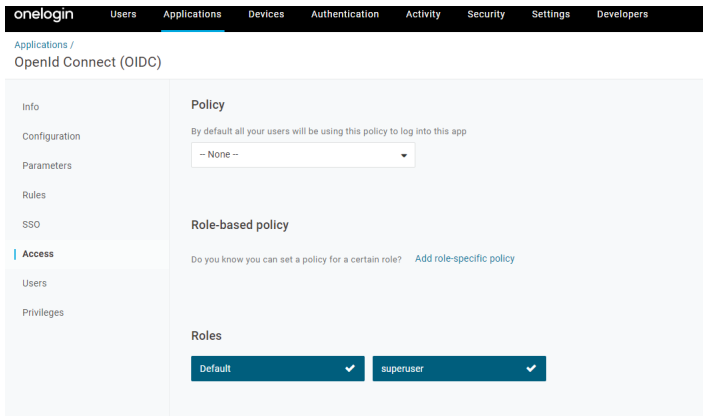
g Dans l'onglet **SSO**, dans le menu déroulant **Type d'application (Application Type)**, sélectionnez **Web**.

h Dans le menu déroulant **Méthode d'authentification (Authentication Method)**, sélectionnez **POST** comme point de terminaison du jeton, puis cliquez sur **Enregistrer (Save)**.

Notez également les informations d'identification client (ID de client et clé secrète de client) à utiliser lors de la configuration SSO dans SD-WAN Orchestrator.



i Dans l'onglet **Accès (Access)**, choisissez les rôles qui seront autorisés à se connecter, puis cliquez sur **Enregistrer (Save)**.



3 Pour ajouter des rôles et des utilisateurs à votre application SD-WAN Orchestrator :

a Cliquez sur **Utilisateurs (Users)** > **Utilisateurs (Users)** et sélectionnez un utilisateur.

b Dans l'onglet **Application**, dans le menu déroulant **Rôles (Roles)**, sur la gauche, sélectionnez un rôle à mapper à l'utilisateur.

c Cliquez sur **Enregistrer les utilisateurs (Save Users)**.

Résultats

Vous avez terminé la configuration d'une application basée sur OIDC dans OneLogin pour SSO.

Étape suivante

Configurez l'authentification unique dans SD-WAN Orchestrator.

Créer un rôle dans OneLogin

Pour créer un rôle, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Utilisateurs (Users)** > **Rôles (Roles)**.

2 Cliquez sur **Nouveau rôle (New Role)**.

3 Entrez un nom pour le rôle.

Lorsque vous configurez un rôle pour la première fois, l'onglet **Applications** affiche toutes les applications dans le catalogue de votre entreprise.

4 Cliquez sur une application pour la sélectionner, puis cliquez sur **Enregistrer (Save)** pour ajouter les applications sélectionnées au rôle.

Créer un utilisateur dans OneLogin

Pour créer un utilisateur, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Utilisateurs (Users)** > **Utilisateurs (Users)** > **Nouvel utilisateur (New User)**.

L'écran **Nouvel utilisateur (New User)** s'affiche.

2 Entrez toutes les informations obligatoires, telles que le prénom, le nom de famille et l'ID d'e-mail de l'utilisateur, puis cliquez sur **Enregistrer l'utilisateur (Save User)**.

Configurer PingIdentity pour l'authentification unique

Pour configurer une application basée sur OpenID Connect (OIDC) dans PingIdentity pour l'authentification unique (SSO, Single Sign-On), suivez les étapes de cette procédure.

Conditions préalables

Assurez-vous de disposer d'un compte PingOne pour vous connecter.

Note Actuellement, SD-WAN Orchestrator prend en charge PingOne en tant que partenaire d'identité (IDP). Cependant, tous les produits PingIdentity prenant en charge OIDC peuvent être facilement configurés.

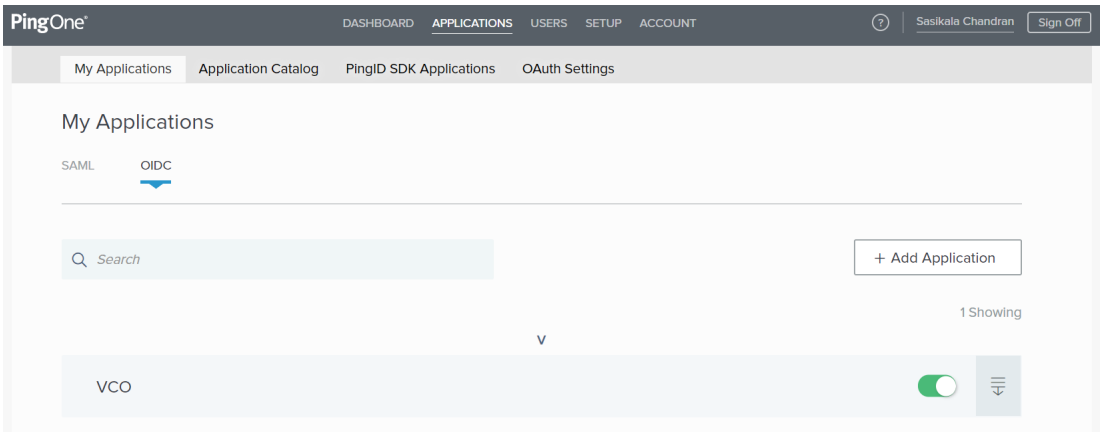
Procédure

1 Connectez-vous à votre compte PingOne en tant qu'utilisateur admin.

L'écran d'accueil **PingOne** s'affiche.

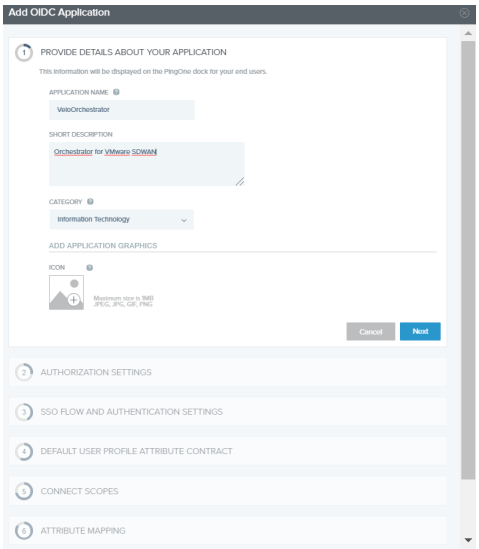
2 Pour créer une application :

a Dans la barre de navigation supérieure, cliquez sur **Applications**.



b Dans l'onglet **Mes applications (My Applications)**, sélectionnez **OIDC**, puis cliquez sur **Ajouter une application (Add Application)**.

La fenêtre contextuelle **Ajouter une application OIDC (Add OIDC Application)** s'affiche.



c Fournissez des détails de base tels que le nom, une description courte et la catégorie de l'application, puis cliquez sur **Suivant (Next)**.

d Sous **AUTHORIZATION SETTINGS**, sélectionnez **Code d'autorisation (Authorization Code)** comme types d'attributions autorisés et cliquez sur **Suivant (Next)**.

Notez également l'URL de découverte et les informations d'identification de client (ID de client et clé secrète de client) à utiliser lors de la configuration SSO dans SD-WAN Orchestrator.

e Sous **SSO FLOW AND AUTHENTICATION SETTINGS**, fournissez des valeurs valides pour l'URL de démarrage SSO (Start SSO URL) et l'URL de redirection (Redirect URL), puis cliquez sur **Suivant (Next)**.

Dans l'application SD-WAN Orchestrator, en bas de l'écran **Configurer l'authentification (Configure Authentication)**, vous trouverez le lien d'URL de direction. Idéalement, l'URL de direction de SD-WAN Orchestrator est au format suivant : https://<Orchestrator URL>/login/ssologin/openidCallback. L'URL de démarrage SSO est au format suivant : https://<vco>/<domain name>/login/doEnterpriseSsoLogin.

f Sous **DEFAULT USER PROFILE ATTRIBUTE CONTRACT**, cliquez sur **Ajouter un attribut (Add Attribute)** pour ajouter des attributs de profil d'utilisateur supplémentaires.

g Dans la zone de texte **Nom d'attribut (Attribute Name)**, entrez *group_membership*, puis cochez la case **Required (Requis)** et sélectionnez **Suivant (Next)**.

Note L'attribut *group_membership* est requis pour récupérer des rôles à partir de PingOne.

h Sous **CONNECT SCOPES**, sélectionnez les étendues qui peuvent être demandées pour votre application SD-WAN Orchestrator pendant l'authentification, puis cliquez sur **Suivant (Next)**.

i Sous **Mappage d'attributs (Attribute Mapping)**, mappez vos attributs de référentiel d'identités aux réclamations disponibles pour votre application SD-WAN Orchestrator.

Note Les mappages minimaux requis pour que l'intégration fonctionne sont email, given_name, family_name, phone_number, sub et group_membership (mappés à memberOf).

j Sous **Accès des groupes (Group Access)**, sélectionnez tous les groupes d'utilisateurs qui doivent avoir accès à votre application SD-WAN Orchestrator, puis cliquez sur **Terminé (Done)**.

L'application est ajoutée à votre compte et elle sera disponible sur l'écran **Mon application (My Application)**.

Résultats

Vous avez terminé la configuration d'une application basée sur OIDC dans PingOne pour SSO.

Étape suivante

Configurez l'authentification unique dans SD-WAN Orchestrator.

Créer un groupe d'utilisateurs dans PingIdentity

Pour créer un groupe d'utilisateurs, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Utilisateurs (Users)** > **Annuaire d'utilisateurs (User Directory)**.

2 Dans l'onglet **Groupes (Groups)**, cliquez sur **Ajouter un groupe (Add Group)**

L'écran **Nouveau groupe (New Group)** s'affiche.

3 Dans la zone de texte **Nom (Name)**, entrez un nom pour le groupe et cliquez sur **Enregistrer (Save)**.

Créer un utilisateur dans PingIdentity

Pour ajouter un nouvel utilisateur, suivez les étapes de cette procédure.

Procédure

1 Cliquez sur **Utilisateurs (Users)** > **Annuaire d'utilisateurs (User Directory)**.

2 Dans l'onglet **Utilisateurs (Users)**, cliquez sur le menu déroulant **Ajouter des utilisateurs (Add Users)**, puis sélectionnez **Créer un utilisateur (Create New User)**.

L'écran **Utilisateur (User)** s'affiche.

3 Entrez toutes les informations obligatoires, telles que le nom d'utilisateur, le mot de passe et l'ID d'e-mail de l'utilisateur.

4 Sous **Appartenances au groupe (Group Memberships)**, cliquez sur **Ajouter (Add)**.

La fenêtre contextuelle **Ajouter une appartenance au groupe (Add Group Membership)** s'affiche.

5 Recherchez et ajoutez l'utilisateur à un groupe, puis cliquez sur **Enregistrer (Save)**.

Configurer Azure Active Directory pour l'authentification unique

Pour configurer une application basée sur OpenID Connect (OIDC) dans Microsoft Azure Active Directory (AzureAD) pour l'authentification unique (Single Sign On, SSO), suivez les étapes de cette procédure.

Conditions préalables

Assurez-vous de disposer d'un compte AzureAD pour vous connecter.

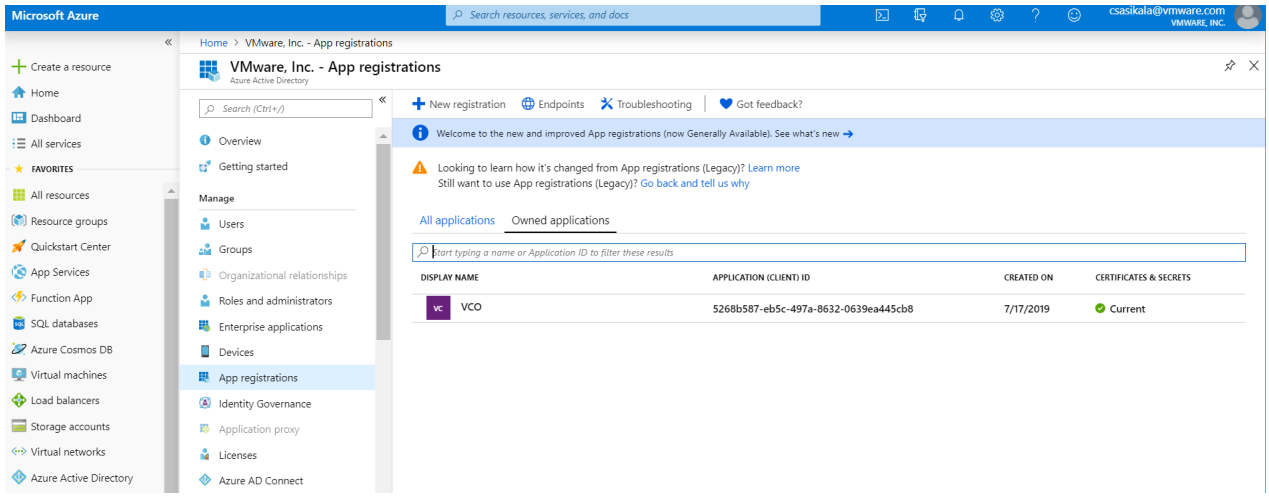
Procédure

1 Connectez-vous à votre compte Microsoft Azure en tant qu'utilisateur admin.

L'écran d'accueil **Microsoft Azure** s'affiche.

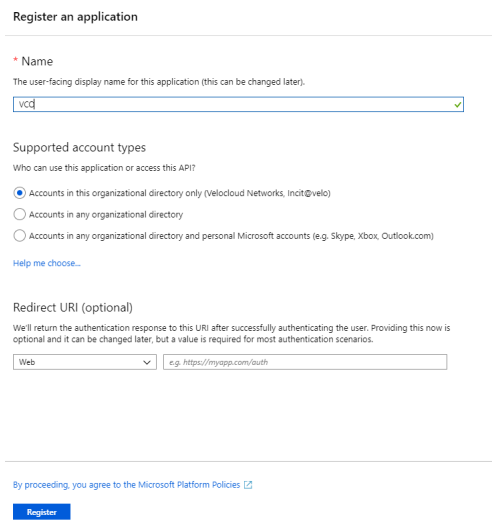
2 Pour créer une application :

a Recherchez le service **Azure Active Directory** et sélectionnez-le.



b Accédez à **Inscription d'application (App registration)** > **Nouvelle inscription (New registration)**.

L'écran **Inscrire une application (Register an application)** s'affiche.



c Dans le champ **Nom (Name)**, entrez le nom de votre application SD-WAN Orchestrator.

d Dans le champ **URL de direction (Redirect URL)**, entrez l'URL de direction que votre application SD-WAN Orchestrator utilise comme point de terminaison de rappel.

Dans l'application SD-WAN Orchestrator, en bas de l'écran **Configurer l'authentification (Configure Authentication)**, vous trouverez le lien d'URL de direction. Idéalement, l'URL de direction de SD-WAN Orchestrator est au format suivant : https://<Orchestrator URL>/login/ssologin/openidCallback.

e Cliquez sur **Inscrire (Register)**.

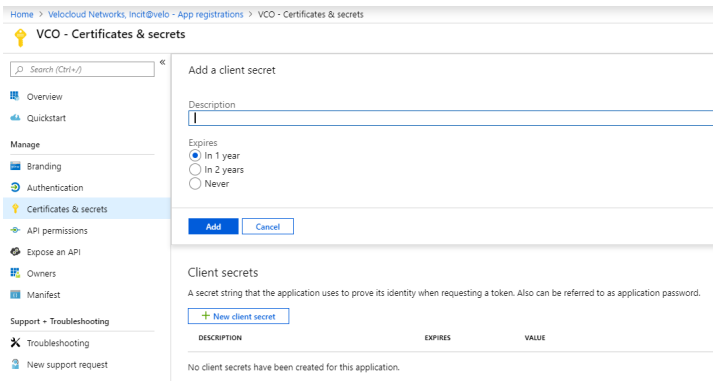
Votre application SD-WAN Orchestrator sera inscrite et affichée dans les onglets **Toutes les applications (All applications)** et **Applications détenues (Owned applications)**. Assurez-vous de noter l'ID de client/l'ID de l'application à utiliser lors de la configuration de l'authentification unique dans SD-WAN Orchestrator.

f Cliquez sur **Points de terminaison (Endpoints)** et copiez l'URL de configuration connue d'OIDC à utiliser lors de la configuration de l'authentification unique dans SD-WAN Orchestrator.

g Pour créer une clé secrète de client pour votre application SD-WAN Orchestrator, dans l'onglet **Applications détenues (Owned applications)**, cliquez sur votre application SD-WAN Orchestrator.

h Accédez à **Certificats et secrets (Certificates & secrets)** > **Nouvelle clé secrète de client (New client secret)**.

L'écran **Ajouter une clé secrète de client (Add a client secret)** s'affiche.

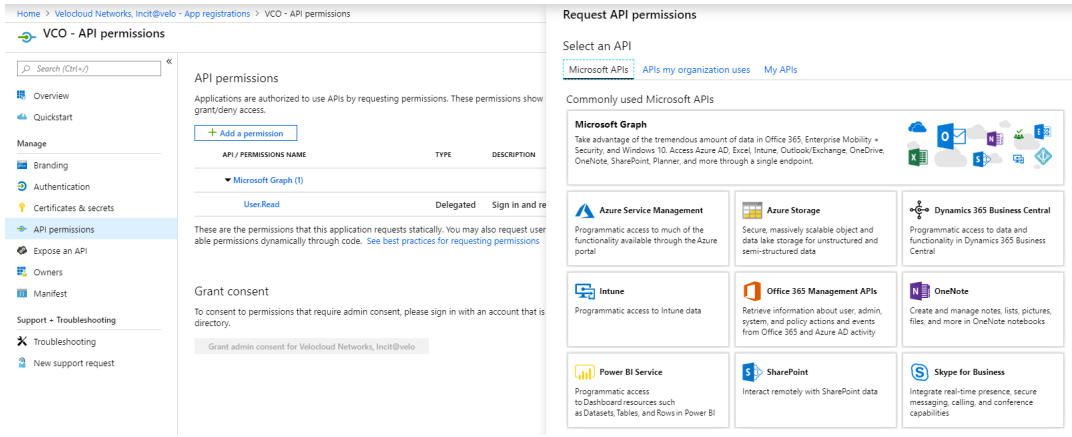


i Fournissez des détails tels que la description et la valeur d'expiration de la clé secrète, puis cliquez sur **Ajouter (Add)**.

La clé secrète de client sera créée pour l'application. Notez la nouvelle valeur de la clé secrète de client à utiliser lors de la configuration de l'authentification unique dans SD-WAN Orchestrator.

j Pour configurer les autorisations de votre application SD-WAN Orchestrator, cliquez sur l'application SD-WAN Orchestrator et accédez à **Autorisations d'API (API permissions)** > **Ajouter une autorisation (Add a permission)**.

L'écran **Demander des autorisations d'API (Request API permissions)** s'affiche.



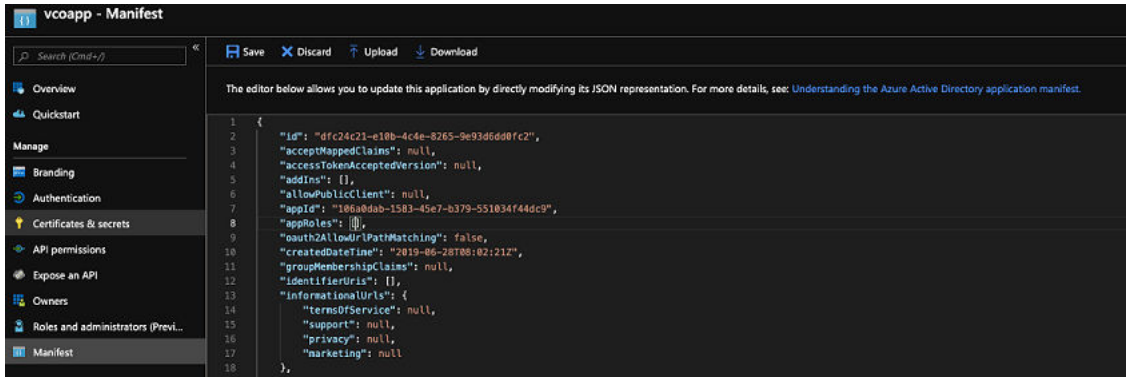
k Cliquez sur **Microsoft Graph** et sélectionnez **Autorisations d'application (Application permissions)** comme type d'autorisation pour votre application.

l Sous **Sélectionner les autorisations (Select permissions)**, dans le menu déroulant **Annuaire (Directory)**, sélectionnez **Directory.Read.All** et dans le menu déroulant **Utilisateur (User)**, sélectionnez **User.Read.All**.

m Cliquez sur **Ajouter des autorisations (Add permissions)**.

- Pour ajouter et enregistrer des rôles dans le manifeste, cliquez sur votre application SD-WAN Orchestrator et, dans l'écran **Présentation (Overview)** de l'application, cliquez sur **Manifeste (Manifest)**.

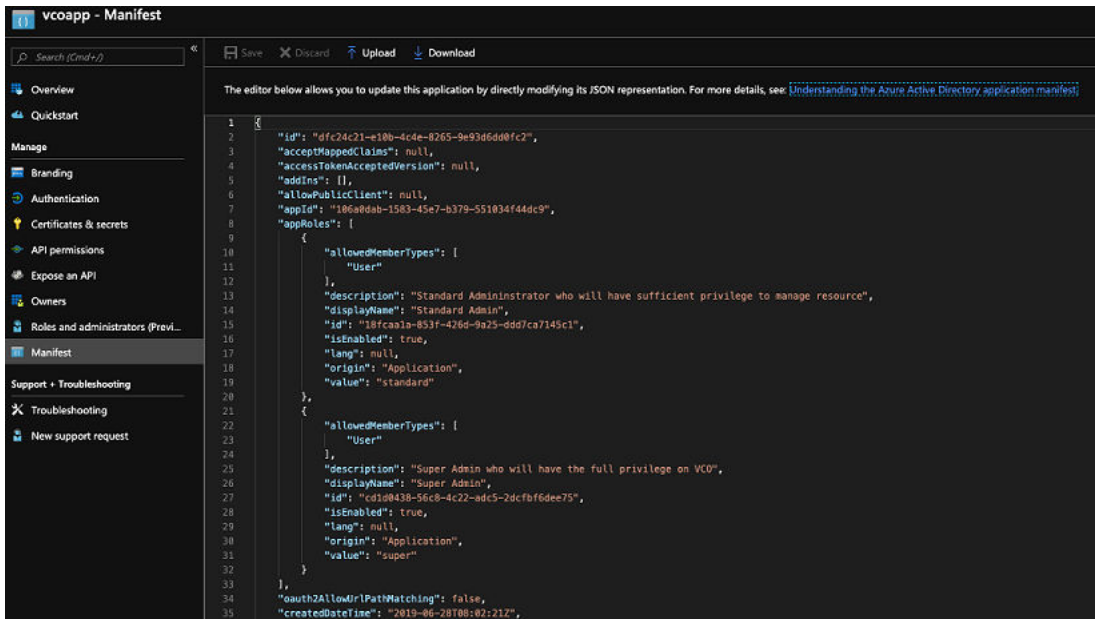
  Un éditeur de manifeste Web s'ouvre, ce qui vous permet de modifier le manifeste dans le portail. Vous pouvez également sélectionner **Télécharger (Download)** pour modifier le manifeste localement, puis utiliser **Charger (Upload)** pour le réappliquer à votre application.



- Dans le manifeste, recherchez le groupe `appRoles`, ajoutez un ou plusieurs objets de rôle comme indiqué dans l'exemple suivant, puis cliquez sur **Enregistrer (Save)**.

  Exemples d'objets de rôle

```
{
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Standard Administrator who will have sufficient privilege
to manage resource",
            "displayName": "Standard Admin",
            "id": "18fcaa1a-853f-426d-9a25-ddd7ca7145c1",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "standard"
        },
        {
            "allowedMemberTypes": [
                "User"
            ],
            "description": "Super Admin who will have the full privilege on SD-WAN
Orchestrator",
            "displayName": "Super Admin",
            "id": "cd1d0438-56c8-4c22-adc5-2dcfbf6dee75",
            "isEnabled": true,
            "lang": null,
            "origin": "Application",
            "value": "superuser"
        }
```



Note Assurez-vous de définir `id` sur une valeur de GUID nouvellement générée.

3 Pour attribuer des groupes et des utilisateurs à votre application SD-WAN Orchestrator :

a Accédez à **Azure Active Directory** > **Applications d'entreprise (Enterprise applications)**.

b Recherchez votre application SD-WAN Orchestrator et sélectionnez-la.

c Cliquez sur **Utilisateurs et groupes (Users and groups)** et attribuez des utilisateurs et des groupes à l'application.

d Cliquez sur **Envoyer (Submit)**.

Résultats

Vous avez terminé la configuration d'une application basée sur OIDC dans AzureAD pour SSO.

Étape suivante

Configurez l'authentification unique dans SD-WAN Orchestrator.

Créer un utilisateur invité dans AzureAD

Pour créer un utilisateur invité, suivez les étapes de cette procédure.

Procédure

1 Accédez à **Azure Active Directory** > **Utilisateurs (Users)** > **Tous les utilisateurs (All users)**.

2 Cliquez sur **Nouvel utilisateur invité (New guest user)**.

La fenêtre contextuelle **Nouvel utilisateur invité (New guest user)** s'affiche.

3 Dans la zone de texte **Adresse e-mail (Email address)**, entrez l'adresse e-mail de l'utilisateur invité, puis cliquez sur **Inviter (Invite)**.

   L'utilisateur invité reçoit immédiatement une invitation personnalisable qui lui permet de se connecter à son panneau d'accès.

4 Les utilisateurs invités dans l'annuaire peuvent être attribués à des applications ou à des groupes.

Configurer VMware CSP pour l'authentification unique

Pour configurer VMware Cloud Services Platform (CSP) pour l'authentification unique (SSO, Single Sign On), suivez les étapes de cette procédure.

Conditions préalables

Connectez-vous à la console VMware CSP [VMware CSP console] (environnement de transfert ou de production) à l'aide de votre ID de compte VMware. Si vous êtes un nouvel utilisateur de VMware Cloud et que vous ne disposez pas encore d'un compte VMware, vous pouvez en créer un au fur et à mesure de votre inscription. Pour plus d'informations, reportez-vous à la section sur les modalités d'inscription à VMware CSP dans la documentation Utilisation de VMware Cloud.

Procédure

1 Contactez le fournisseur de prise en charge VMware pour recevoir un lien d'URL pour l'invitation de service afin d'inscrire votre application SD-WAN Orchestrator sur VMware CSP. Pour savoir comment contacter le fournisseur de prise en charge, reportez-vous aux pages https://kb.vmware.com/s/article/53907 et https://www.vmware.com/support/contacts/us_support.html.

   Le fournisseur de prise en charge VMware crée et partage les éléments suivants :

   - une URL d'invitation de service qui doit être récupérée dans votre organisation cliente ;
   - un UUID de définition de service et un nom de rôle de service à utiliser pour le mappage de rôle dans Orchestrator.

2 Récupérez cette URL pour votre organisation client existante ou créez une organisation client en suivant les étapes de l'écran de l'interface utilisateur.

   Vous devez être propriétaire de l'organisation pour récupérer l'URL d'invitation de service dans votre organisation cliente existante.

3 Après la récupération de l'invitation de service, lors de la connexion à la console VMware CSP (VMware CSP console), vous voyez votre vignette d'application sous la section **Mes services (My Services)** sur la page **VMware Cloud Services**.

   L'organisation à laquelle vous êtes connecté s'affiche sous votre nom d'utilisateur dans la barre de menus. Notez l'ID de l'organisation en cliquant sur votre nom d'utilisateur. Vous l'utiliserez lors de la configuration d'Orchestrator. Une version abrégée de l'ID s'affiche sous le nom de l'organisation. Cliquez sur l'ID pour afficher l'ID d'organisation complet.

4 Connectez-vous à la console VMware CSP et créez une application OAuth. Pour connaître les étapes, reportez-vous à la section Utiliser OAuth 2.0 pour les applications Web. Veillez à définir l'URI de redirection sur l'URL affichée dans l'écran **Configurer l'authentification (Configure Authentication)** d'Orchestrator.

   Une fois que l'application OAuth est créée dans la console VMware CSP, notez les détails de l'intégration IDP, tels que l'ID de client et la clé secrète client. Ces détails seront nécessaires à la configuration SSO dans Orchestrator.

5 Connectez-vous à votre application SD-WAN Orchestrator en tant que super utilisateur admin et configurez SSO en utilisant les détails de l'intégration IDP de la façon suivante.

   a Cliquez sur **Administration** > **Paramètres système (System Settings)**.

      L'écran **Paramètres système (System Settings)** s'affiche.

   b Cliquez sur l'onglet **Informations générales (General Information)** et, dans la zone de texte **Domaine (Domain)**, entrez le nom de domaine de votre entreprise, s'il n'est pas déjà défini.

      Note Pour activer l'authentification unique pour SD-WAN Orchestrator, vous devez configurer le nom de domaine de votre entreprise.

   c Cliquez sur l'onglet **Authentification (Authentication)** et, dans le menu déroulant **Mode d'authentification (Authentication Mode)**, sélectionnez **SSO**.

   d Dans le menu déroulant **Modèle de fournisseur d'identité (Identity Provider template)**, sélectionnez **VMwareCSP**.

   e Dans la zone de texte **ID de l'organisation (Organization Id)**, entrez l'ID de l'organisation (que vous avez noté à l'étape 3) au format suivant : */csp/gateway/am/api/orgs/<full organization ID>*.

   f Dans la zone de texte **URL de configuration connue d'OIDC (OIDC well-known config URL)**, entrez l'URL de configuration OpenID Connect (OIDC) (https://console.cloud.vmware.com/csp/gateway/am/api/.well-known/openid-configuration) pour votre IDP.

      L'application SD-WAN Orchestrator renseigne automatiquement les informations du point de terminaison, par exemple l'émetteur, le point de terminaison d'autorisation, le point de terminaison de jeton et le point de terminaison d'informations utilisateur de votre fournisseur d'identité.

   g Dans la zone de texte **ID de client (Client Id)**, entrez l'ID de client que vous avez noté à l'étape de création de l'application OAuth.

   h Dans la zone de texte **Clé secrète client (Client Secret)**, entrez le code secret client que vous avez noté à l'étape de création de l'application OAuth.

   i Pour déterminer le rôle de l'utilisateur dans SD-WAN Orchestrator, sélectionnez **Utiliser le rôle par défaut (Use Default Role)** ou **Utiliser les rôles de fournisseur d'identité (Use Identity Provider Roles)**.

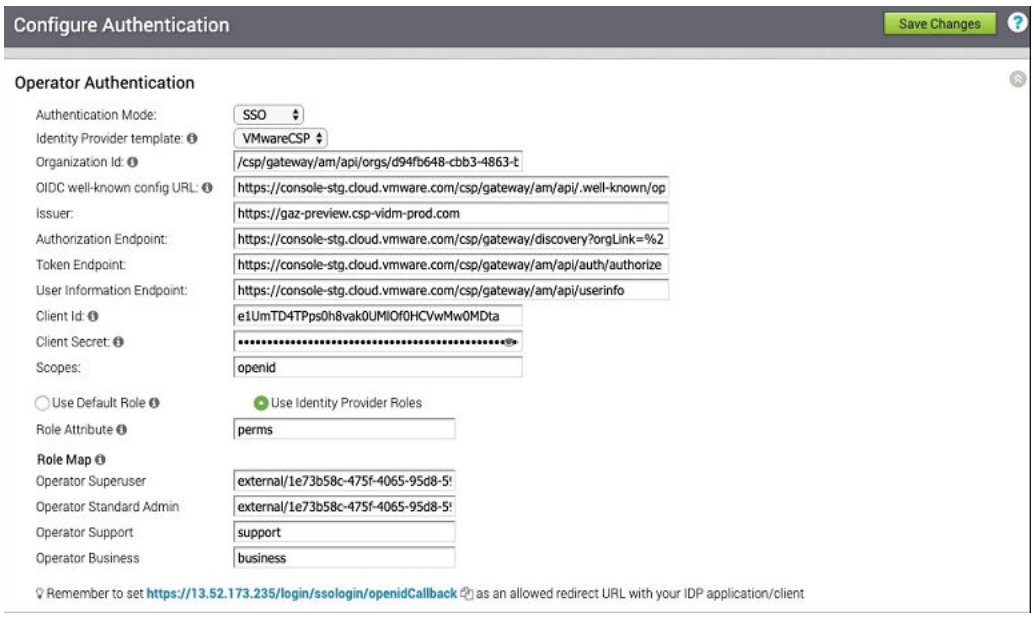
j Lorsque vous sélectionnez l'option **Utiliser les rôles de fournisseur d'identité (Use Identity Provider Roles)**, dans la zone de texte **Attribut de rôle (Role Attribute)**, entrez le nom de l'attribut défini dans VMware CSP pour renvoyer les rôles.

k Dans la zone **Mappage de rôle (Role Map)**, mappez les rôles fournis par VMwareCSP à chacun des rôles SD-WAN Orchestrator, séparés par des virgules.

Les rôles dans VMware CSP sont au format suivant : external/<service definition uuid>/ <service role name mentioned during service template creation>. Utilisez le même UUID de définition de service et nom de rôle de service que ceux que vous avez reçus de votre fournisseur de prise en charge.

6 Pour enregistrer la configuration SSO, cliquez sur **Enregistrer les modifications (Save Changes)**.

7 Cliquez sur **Tester la configuration (Test Configuration)** pour valider la configuration OpenID Connect (OIDC) entrée.



L'utilisateur accède au site Web de VMware CSP et est autorisé à entrer les informations d'identification. Lors de la vérification du fournisseur d'identité et de la redirection réussie vers le rappel de test SD-WAN Orchestrator, un message signalant la réussite de la validation s'affiche.

Résultats

Vous avez terminé l'intégration de l'application SD-WAN Orchestrator dans VMware CSP pour SSO et vous pouvez accéder à l'application SD-WAN Orchestrator en vous connectant à la console VMware CSP.

Étape suivante

- Au sein de l'organisation, gérez les utilisateurs en ajoutant les nouveaux utilisateurs et en attribuant le rôle approprié aux utilisateurs. Pour plus d'informations, reportez-vous à la section *Gestion des identités et des accès* de la documentation Utilisation de VMware Cloud.

Mettre à niveau SD-WAN Orchestrator à l'aide du déploiement de la récupération d'urgence

18

Cette section décrit comment mettre à niveau SD-WAN Orchestrator avec le déploiement de la récupération d'urgence (DR).

Ce chapitre contient les rubriques suivantes :

Présentation de la mise à niveau de SD-WAN Orchestrator

Les étapes suivantes sont requises pour mettre à niveau une instance de SD-WAN Orchestrator.

Pour plus d'informations sur la récupération d'urgence de SD-WAN Orchestrator, reportez-vous aux sections Configurer DR dans l'instance de VMware et Mettre à niveau la configuration DR.

1 Étape 1 : Préparation de la mise à niveau d'Orchestrator

2 Étape 2 : Envoi de l'annonce de mise à niveau

3 Étape 3 : Mise à niveau d'Orchestrator

4 Étape 4 : Fin de la mise à niveau d'Orchestrator

Mettre à niveau une instance d'Orchestrator

Cette section décrit comment mettre à niveau une instance d'Orchestrator.

Étape 1 : Préparation de la mise à niveau d'Orchestrator

Contactez l'équipe du support VMware pour préparer la mise à niveau d'Orchestrator, comme indiqué dans cette section.

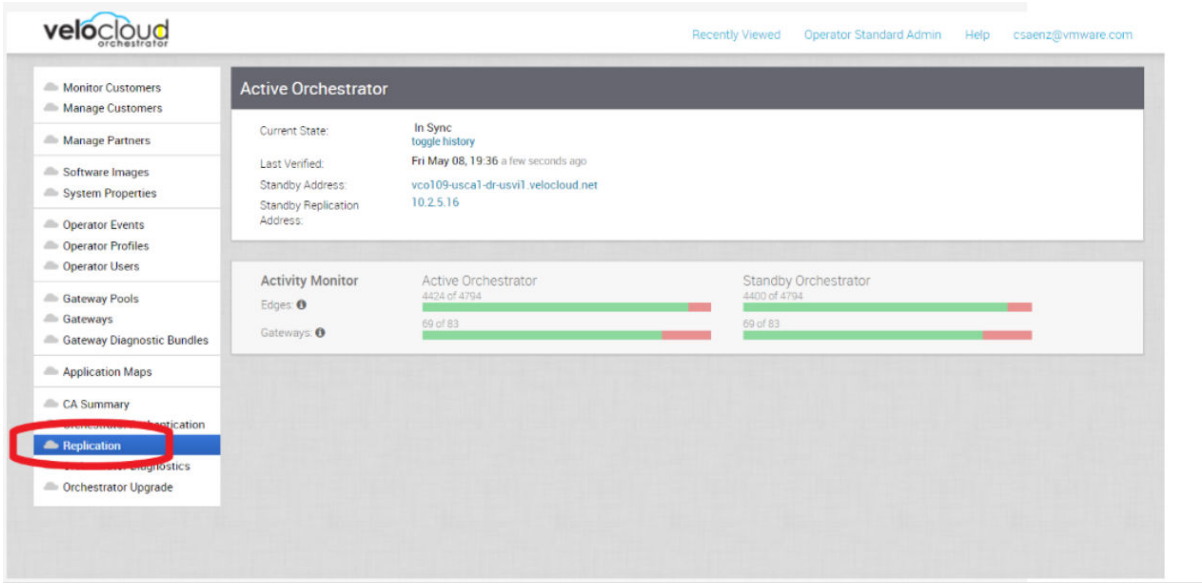
Pour mettre à niveau SD-WAN Orchestrator :

1 Le support VMware vous aidera à effectuer votre mise à niveau. Collectez les informations suivantes avant de contacter le support.

- Fournissez les versions actuelle et cible d'Orchestrator, par exemple : version actuelle (c'est-à-dire 2.5.2 GA-20180430), version cible (3.3.2 p2).

  Note Pour la version actuelle, ces informations sont disponibles dans le coin supérieur droit d'Orchestrator en cliquant sur le lien **Aide (Help)** et en choisissant **À propos (About)**.

- Fournissez une capture d'écran du tableau de bord de réplication d'Orchestrator, comme indiqué ci-dessous.



- Type et version de l'hyperviseur (c'est-à-dire, vSphere 6.7)
- Commandes disponibles depuis Orchestrator :

  Note Les commandes doivent être exécutées en tant qu'utilisateur racine (par exemple « sudo <command> » ou « sudo -i »).

  - Exécutez le script /opt/vc/scripts/vco_upgrade_check.sh pour vérifier les éléments suivants :
    - Disposition de LVM
    - Informations sur la mémoire
    - Informations sur le CPU
    - Paramètres du noyau
    - Certaines propriétés système
    - Configurations SSH
    - Tailles du schéma et de la base de données MySQL

        - Emplacements et tailles de File_store
    - Copie de /var/log
        - tar -czf /store/log-`date +%Y%M%S`.tar.gz --newer-mtime="36 hours ago" /var/log
    - À partir de l'instance d'Orchestrator en veille :
        - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW SLAVE STATUS \G'
- À partir de l'instance active d'Orchestrator :
    - sudo mysql --defaults-extra-file=/etc/mysql/velocloud.cnf velocloud -e 'SHOW MASTER STATUS \G'

2 Contactez le support VMware à l'adresse https://kb.vmware.com/s/article/53907 en vous munissant des informations susmentionnées pour obtenir de l'aide pour la mise à niveau d'Orchestrator.

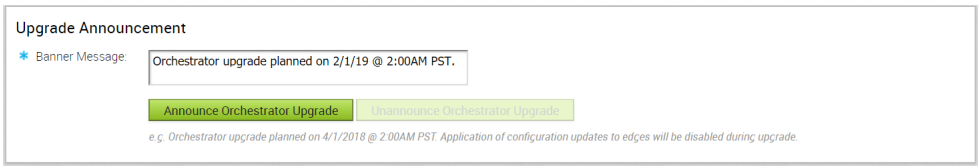
Étape 2 : Envoi de l'annonce de mise à niveau

La zone **Annonce de mise à niveau (Upgrade Announcement)** vous permet de configurer et d'envoyer un message concernant une mise à niveau à venir. Ce message s'affichera à tous les utilisateurs la prochaine fois qu'ils se connecteront à SD-WAN Orchestrator.

Pour envoyer une annonce de mise à niveau :

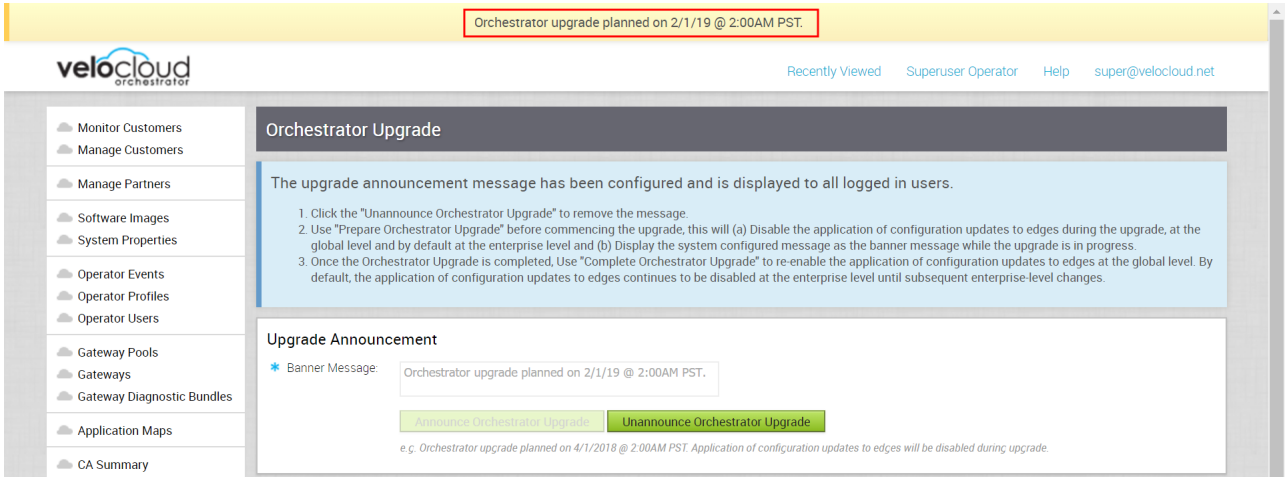
1 Dans SD-WAN Orchestrator, sélectionnez **Mettre à niveau Orchestrator (Orchestrator Upgrade)** dans le panneau de navigation.

2 Dans la section **Annonce de mise à niveau (Upgrade Announcement)**, saisissez votre message dans la zone de texte **Message de bannière (Banner Message)**.



3 Cliquez sur le bouton **Annoncer la mise à niveau d'Orchestrator (Announce Orchestrator Upgrade)**.

Un message contextuel s'affiche, indiquant que l'annonce a été correctement créée et que le message de bannière s'affiche en haut de SD-WAN Orchestrator.



4 (Facultatif) Vous pouvez supprimer l'annonce de SD-WAN Orchestrator en cliquant sur le bouton **Supprimer l'annonce de mise à niveau d'Orchestrator (Unannounce Orchestrator Upgrade)**. Un message contextuel s'affiche, indiquant que l'annonce de la mise à niveau d'Orchestrator a été correctement supprimée. L'annonce qui était affichée en haut de SD-WAN Orchestrator sera supprimée.

Étape 3 : Mise à niveau d'Orchestrator

Contactez le support VMware à l'adresse `https://kb.vmware.com/s/article/53907` pour obtenir de l'aide pour la mise à niveau d'Orchestrator.

Étape 4 : Fin de la mise à niveau d'Orchestrator

Une fois que vous avez terminé la mise à niveau d'Orchestrator, cliquez sur le bouton **Terminer la mise à niveau d'Orchestrator (Complete Orchestrator Upgrade)**. Cela permet de réactiver l'application des mises à jour de configuration des dispositifs Edge au niveau global.

Pour vérifier que la mise à niveau est terminée, exécutez la commande suivante pour afficher le numéro de version correct de tous les modules :

```
dpkg -l|grep vco
```

Lorsque vous êtes connecté en tant qu'opérateur, le même numéro de version doit s'afficher dans le coin inférieur droit de SD-WAN Orchestrator.

Récupération d'urgence de SD-WAN Orchestrator

Cette section décrit comment configurer et mettre à niveau la récupération d'urgence dans SD-WAN Orchestrator.

Configurer DR dans l'instance de VMware

Pour configurer la récupération d'urgence (DR) dans l'instance de SD-WAN Orchestrator :

1 Installez une nouvelle instance de SD-WAN Orchestrator dont la version correspond à la version de VMware qui est actuellement l'instance de SD-WAN Orchestrator active.

2 Définissez les propriétés suivantes dans l'instance de SD-WAN Orchestrator active et en veille, si nécessaire.

- `vco.disasterRecovery.transientErrorToleranceSecs` à une valeur différente de zéro (la valeur par défaut est de 900 secondes dans les versions 3.3 et ultérieures, zéro dans les versions précédentes). Cela empêche toute erreur passagère résultant d'une mise à jour du plan de gestion du dispositif Edge/de la passerelle.
- `vco.disasterRecovery.mysqlExpireLogsDays` (la valeur par défaut est de 1 jour). Il s'agit de la durée pendant laquelle l'instance de SD-WAN Orchestrator active conserve les données binlog de MySQL.

3 Configurez la propriété `network.public.address` dans les instances Active et En veille sur l'adresse contactée par les dispositifs Edge (pulsations).

4 Configurez DR en suivant la procédure de configuration de récupération d'urgence habituelle décrite dans la section *Récupération d'urgence de SD-WAN Orchestrator*.

Mettre à niveau la configuration DR

Pour mettre à niveau une paire de SD-WAN Orchestrator compatible DR, procédez comme suit.

Pour mettre à niveau une paire de VCO compatible DR :

Note Si la mise à niveau d'Orchestrator passe de 2.X à 3.2.X, exécutez le script dr-standby-schema.sh sur l'instance en veille avant de démarrer la mise à niveau.

1 Préparez la mise à niveau. Pour obtenir des instructions, accédez à Étape 1 : Préparation de la mise à niveau d'Orchestrator de la section intitulée Mettre à niveau une instance d'Orchestrator avec le déploiement DR.

2 Procédez à la mise à niveau d'Orchestrator. Pour obtenir des instructions, accédez à Étape 3 : Mise à niveau d'Orchestrator de la section intitulée Mettre à niveau une instance d'Orchestrator avec le déploiement DR.

Configurer la récupération d'urgence de SD-WAN Orchestrator

19

Cette section fournit des instructions de récupération d'urgence (DR) pour SD-WAN Orchestrator.

Ce chapitre contient les rubriques suivantes :

Présentation de la récupération d'urgence de SD-WAN Orchestrator

La fonctionnalité de récupération d'urgence (DR) de SD-WAN Orchestrator empêche la perte de données stockées et reprend les services de SD-WAN Orchestrator en cas de défaillance du système ou du réseau.

La récupération d'urgence de SD-WAN Orchestrator implique la configuration d'une paire d'instances de SD-WAN Orchestrator active/en veille avec la réplication des données et un mécanisme de basculement déclenché manuellement.

- L'objectif de temps de récupération (RTO) est donc dépendant de l'action explicite de l'opérateur pour déclencher la promotion de l'instance en veille.
- Toutefois, l'objectif de point de récupération (RPO) est essentiellement de zéro, quel que soit le temps de récupération, car toutes les configurations sont répliquées instantanément. Les données de surveillance qui auraient été collectées pendant la panne sont mises en cache sur les dispositifs Edge et les passerelles en attente de la promotion de l'instance en veille.

Note La récupération d'urgence est obligatoire. Pour obtenir des licences et des tarifs, contactez l'équipe commerciale de VMware.

Paire d'instances active/en veille

Dans un déploiement de récupération d'urgence de SD-WAN Orchestrator, deux systèmes SD-WAN Orchestrator identiques sont configurés en tant que paire d'instances active/en veille. L'opérateur peut afficher l'état d'avancement de la récupération d'urgence via l'interface utilisateur Web de l'un des serveurs. Les dispositifs Edge et les passerelles connaissent les deux instances de SD-WAN Orchestrator et, tandis qu'ils reçoivent les modifications de configuration uniquement depuis l'instance de SD-WAN Orchestrator active, ils envoient régulièrement des pulsations DR aux deux systèmes pour signaler leur vue des deux serveurs et interroger l'état du système DR. Lorsque l'opérateur déclenche un basculement, les dispositifs Edge et les passerelles sont informés de la modification dans la pulsation DR suivante.

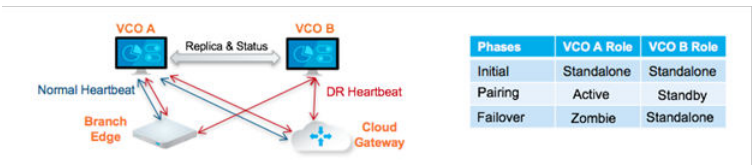
États de récupération d'urgence

Depuis la vue d'un opérateur, des dispositifs Edge et des passerelles, une instance de SD-WAN Orchestrator présente l'un des quatre états DR suivants :

État de récupération d'urgence	Description
Autonome	Aucune récupération d'urgence configurée.
Actif (Active)	Récupération d'urgence configurée, agissant comme le serveur SD-WAN Orchestrator principal.
En veille	Récupération d'urgence configurée, agissant comme un serveur réplica SD-WAN Orchestrator inactif.
Zombie	Récupération d'urgence précédemment configurée et active, mais n'agissant plus comme l'instance active ou en veille.

Opération d'exécution

Lorsque la récupération d'urgence est configurée, le serveur en veille s'exécute en mode limité, bloquant tous les appels d'API, à l'exception de ceux liés à l'état de DR et aux pulsations DR. Lorsque l'opérateur appelle un basculement, l'instance en veille est promue afin de devenir entièrement opérationnelle en tant que serveur autonome. Le serveur qui était précédemment actif passe automatiquement à un état de zombie s'il est réactif et visible à partir de l'instance en veille promue. À l'état de zombie, les services de configuration de gestion sont bloqués et tous les contacts des dispositifs Edge et des passerelles qui n'ont pas été migrés vers la nouvelle instance de SD-WAN Orchestrator active sont redirigés vers le serveur promu.



Phases	VCO A Role	VCO B Role
Initial	Standalone	Standalone
Pairing	Active	Standby
Failover	Zombie	Standalone

Configuration de la réplication de SD-WAN Orchestrator

Deux instances de SD-WAN Orchestrator installées sont requises pour lancer la réplication.

- L'instance en veille sélectionnée est placée dans un état de `STANDBY_CANDIDATE`, ce qui lui permet d'être configurée par le serveur actif.
- Le serveur actif reçoit ensuite l'adresse et les informations d'identification de l'instance en veille et il passe à l'état `ACTIVE_CONFIGURING`.

Lorsque l'instance de `STANDBY_CONFIG_RQST` passe d'active à en veille, les deux serveurs se synchronisent à l'aide des transitions d'état.

Les deux dispositifs Orchestrator sur lesquels vous devez établir la récupération d'urgence (Disaster Recovery, DR) doivent disposer de la même heure. Avant de lancer la réplication de SD-WAN Orchestrator, veillez à vérifier les configurations NTP suivantes :

- Le fuseau horaire de la passerelle doit être défini sur **Etc/UTC**. Utilisez la commande suivante pour afficher le fuseau horaire NTP.

  ```
  vcadmin@vcg1-example:~$ cat /etc/timezone
  Etc/UTC
  vcadmin@vcg1-example:~$
  ```

  Si le fuseau horaire est incorrect, utilisez les commandes suivantes pour mettre à jour le fuseau horaire.

  ```
  echo "Etc/UTC" | sudo tee /etc/timezone
  sudo dpkg-reconfigure --frontend noninteractive tzdata
  ```

- Le décalage NTP doit être inférieur ou égal à 15 millisecondes. Utilisez la commande suivante pour afficher le décalage NTP.

  ```
  sudo ntpqvcadmin@vcg1-example:~$ sudo ntpq -p
       remote           refid      st t when poll reach   delay   offset  jitter
  ==============================================================================
  *ntp1-us1.prod.v 74.120.81.219    3 u  474 1024  377   10.171   -1.183   1.033
   ntp1-eu1-old.pr .INIT.          16 u    - 1024    0    0.000    0.000   0.000
  vcadmin@vcg1-example:~$
  ```

  Si le décalage est incorrect, utilisez les commandes suivantes pour mettre à jour le décalage NTP.

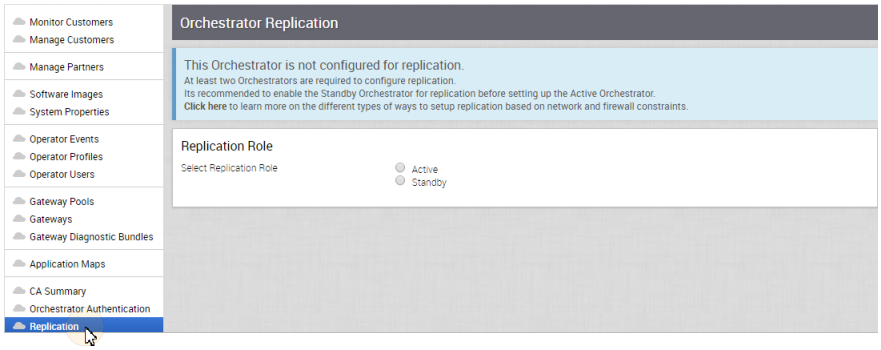
  ```
  sudo systemctl stop ntp
  sudo ntpdate <server>
  sudo systemctl start ntp
  ```

- Par défaut, une liste de serveurs NTP est configurée dans le fichier `/etc/ntpd.conf`. Les dispositifs Orchestrator sur lesquels vous devez établir la récupération d'urgence (DR) doivent disposer d'Internet pour accéder aux serveurs NTP par défaut et garantir la synchronisation de l'heure sur les deux dispositifs Orchestrator. Pour synchroniser l'heure, les clients peuvent également utiliser leur serveur NTP local s'exécutant dans leur environnement.

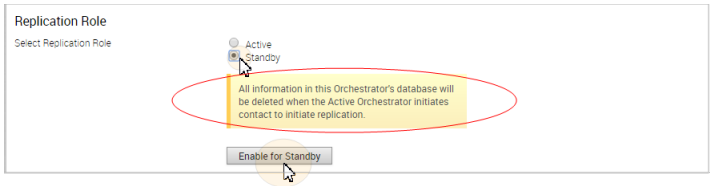
Configurer l'instance d'Orchestrator en veille

Pour configurer la réplication de SD-WAN Orchestrator, procédez comme suit :

1 Cliquez sur **Réplication (Replication)** dans le panneau de navigation pour afficher l'écran **Réplication d'Orchestrator (Orchestrator Replication)**.

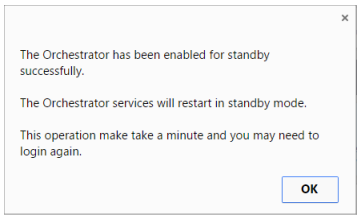


2 Activez l'instance d'Orchestrator en veille en sélectionnant la case d'option **En veille (rôle de réplication) (Standby (Replication Role))**.

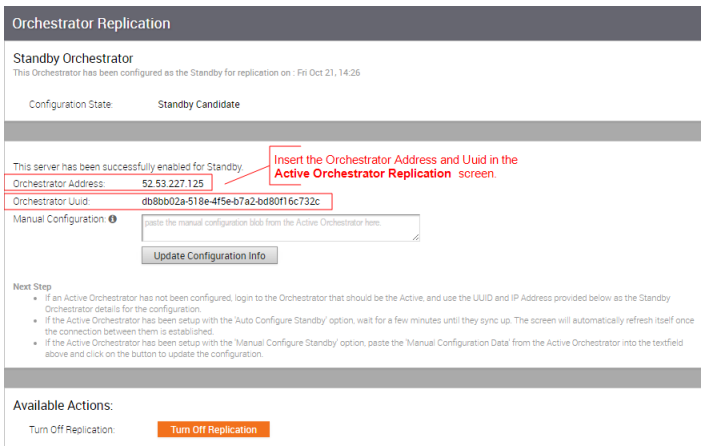


3 Cliquez sur le bouton **Activer pour le mode veille (Enable for Standby)**.

La boîte de dialogue **Réussite d'Orchestrator (Orchestrator Success)** s'affiche, indiquant que l'instance d'Orchestrator a été activée pour le mode veille et qu'elle redémarrera dans ce mode.



4 Cliquez sur **OK**.



Une fois que l'instance d'Orchestrator en veille a été configurée pour la réplication, configurez l'instance d'Orchestrator active en suivant les instructions ci-dessous.

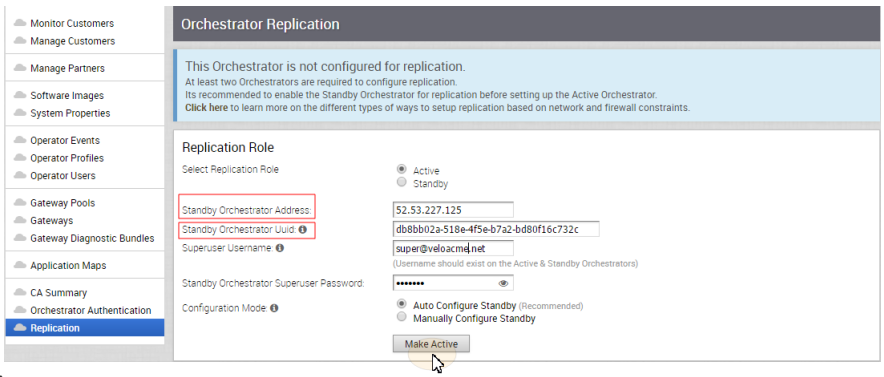
Configurer l'instance active d'Orchestrator

Pour configurer la seconde instance d'SD-WAN Orchestrator pour qu'elle soit l'instance active d'Orchestrator :

1 Dans le panneau de navigation, cliquez sur **Réplication (Replication)**. L'écran **Réplication d'Orchestrator (Orchestrator Replication)** s'affiche.

2 Choisissez le **Rôle de réplication active (Active Replication Role)**.

3 Entrez l'**Adresse de l'instance en veille d'Orchestrator (Standby Orchestrator Address)** et l'**UUID de l'instance en veille d'Orchestrator (Standby Orchestrator Uuid)**. L'adresse et l'UUID d'Orchestrator s'affichent dans l'écran **Instance en veille d'Orchestrator (Standby Orchestrator)**.

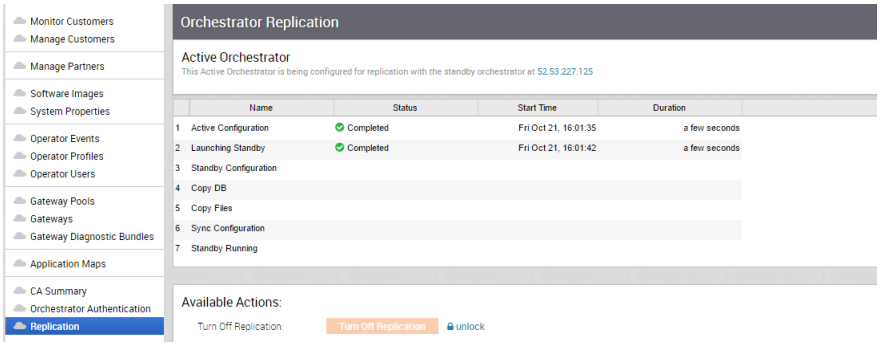


4 Entrez le nom d'utilisateur et le mot de passe du super utilisateur Orchestrator à utiliser pour la réplication.

Note Ce super utilisateur doit déjà être présent sur les deux systèmes.

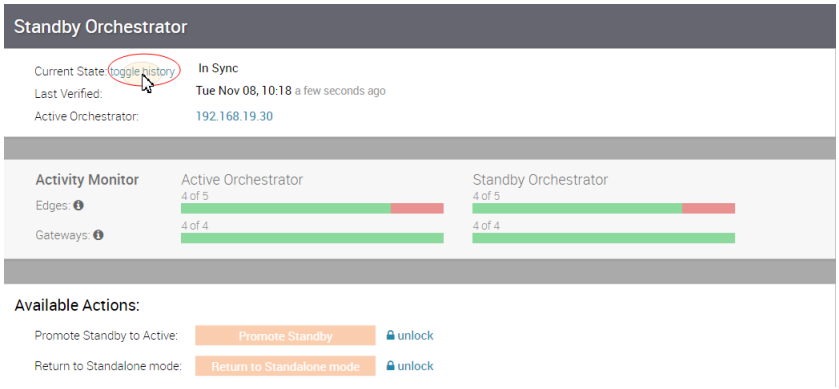
5 Cliquez sur le bouton **Rendre actif (Make Active)**.

L'écran **Instance active d'Orchestrator (Active Orchestrator)** s'affiche et indique un statut de l'état actuel.

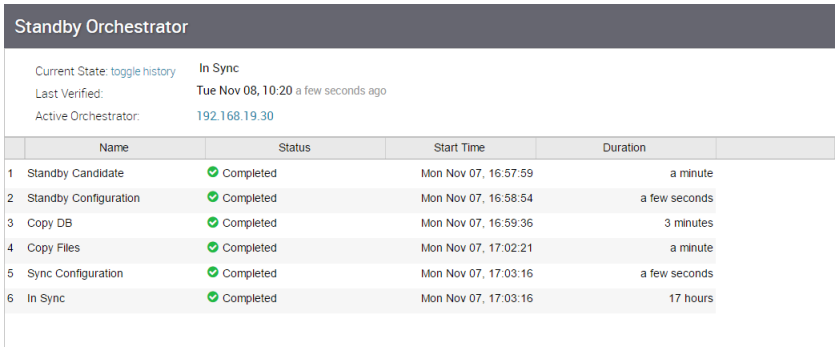


Une fois la configuration terminée, les deux instances d'Orchestrator (En veille et Actif) seront synchronisées.

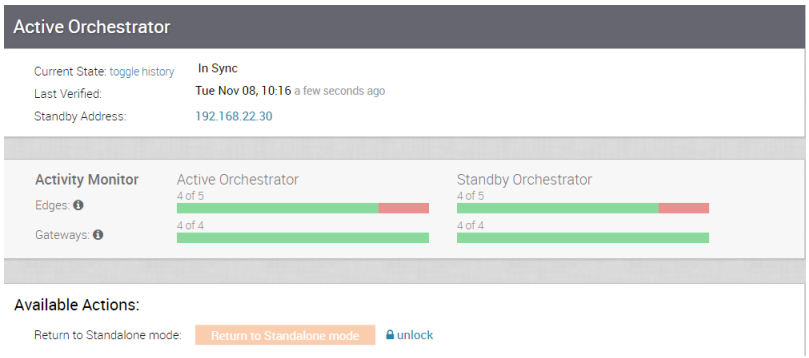
Instance en veille d'Orchestrator synchronisée



Vous pouvez cliquer sur le lien **Activer/désactiver l'historique (toggle history)** pour afficher le statut de chaque état.



Instance active d'Orchestrator synchronisée



Basculement de test

Les scénarios de basculement de test suivants sont des basculements forcés fournis à titre d'exemple. Vous pouvez effectuer ces actions dans la zone **Actions disponibles (Available Actions)** des écrans **Active (Active)** et **En veille (Standby)**.

Promouvoir une instance d'Orchestrator en veille

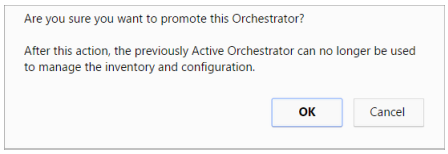
Cette section décrit comment promouvoir une instance d'Orchestrator en veille.

Pour promouvoir une instance d'Orchestrator en veille

1 Cliquez sur le lien **déverrouiller (unlock)**.

2 Cliquez sur le bouton **Promouvoir le mode veille (Promote Standby)** dans la zone **Actions disponibles (Available Actions)** de l'écran Orchestrator en veille.

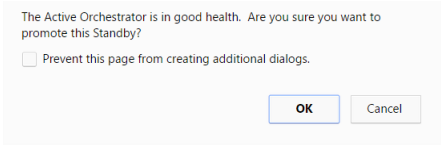
La boîte de dialogue suivante s'affiche, indiquant que lorsque vous promouvez votre instance d'Orchestrator en veille, les administrateurs ne pourront plus gérer SD-WAN Orchestrator à l'aide de l'instance d'Orchestrator précédemment active.



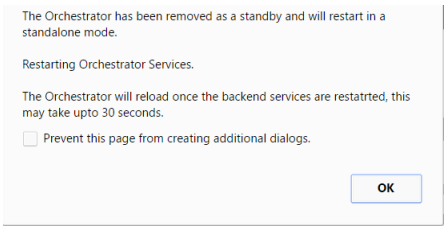
3 Cliquez sur le bouton **OK** pour promouvoir l'instance d'Orchestrator en veille.

Une autre boîte de dialogue de message s'affiche pour vérifier votre demande de promotion de l'instance d'Orchestrator en veille. Ce message s'affiche uniquement si l'instance d'Orchestrator en veille perçoit que l'instance d'Orchestrator active est en bonne santé, ce qui signifie que l'instance en veille communique avec les données actives et de duplication.

4 Cliquez sur **OK** pour promouvoir l'instance d'Orchestrator.

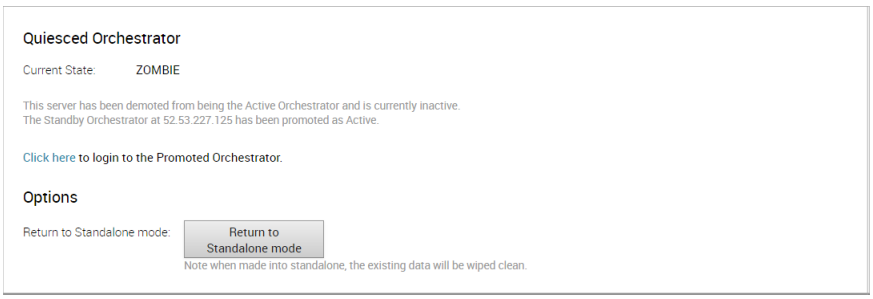


Une boîte de dialogue finale s'affiche, indiquant que l'instance d'Orchestrator n'est plus en veille et qu'elle redémarrera en mode autonome.



Lorsque vous promouvez une instance d'Orchestrator en veille, elle redémarre en mode autonome.

Si l'instance en veille peut communiquer avec l'instance d'Orchestrator précédemment active, elle demande à cette instance d'Orchestrator de passer à l'état de zombie. À l'état de zombie, l'instance d'Orchestrator communique avec ses clients (dispositifs Edge, passerelles, interface utilisateur/API) pour leur signaler qu'elle n'est plus active et qu'ils doivent communiquer avec la nouvelle instance d'Orchestrator promue. Si l'instance en veille promue ne peut pas communiquer avec l'instance d'Orchestrator précédemment active, l'opérateur doit, si possible, rétrograder manuellement l'instance d'Orchestrator précédemment active.



Revenir au mode autonome

Pour remettre le zombie en mode autonome, cliquez sur le bouton **Revenir au mode autonome (Return to Standalone Mode)** dans la zone **Actions disponibles (Available Actions)** des écrans **Instance active d'Orchestrator (Active Orchestrator)** ou **Instance en veille d'Orchestrator (Standby Orchestrator)**.

Note Le dispositif Orchestrator peut revenir de l'état Zombie au mode autonome après le délai spécifié dans la propriété système « vco.disasterRecovery.zombie.expirySeconds » qui est par défaut de 1 800 secondes.

Dépannage de la récupération d'urgence de SD-WAN Orchestrator

Cette section décrit les états de panne du système. Ceux-ci sont également répertoriés dans l'interface utilisateur avec une description plus détaillée de la panne. Des informations supplémentaires sont disponibles dans le journal de VMware.

Pannes récupérables

Les erreurs suivantes sont des pannes récupérables susceptibles se produire après que la récupération d'urgence de SD-WAN Orchestrator a atteint l'état synchronisé. Si le problème entraînant ces pannes est corrigé, la récupération d'urgence de SD-WAN Orchestrator reviendra automatiquement à un fonctionnement normal.

- `FAILURE_SYNCING_FILES`
- `FAILURE_GET_STANDBY_STATUS`
- `FAILURE_MYSQL_ACTIVE_STATUS`
- `FAILURE_MYSQL_STANDBY_STATUS`

Pannes irrécupérables

Les pannes suivantes peuvent se produire lors de la configuration de la récupération d'urgence de SD-WAN Orchestrator. La récupération d'urgence de SD-WAN Orchestrator ne récupérera pas automatiquement après ces pannes.

- `FAILURE_ACTIVE_CONFIGURING`
- `FAILURE_LAUNCHING_STANDBY`
- `FAILURE_STANDBY_CONFIGURING`
- `FAILURE_COPYING_DB`
- `FAILURE_COPYING_FILES`
- `FAILURE_SYNC_CONFIGURING`
- `FAILURE_GET_STANDBY_CONFIG`

- FAILURE_STANDBY_CANDIDATE
- FAILURE_STANDBY_UNCONFIG
- FAILURE_STANDBY_PROMOTION
- FAILURE_ACTIVE_DEMOTION

Gérer les contrats d'utilisateur 20

SD-WAN Orchestrator permet à un super utilisateur opérateur de créer et de gérer des contrats de licence d'utilisateur final.

Seul un super utilisateur opérateur peut créer un contrat de licence d'utilisateur final.

Par défaut, l'option Contrat d'utilisateur (User Agreement) est désactivée. Pour activer cette option, accédez à **Propriétés système (System Properties)** dans le portail de l'opérateur et définissez la valeur de la propriété système `session.options.enableUserAgreements` sur **True**.

En outre, vous pouvez configurer le mode d'affichage du contrat d'utilisateur en définissant la valeur de la propriété système `vco.enterprise.userAgreement.display.mode` comme suit :

- **NONE** : le contrat d'utilisateur ne s'affiche pas pour les utilisateurs d'entreprise. Il s'agit de la valeur par défaut.
- **ALL** : le contrat d'utilisateur s'affiche pour tous les utilisateurs d'entreprise.
- **WITH_MSPS** : le contrat d'utilisateur s'affiche pour tous les utilisateurs d'entreprise disposant de MSP.
- **WITHOUT_MSPS** : le contrat d'utilisateur s'affiche pour tous les utilisateurs d'entreprise ne disposant pas de MSP.

Les paramètres d'affichage ci-dessus sont appliqués à tous les clients gérés par l'opérateur. En tant qu'opérateur, vous pouvez remplacer ces paramètres pour chaque client d'entreprise, comme décrit dans la section Configurer les clients.

Seul un super utilisateur d'entreprise ou un super utilisateur partenaire peut accepter un contrat de licence, en fonction des paramètres de propriétés système.

Pour créer et gérer le contrat d'utilisateur, accédez à la page **Contrats d'utilisateur (User Agreements)** dans le portail de l'opérateur. Cliquez sur **Actions** pour effectuer les opérations suivantes :

- **Nouveau (New)** : crée un contrat de licence d'utilisateur final. Reportez-vous également à la section Créer un contrat d'utilisateur.
- **Cloner (Clone)** : clone et crée une copie du contrat d'utilisateur sélectionné.
- **Mettre à jour (Update)** : permet de modifier les valeurs du contrat d'utilisateur sélectionné.
- **Supprimer (Delete)** : supprime les contrats d'utilisateur sélectionnés.

- **Exporter le rapport d'acceptation (Export Acceptance Report)** : exporte un rapport de tous les clients ayant accepté les contrats d'utilisateur, dans un fichier CSV.

Ce chapitre contient les rubriques suivantes :

Créer un contrat d'utilisateur

Seuls les super utilisateurs opérateurs peuvent créer un contrat d'utilisateur. Vous pouvez créer plusieurs contrats, mais un seul contrat à la fois peut être actif.

Sur le portail opérateur, cliquez sur **Contrats d'utilisateur (User Agreements)**.

1 Cliquez sur **Nouveau contrat d'utilisateur (New User Agreement)** ou sur **Actions > Nouveau (New)**.

2 Dans la fenêtre **Contrat d'utilisateur (User Agreement)**, entrez les éléments suivants :

- **Nom (Name)** : entrez le nom du client.
- **Activé (Enabled)** : par défaut, cette case est cochée. Si vous décochez la case, le contrat d'utilisateur est inactif.

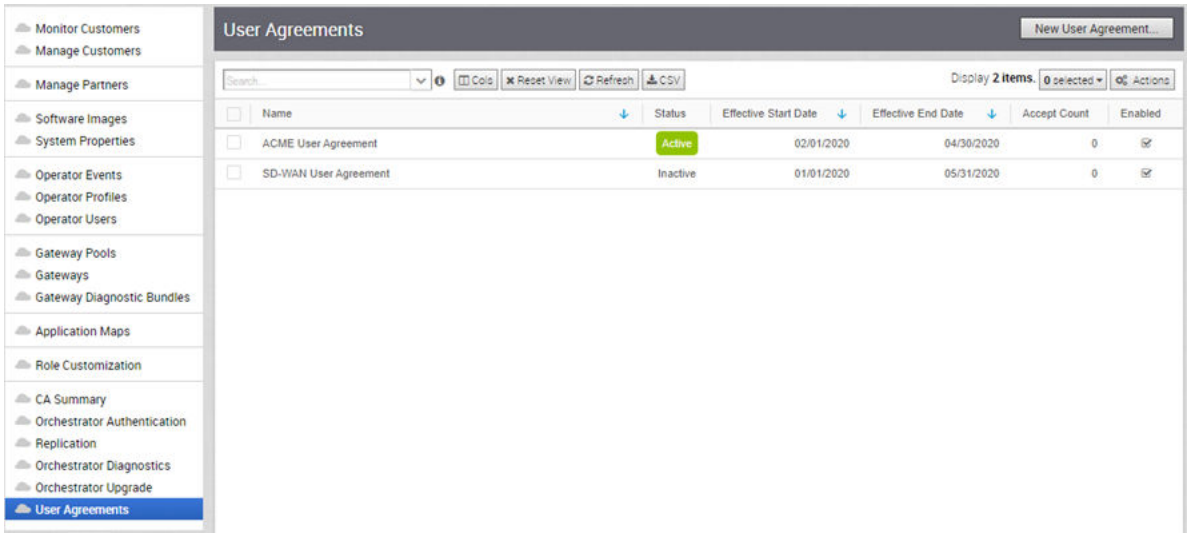
  Note Un seul contrat d'utilisateur à la fois peut être actif. Lorsque vous disposez de plusieurs contrats, veillez à sélectionner l'option **Activé (Enabled)** uniquement pour le contrat qui doit être dans l'état Actif et à désactiver cette option pour les autres contrats d'utilisateur.

- **Date de début de validité (Effective Start Date)** : entrez la date à partir de laquelle le contrat d'utilisateur est valide.
- **Date de fin de validité (Effective End Date)** : entrez la date jusqu'à laquelle le contrat d'utilisateur est valide.
- **Texte de titre de dialogue (Dialog Title Text)** : entrez un titre pour le contrat d'utilisateur.
- **Texte de corps de dialogue (Dialog Body Text)** : entrez le texte descriptif du contrat d'utilisateur visible par le client.

- **Texte de bouton de dialogue (Dialog Button Text)** : entrez le texte à afficher sur le bouton sur lequel le client doit cliquer pour accepter le contrat.

3 Cliquez sur **Créer (Create)**.

Les contrats s'affichent sur la page **Contrats d'utilisateur (User Agreements)**.



Lorsqu'un super utilisateur de l'entreprise ou un super utilisateur du partenaire se connecte à SD-WAN Orchestrator, la fenêtre Contrat d'utilisateur (User Agreement) l'invite à accepter le contrat. Si les utilisateurs n'acceptent pas le contrat, ils sont automatiquement déconnectés.

L'opérateur peut afficher le nombre de clients ayant accepté le contrat sur la page **Contrats d'utilisateur (User Agreements)**. Les contrats acceptés sont archivés et vous ne pouvez pas les supprimer.

Mise à niveau de VMware SD-WAN Orchestrator de la version 3.3.2 ou 3.4 vers la version 4.0

21

Ce document fournit une présentation et des recommandations sur la mise à niveau de VMware SD-WAN Orchestrator de la version 3.3.2 ou 3.4 vers la version 4.0. Toutefois, contactez le support VMware pour qu'il vous aide à mettre à niveau la version 3.3.2 ou 3.4 vers la version 4.0 à l'adresse https://kb.vmware.com/s/article/53907

Vous ne pouvez mettre à niveau que des instances d'Orchestrator versions 3.3.2 et 3.4 vers la version 4.0. Si vous exécutez une version 3.3.1 ou une version antérieure d'Orchestrator, vous devez effectuer une mise à niveau vers la version 3.3.2 au minimum avant de procéder à la mise à niveau vers la version 4.0.

Tenez compte des éléments suivants lors de la mise à niveau :

- Cette tâche de mise à niveau ne modifie pas les API existantes.
- Tout comme les autres versions, des modifications de schéma sont apportées à la version 4.0. Cependant, ces modifications n'ont aucune incidence sur le processus de mise à niveau.

Le système d'exploitation du dispositif virtuel SD-WAN Orchestrator et les banques de données sous-jacentes qui stockent les données de configuration et de statistiques sont en cours de mise à niveau. Les mises à niveau spécifiques incluent les éléments suivants :

- La version du système d'exploitation passe d'Ubuntu 14.04 à 18.04.
- Le magasin de configurations est en cours de migration vers MySQL 8.0.
- Le magasin de statistiques est en cours de migration vers ClickhouseDB.

Note Le système d'exploitation, la base de données et plusieurs autres composants dépendants d'Orchestrator en cours d'utilisation ont atteint leur fin de vie et ne seront plus pris en charge.

Les avantages de la mise à niveau vers la version 4.0 sont les suivants :

- Meilleure évolutivité globale en termes de nombre de dispositifs Edge, de flux et d'interface utilisateur.
- Performances des requêtes plus rapides pour les statistiques, rétention plus longue prête à l'emploi des statistiques de flux.
- Performances de configuration de la récupération d'urgence (DR) initiale plus rapides.

- Utilisation inférieure des ressources - Disque, CPU, RAM.
- Meilleure sécurité en raison de composants avec LTS actif.

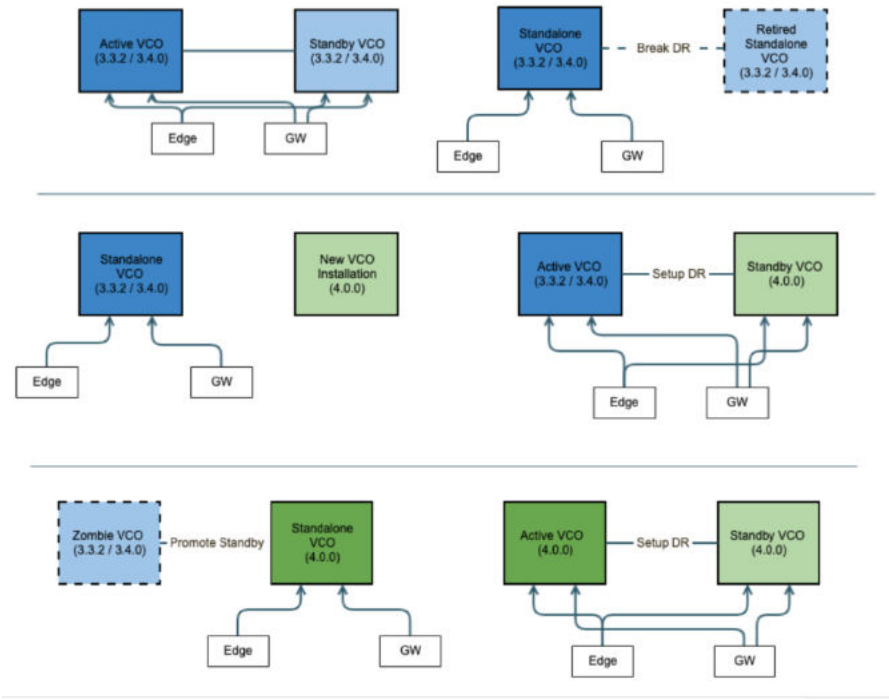
Meilleures pratiques/recommandations :

Vous trouverez ci-dessous répertoriées certaines recommandations de mise à niveau :

- Sur la page Propriétés système dans Orchestrator, notez la valeur de la propriété système edge.heartbeat.spread.factor. Ensuite, remplacez le facteur de propagation de pulsations par une valeur relativement élevée pour une instance élevée d'Orchestrator (par exemple, 20, 40, 60). Cela permet de réduire le pic soudain de l'utilisation des ressources (CPU, E/S) sur le système. Vérifiez que toutes les passerelles et tous les dispositifs Edge sont dans un état connecté avant de restaurer la valeur edge.heartbeat.spread.factor précédente sur la page Propriété système (System Property) dans Orchestrator.
- Laissez l'instance de SD-WAN Orchestrator rétrogradée pendant quelques heures avant de terminer l'arrêt ou la désaffectation.
- Bloquez les modifications de configuration pour éviter toute modification de configuration supplémentaire jusqu'à la fin du processus de mise à niveau.

Présentation de la procédure de mise à niveau

Ce document fournit les étapes nécessaires à la mise à niveau de la version 3.3.2 ou 3.4 vers la version 4.0. La mise à niveau du système d'exploitation et de la récupération d'urgence de SD-WAN Orchestrator présente des étapes semblables aux procédures de récupération d'urgence décrites au Chapitre 19 Configurer la récupération d'urgence de SD-WAN Orchestrator. Cependant, suivez les étapes de la section Procédures de mise à niveau de ce document pour terminer le processus de mise à niveau de la version 3.3.2 ou 3.4 vers la version 4.0. L'image ci-dessous illustre le processus de mise à niveau. Reportez-vous aux procédures de mise à niveau ci-dessous.



Procédures de mise à niveau

Contactez le support VMware pour qu'il vous aide à mettre à niveau la version 3.3.2 ou 3.4 vers la version 4.0 à l'adresse https://kb.vmware.com/s/article/53907.

Dépannage de SD-WAN Orchestrator

22

Cette section décrit le dépannage de SD-WAN Orchestrator.

Ce chapitre contient les rubriques suivantes :

Diagnostics d'Orchestrator

Cette section décrit le bundle Diagnostics d'Orchestrator.

Présentation de Diagnostics de SD-WAN Orchestrator

Le bundle Diagnostics de SD-WAN Orchestrator est un ensemble d'informations de diagnostic dont les services de support et d'ingénierie ont besoin pour dépanner SD-WAN Orchestrator. Pour l'installation sur site d'Orchestrator, les opérateurs peuvent récupérer le bundle Diagnostics de SD-WAN Orchestrator à partir de l'interface utilisateur d'Orchestrator et le fournir à l'équipe de support VMware pour une analyse et une résolution des problèmes hors ligne.

Onglet Bundle de diagnostics

Les utilisateurs peuvent demander et télécharger un bundle de diagnostics dans l'onglet **Bundle de diagnostics (Diagnostics Bundle)**.

Colonnes de l'onglet Bundle de diagnostics (Diagnostics Bundle)

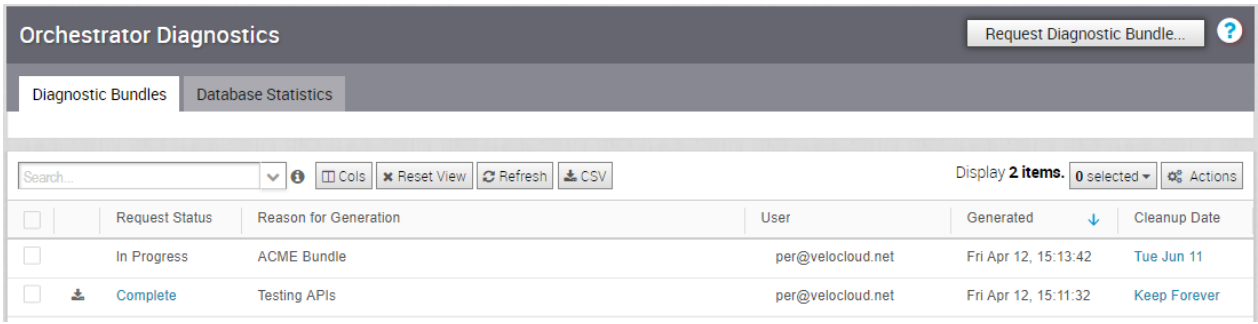
La grille de la table Diagnostics d'Orchestrator (Orchestrator Diagnostics) comprend les colonnes suivantes :

Nom de la colonne (Column Name)	Description
État des demandes (Request Status)	Il existe deux types d'états pour les demandes : ■ Terminé ■ En cours Si le téléchargement du bundle n'est pas terminé, l'état **En cours (In Progress)** s'affiche.
Motif de la génération (Reason for Generation)	Raison spécifique fournie pour la génération d'un bundle de diagnostics. Pour inclure une description du bundle, cliquez sur **Demander le bundle de diagnostics (Request Diagnostic Bundle)**.
Utilisateur	La personne connectée à SD-WAN Orchestrator.
Généré (Generated)	Date et heure d'envoi de la demande du bundle de diagnostics.
Date de nettoyage (Cleanup Date)	La **Date de nettoyage (Cleanup Date)** par défaut se situe trois mois après la date de génération lors de la suppression automatique du bundle. Pour prolonger la période de nettoyage, cliquez sur le lien **Date de nettoyage (Cleanup Date)** situé sous la colonne **Date de nettoyage (Cleanup Date)**. Pour plus d'informations, reportez-vous à la section *Mise à jour de la date de nettoyage*.

Demander un bundle de diagnostics

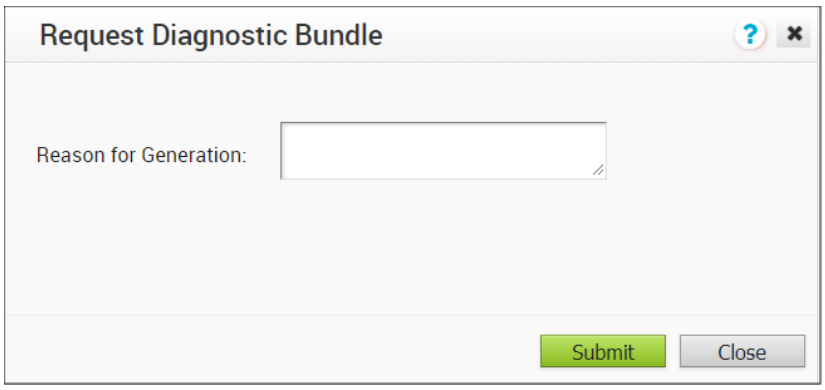
Pour demander un bundle de diagnostics :

1 Dans le panneau de navigation de SD-WAN Orchestrator, cliquez sur **Diagnostics d'Orchestrator (Orchestrator Diagnostics)**.



2 Dans l'onglet **Demander le bundle de diagnostics (Request Diagnostic Bundle)**, cliquez sur le bouton **Demander le bundle de diagnostics (Request Diagnostic Bundle)**.

3 Dans la boîte de dialogue **Demander le bundle de diagnostics (Request Diagnostic Bundle)**, entrez le motif de la demande dans la zone appropriée.



4 Cliquez sur **Envoyer (Submit)**. La demande de bundle que vous avez créée s'affiche dans la zone de grille de l'écran **Bundle de diagnostics (Diagnostics Bundle)** avec un état **En cours (In Progress)**.

5 Actualisez votre écran pour vérifier l'état de la demande du bundle de diagnostics. Lorsque le bundle est prêt à être téléchargé, un état **Terminé (Complete)** s'affiche.

Télécharger un bundle de diagnostics

Pour télécharger un bundle de diagnostics :

1 Sélectionnez un bundle de diagnostics à télécharger.

2 Cliquez sur le bouton **Actions**, puis choisissez **Télécharger le bundle de diagnostics (Download Diagnostic Bundle)**. Vous pouvez également cliquer sur le lien **Terminé (Complete)** pour télécharger le bundle de diagnostics.

Le bundle de diagnostics se télécharge.

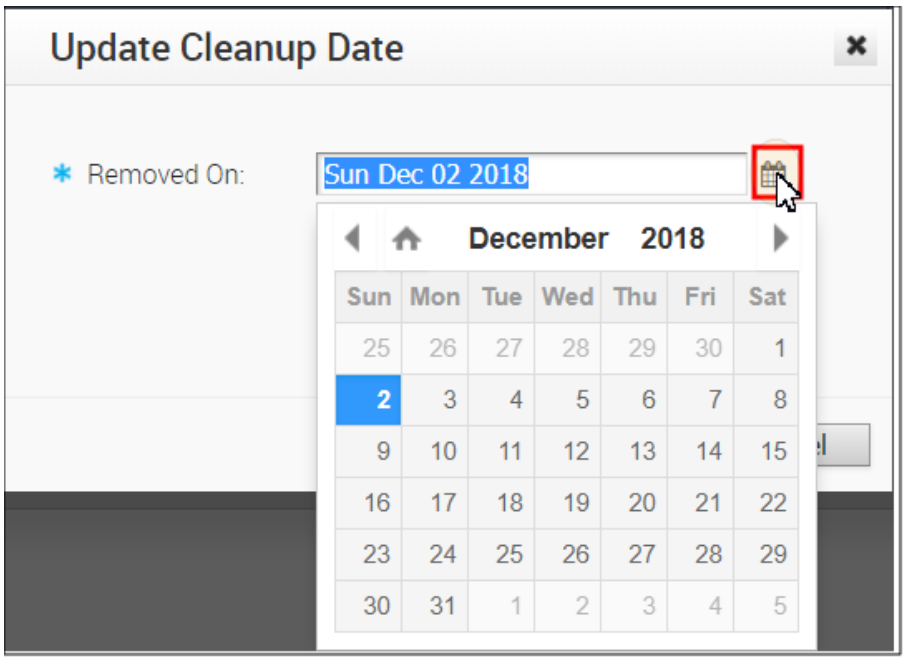
Mettre à jour la date de nettoyage

La date de nettoyage représente la date de suppression automatique du bundle généré, qui par défaut est trois mois après la date de génération. Vous pouvez modifier la date de nettoyage ou choisir de conserver indéfiniment le bundle.

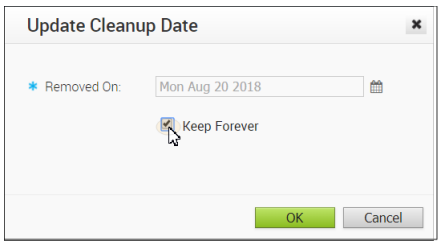
Pour mettre à jour la date de nettoyage :

1 Dans la colonne **Date de nettoyage (Cleanup Date)**, cliquez sur le lien **Date de nettoyage (Cleanup Date)** de votre bundle de diagnostics choisi.

2 Dans la boîte de dialogue **Mettre à jour la date de nettoyage (Update Cleanup Date)**, cliquez sur l'icône **Calendrier (Calendar)** pour modifier la date.

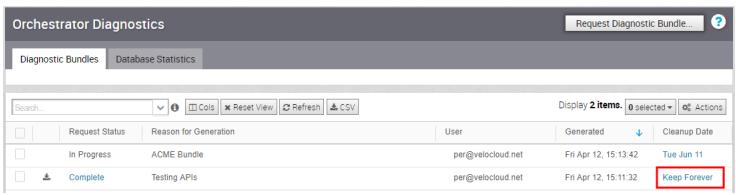


3 Vous pouvez également choisir de conserver indéfiniment le bundle en cochant la case **Conserver indéfiniment (Keep Forever)**.



4 Cliquez sur **OK**.

La grille de la table Diagnostics d'Orchestrator (Orchestrator Diagnostics) est mise à jour pour refléter les modifications de la date de nettoyage.

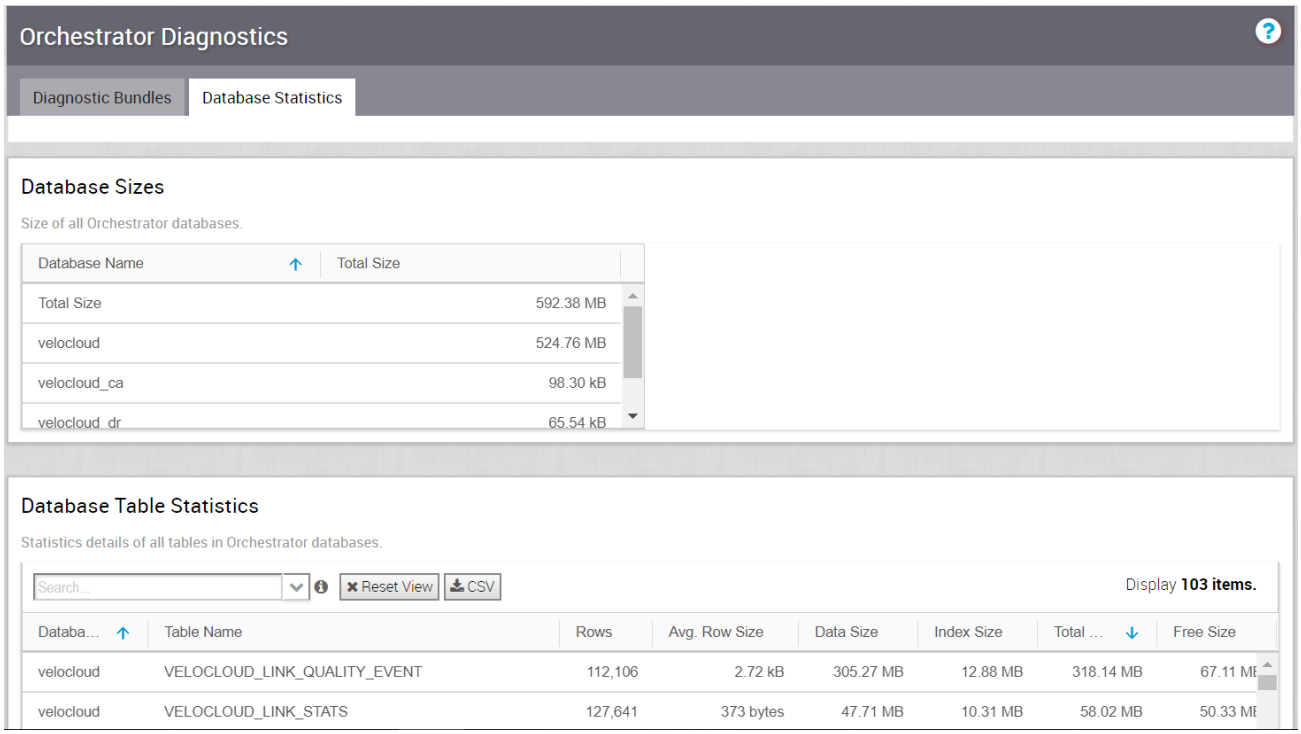


Onglet Statistiques de base de données

L'onglet **Statistiques de base de données (Database Statistics)** fournit une vue d'accès en lecture seule de certaines informations d'un bundle de diagnostics.

Si vous avez besoin d'informations supplémentaires, accédez à l'onglet **Bundles de diagnostics (Diagnostic Bundles)**, demandez un bundle de diagnostics et téléchargez-le localement. Pour plus d'informations, reportez-vous à la section *Demander le bundle de diagnostics*.

L'onglet **Statistiques de base de données (Database Statistics)** affiche les informations suivantes :



Champ	Description
Tailles des bases de données (Database Sizes)	Tailles des bases de données Orchestrator.
Statistiques de la table de base de données (Database Table Statistics)	Informations statistiques de toutes les tables de la base de données Orchestrator.
Informations de stockage de la base de données (Database Storage Info)	Détails de stockage des emplacements montés.
Liste des processus de base de données (Database Process List)	20 premiers enregistrements des requêtes SQL de longue durée.
Variable d'état de base de données (Database Status Variable)	Variables d'état du serveur MySQL.
Variable système de base de données (Database System Variable)	Variables système du serveur MySQL.
État du moteur de base de données (Database Engine Status)	État du moteur InnoDB du serveur MySQL.

Surveillance des mesures système

Cette section décrit la surveillance des mesures système sur Orchestrator.

Présentation de la surveillance des mesures système sur Orchestrator

Orchestrator est fourni avec une pile de surveillance de mesures système intégrée, qui comprend un collecteur de mesures et une base de données de séries chronologiques. La pile de surveillance simplifie la vérification de la condition de santé et de la charge du système d'Orchestrator.

Pour activer la pile de surveillance, exécutez la commande suivante sur Orchestrator :

- sudo /opt/vc/scripts/vco_observability_manager.sh enable

Pour vérifier l'état de la pile de surveillance, exécutez la commande suivante :

- sudo /opt/vc/scripts/vco_observability_manager.sh status

Pour désactiver la pile de surveillance, exécutez la commande suivante :

- sudo /opt/vc/scripts/vco_observability_manager.sh disable

Collecteur de mesures

Telegraf est utilisé comme collecteur de mesures système d'Orchestrator, qui comporte des plug-ins pour collecter des mesures système. Les mesures suivantes sont activées par défaut.

Nom de la mesure	Description
inputs.cpu	Mesures sur l'utilisation du CPU.
inputs.mem	Mesures sur l'utilisation de la mémoire.
inputs.net	Mesures sur les interfaces réseau.
inputs.system	Mesures sur la charge du système et le temps d'activité.
inputs.processes	Nombre de processus regroupés par état.
inputs.disk	Mesures sur l'utilisation du disque.
inputs.diskio	Mesures concernant les E/S de disque par périphérique.
inputs.procstat	Utilisation du CPU et de la mémoire pour des processus spécifiques.
inputs.nginx	Informations sur l'état de base de Nginx (ngx_http_stub_status_module).
inputs.mysql	Données statistiques du serveur MySQL.
inputs.clickhouse	Mesures d'un ou de plusieurs serveurs ClickHouse.
inputs.redis	Mesures d'un ou de plusieurs serveurs Redis.
inputs.filecount	Nombre et taille totale des fichiers dans les répertoires spécifiés.

Nom de la mesure	Description
inputs.ntpq	Mesures de requête NTP standard (nécessite un exécutable ntpq).
Inputs.x509_cert	Mesures d'un certificat SSL.

Pour activer davantage de mesures ou désactiver certaines mesures activées, modifiez le fichier de configuration Telegraf sur Orchestrator en procédant comme suit :

- sudo vi /etc/telegraf/telegraf.d/system_metrics_input.conf
- sudo systemctl restart telegraf

Base de données de séries chronologiques

Prometheus permet de stocker les mesures système collectées par Telegraf. Les données de mesures sont conservées dans la base de données pendant trois semaines au maximum. Par défaut, Prometheus écoute sur le port 9090. Si vous disposez d'un outil de surveillance externe, fournissez la base de données Prometheus en tant que source, afin de pouvoir afficher les mesures système d'Orchestrator sur votre interface utilisateur de surveillance.

Demandes d'API de limite de débit

Lors de l'envoi d'un trop grand nombre de demandes d'API simultanées, cela a une incidence sur les performances du système. Vous pouvez activer la limite de débit, ce qui applique une limite au nombre de demandes d'API envoyées par chaque utilisateur.

SD-WAN Orchestrator utilise certains mécanismes de défense qui permettent de limiter les abus d'API et assure la stabilité du système. Les demandes d'API qui dépassent les limites de demandes autorisées sont bloquées et renvoyées avec le code d'état HTTP 429 (trop de demandes). Le système doit passer par une période de refroidissement avant de refaire les demandes.

Les types de limiteurs de débit suivants sont déployés sur SD-WAN Orchestrator :

- **Limiteur de seau percé (Leaky bucket limiter)** : limite la rafale de demandes et n'autorise qu'un nombre prédéfini de demandes. Ce limiteur veille à limiter le nombre de demandes autorisées dans une fenêtre de temps donnée.
- **Limiteur de simultanéité (Concurrency limiter)** : limite le nombre de demandes autorisées qui se produisent en parallèle, ce qui génère des demandes simultanées en quête de ressources et peut entraîner des requêtes de longue durée.

Voici les principales raisons qui conduisent à une limite de débit pour les demandes d'API :

- Grand nombre de demandes actives ou simultanées.
- Pics soudains du volume de demandes.
- Abandon des demandes conduisant à des requêtes de longue durée sur Orchestrator qui mobilisent longtemps des ressources système.

Les développeurs qui s'appuient sur l'API peuvent adopter les mesures suivantes pour améliorer la stabilité de leur code lorsque la capacité de limite de débit VCO est activée.

- Gérez le code de réponse HTTP 429 lorsque les demandes dépassent les limites de débit.
- La durée de la pénalité est de 5 000 ms lorsque le limiteur de débit atteint le nombre maximal de demandes autorisées dans une période donnée. Il est prévu, en cas de blocage, que les clients observent une période de refroidissement de 5 000 ms avant d'effectuer des demandes. Les demandes effectuées pendant la période de refroidissement de 5 000 ms restent limitées en débit.
- Utilisez des intervalles de temps plus courts pour les API de séries chronologiques qui n'autorisent pas l'expiration de la demande en raison de requêtes de longue durée.
- Dans la mesure du possible, préférez les méthodes de requête par lot à celles qui interrogent des clients ou des dispositifs Edge individuels.

Note Les super utilisateurs opérateurs configurent des limites de débit discrètement en fonction de l'environnement. Pour les requêtes sur les stratégies pertinentes, contactez votre opérateur.

Configurer les stratégies de limite de débit à l'aide de propriétés système

Vous pouvez utiliser les propriétés système suivantes pour activer la limite de débit et définir l'ensemble de stratégies par défaut :

- vco.api.rateLimit.enabled
- vco.api.rateLimit.mode.logOnly
- vco.api.rateLimit.rules.global
- vco.api.rateLimit.rules.enterprise.default
- vco.api.rateLimit.rules.enterpriseProxy.default

Pour plus d'informations sur les propriétés système, reportez-vous à la section Tableau 11-10. API de limite de débit.

Configurer les stratégies de limite de débit à l'aide d'API

Il est recommandé de configurer les stratégies du limiteur de débit comme règles globales à l'aide des propriétés système, car cette approche génère les meilleures performances d'API possibles, facilite le dépannage et garantit une expérience utilisateur cohérente pour tous les partenaires et les clients. Dans de rares cas cependant, les opérateurs peuvent décider que les stratégies globales sont trop souples pour un locataire ou un utilisateur particulier. Dans ces cas spécifiques, VMware prend en charge les API d'opérateur uniquement suivantes pour définir des politiques pour des partenaires et des entreprises spécifiques.

- **enterpriseProxy/insertOrUpdateEnterpriseProxyRateLimits** : permet de configurer les stratégies spécifiques au partenaire.

- **enterprise/insertOrUpdateEnterpriseRateLimits** : permet de configurer les stratégies spécifiques au client.

Pour plus d'informations sur les API, reportez-vous à la section https://code.vmware.com/apis/1037/velocloud-sdwan-vco-api.