Gestion du centre de données VMware Cloud on AWS

8 juin 2023
SDDC version 1.22
VMware Cloud on AWS

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 de la gestion du centre de données VMware Cloud™ on AWS 5

Composants et interfaces de vSphere 6

1 Administration de vSphere dans VMware Cloud on AWS 9

Autorisations et privilèges vSphere dans VMware Cloud on AWS 11

Privilèges de CloudAdmin 12

Fédération d'entreprise avec VMware Cloud Services 17

Activer la connexion fédérée pour vCenter 17

Désactiver la connexion fédérée pour vCenter 19

Accès d'urgence à vCenter en cas d'échec de la connexion fédérée 20

Configuration d'Hybrid Linked Mode 21

Conditions préalables de Hybrid Linked Mode 22

Configuration de Hybrid Linked Mode à l'aide du dispositif VMware Cloud Gateway 25

Configuration de Hybrid Linked Mode depuis le SDDC de cloud 29

Dépannage de la mise en réseau pour le mode Hybrid Linked Mode 32

Annuler le lien d'un SDDC de cloud 37

2 Clusters et pools de ressources dans VMware Cloud on AWS 39

Clusters et pools de ressources prédéfinis 41

Examiner les machines virtuelles et les hôtes du cluster 41

Examiner et surveiller vSphere DRS 42

Examiner et surveiller vSphere HA 43

Examiner la configuration du cluster 44

Créer et gérer des pools de ressources enfants 45

3 Stockage vSAN dans VMware Cloud on AWS 48

Capacité de stockage et redondance des données 49

vSAN Déduplication et compression 49

Activation des commandes TRIM/UNMAP pour les clusters VMware Cloud on AWS 50

Chiffrement vSAN dans VMware Cloud on AWS 51

Générer de nouvelles clés de chiffrement dans VMware Cloud on AWS 51

Stratégies vSAN 52

Définir une stratégie de stockage de machine virtuelle pour vSAN 58

Attribuer des stratégies de stockage à des machines virtuelles 58

Appliquer une stratégie de stockage gérée aux machines virtuelles non conformes 60

Mettre à jour la stratégie de stockage par défaut pour un cluster ayant une stratégie non conforme 61

Prise en charge du matériel virtuel dans le SDDC VMware Cloud on AWS 62

Clusters de stockage partagé sur vSAN 62

Gestion des machines virtuelles dans VMware Cloud on AWS 64

Configurations de machines virtuelles ayant une prise en charge limitée ou nulle dans le SDDC de cloud 65

Utilisation de PowerCLI et de l'API des opérations du système invité 68

Déployer une machine virtuelle à partir d'un modèle OVF dans une bibliothèque de contenu 69

À propos de la gestion du centre de données VMware Cloud™ on AWS

La documentation de *Gérer VMware Cloud sur le centre de données AWS* explique comment configurer et gérer votre SDDC (Software-Defined Data Center) VMware Cloud on AWS et les machines virtuelles qui s'y exécutent.

Public cible

Ces informations sont destinées aux administrateurs qui ont une compréhension de base de la configuration et de la gestion de vSphere dans un environnement sur site, et sont familiarisés avec les concepts de virtualisation VMware. Des connaissances approfondies d'Amazon Web Services ne sont pas nécessaires.

Gestion de vSphere dans VMware Cloud on AWS

Une fois la configuration initiale de votre SDDC VMware Cloud on AWS et de ses réseaux terminée, créez des dossiers et des pools de ressources, ajoutez une source d'identité vCenter Single Sign-On et effectuez d'autres opérations avec lesquelles vous êtes peut-être déjà familiarisé à partir d'un environnement sur site. Vous pouvez également utiliser Hybrid Linked Mode pour afficher et gérer votre vCenter Server sur site et celui de votre SDDC VMware Cloud on AWS avec un ensemble commun d'identités d'utilisateur. Vous avez également la possibilité d'activer la connexion fédérée à vCenter, ce qui configure le SDDC vCenter Server pour approuver VMware Cloud Services en tant que fournisseur d'identité afin que les membres de l'organisation doivent utiliser leurs informations d'identification VMware Cloud Services au lieu d'un compte vSphere SSO ou local pour se connecter au SDDC vCenter Server.

Que lire ensuite ?

- Composants et interfaces de vSphere

  VMware vSphere est une suite de composants logiciels de virtualisation. Ils comprennent ESXi, vCenter Server et d'autres composants logiciels qui remplissent plusieurs fonctions différentes dans l'environnement vSphere. VMware gère pour vous de nombreux éléments de votre SDDC VMware Cloud on AWS, mais vous pouvez examiner tous les composants et modifier certaines parties de la configuration.

Composants et interfaces de vSphere

VMware vSphere est une suite de composants logiciels de virtualisation. Ils comprennent ESXi, vCenter Server et d'autres composants logiciels qui remplissent plusieurs fonctions différentes dans l'environnement vSphere. VMware gère pour vous de nombreux éléments de votre SDDC VMware Cloud on AWS, mais vous pouvez examiner tous les composants et modifier certaines parties de la configuration.

Composants de vSphere

vSphere inclut les composants logiciels suivants :

ESXi

L'hyperviseur sur lequel vous exécutez les machines virtuelles comme un ensemble de fichiers de configuration et de disque qui exécutent ensemble toutes les fonctions d'une machine physique.

Note Aucun utilisateur de VMware Cloud on AWS ne dispose d'un accès physique au matériel de l'hôte ESXi ou à la racine du système d'exploitation ESXi. Les procédures qui nécessitent ce type d'accès doivent être effectuées par le personnel VMware. Cela signifie que vous ne pouvez pas ajouter, supprimer ou gérer des utilisateurs ESXi, ni entreprendre d'autres opérations de la Gestion des hôtes avec VMware Host Client.

vCenter Server

Un service qui intervient en tant qu'administrateur central des hôtes VMware ESXi.

vCenter Server fonctionne en continu en arrière-plan. Il exécute ses activités de surveillance et de gestion même si aucun client n'est connecté.

VMware Cloud on AWS inclut une seule instance de vCenter Server qui peut être connectée à une instance de vCenter Server sur site à l'aide du mode Hybrid Linked Mode.

vCenter Single Sign-On

Service qui fait partie de l'infrastructure de gestion vCenter Server. Le service d'authentification de vCenter Single Sign-On renforce la sécurité de la plate-forme de l'infrastructure VMware cloud, car elle permet aux divers composants logiciels vSphere de communiquer entre eux par le biais d'un mécanisme d'échange de jetons sécurisé, au lieu de demander à chaque composant d'authentifier séparément un utilisateur avec un service d'annuaire comme Active Directory.

Interfaces vSphere

L'interface de vSphere que vous utilisez dépend de la tâche que vous souhaitez effectuer et du composant que vous souhaitez gérer.

vSphere Client

vSphere Client est un client basé sur HTML5 pour la gestion de VMware Cloud on AWS. vSphere Client effectue également la plupart des tâches de configuration des SDDC vSphere sur site.

vSphere Command-Line Interfaces

vSphere prend en charge plusieurs interfaces de ligne de commande pour configurer les machines virtuelles et d'autres composants vSphere.

vSphere SDKs

vSphere prend en charge plusieurs SDK pour la gestion des différents aspects de votre environnement vSphere.

Console de machine virtuelle

Tout comme une machine physique, chaque machine virtuelle dispose d'une console qui prend en charge certaines tâches de gestion, selon le système d'exploitation.

Fonctionnalités de vCenter Server

De nombreuses fonctionnalités vCenter Server nécessitant une licence spéciale dans les versions antérieures du produit sont disponibles dans le cadre de la licence vSphere Standard dans vSphere 6.x et sont également prises en charge pour VMware Cloud on AWS.

Les fonctionnalités vCenter Server incluent :

vSphere vMotion

Vous permet de déplacer des machines virtuelles en cours d'exécution d'un hôte ESXi vers un autre sans interruption de service.ESXi

Storage vMotion

Vous permet de déplacer les disques et le fichier de configuration d'une machine virtuelle en service d'une banque de données à une autre sans interruption de service.

vSphere High Availability

vSphere High Availability garantit qu'en cas d'échec d'un hôte dans un cluster SDDC, toutes les machines virtuelles sur l'hôte sont redémarrées sur un autre hôte dans le même cluster. Les paramètres de vSphere High Availability sont préconfigurés dans VMware Cloud on AWS et ne peuvent pas être modifiés par les clients.

vSphere DRS

Contribue à améliorer l'allocation des ressources et la consommation électrique à travers tous les hôtes et pools de ressources. vSphere DRS recueille les informations sur l'utilisation

des ressources par tous les hôtes et machines virtuelles du cluster et transfère les machines virtuelles dans l'une des situations suivantes :

- Placement initial – Quand vous mettez une machine virtuelle sous tension pour la première fois dans le cluster, soit DRS la place sur un hôte, soit il soumet une recommandation.
- Équilibrage de charge – DRS tente d'améliorer l'utilisation des ressources dans le cluster soit en effectuant des migrations automatiques de machines virtuelles (vMotion), soit en soumettant des recommandations de migration de machines virtuelles.

Pour plus de détails sur les stratégies de stockage qui régissent le fonctionnement de DRS dans le SDDC, reportez-vous à la section Utilisation de stratégies et de profils.

Administration de vSphere dans VMware Cloud on AWS

1

vSphere dans un centre de données défini par logiciel de cloud comme votre SDDC VMware Cloud on AWS fonctionne de la même manière que votre instance de vSphere sur site. Dans le SDDC, certains composants de vSphere sont détenus et gérés par VMware, de sorte que certains des workflows d'administration sur site qui vous sont familiers présentent des différences ou ne sont pas nécessaires.

Quelles sont les différences dans le cloud ?

Pour plus d'informations sur l'administration de vSphere dans VMware Cloud on AWS, vous devez vous reporter à la documentation de vSphere, mais vous devez aussi garder à l'esprit quelques différences générales lors de la lecture de ces rubriques :

- Les utilisateurs de VMware Cloud on AWS ne disposent pas d'un accès physique pour accéder au matériel de l'hôte ESXi et ne peuvent pas se connecter au système d'exploitation de l'hôte ESXi. Les procédures qui nécessitent ce type d'accès sont effectuées par le personnel VMware.
- Les Autorisations globales définies dans votre instance de vCenter Server sur site ne s'appliquent pas aux objets que VMware gère pour vous, tels que les hôtes SDDC et les banques de données, de sorte qu'ils ne sont pas répliqués de votre environnement sur site vers l'instance de vCenter Server de votre SDDC de cloud.

Outre ces différences générales, de nombreuses rubriques de la documentation de vSphere sont écrites spécifiquement pour les utilisateurs sur site et n'incluent pas certaines des informations dont vous avez besoin lors de l'utilisation de vSphere dans le SDDC de cloud. VMware Cloud on AWS fournit également plusieurs méthodes pour consolider la gestion des comptes d'utilisateurs vSphere afin de pouvoir afficher et gérer les utilisateurs et les ressources de plusieurs instances de vCenter via un écran unique.

Tableau 1-1. Différences de contenu des rubriques entre vSphere sur site et dans un SDDC

Rubrique	Points clés
Objets d'inventaire gérés de vSphere	Chaque SDDC VMware Cloud on AWS dispose d'un centre de données unique nommé SDDC-Datacenter. Le centre de données définit l'espace de noms des réseaux et des banques de données. Les noms de ces objets doivent être uniques au sein d'un centre de données. Vous ne pouvez pas avoir deux banques de données portant le même nom dans un centre de données unique. Les machines virtuelles, les modèles et les clusters n'ont pas besoin d'être uniques au sein du centre de données, mais doivent l'être dans leur dossier.
■ Gestion des hôtes avec VMware Host Client ■ Sécurisation des hôtes ESXi	Les utilisateurs de VMware Cloud on AWS ne disposent pas d'un accès physique pour accéder au matériel de l'hôte ESXi et ne peuvent pas se connecter au système d'exploitation de l'hôte ESXi. Les procédures qui nécessitent ce type d'accès sont effectuées par le personnel VMware.
Sécurisation des systèmes vCenter Server	Dans un SDDC sur site, vous êtes responsable de la sécurité de votre système vCenter Server. Dans VMware Cloud on AWS, VMware effectue la plupart de ces tâches à votre place. Vous êtes responsable de suivre les meilleures pratiques de sécurité suivantes, en particulier pour les machines virtuelles de votre environnement, et souhaiterez peut-être connaître certains autres aspects de vCenter Server et de vCenter Single Sign-On, tels que les stratégies de mot de passe et de verrouillage.
Authentification vSphere à l'aide de vCenter Single Sign-On	Lorsque vous modifiez le mot de passe de votre SDDC à partir de vSphere Client, le nouveau mot de passe n'est pas synchronisé avec le mot de passe affiché sur la page Informations d'identification vCenter par défaut. Cette page affiche uniquement les informations d'identification par défaut. Si vous modifiez les informations d'identification, il vous appartient de garder une trace du nouveau mot de passe. Contactez le Support technique et demandez un changement de mot de passe. Après l'installation, cloudadmin@vmc.local dispose d'un accès administrateur à vCenter Single Sign-On et à vCenter Server. Cet utilisateur peut également ajouter des sources d'identité, définir la source d'identité par défaut et définir des stratégies dans le domaine cloudadmin@vmc.local. Certaines opérations de gestion dans le domaine vmc.local sont restreintes au personnel des opérations de VMware Cloud on AWS.

Lisez les sections suivantes :

- Autorisations et privilèges vSphere dans VMware Cloud on AWS
- Fédération d'entreprise avec VMware Cloud Services

- Activer la connexion fédérée pour vCenter
- Configuration d'Hybrid Linked Mode

Autorisations et privilèges vSphere dans VMware Cloud on AWS

Utilisez vSphere Client pour afficher les privilèges accordés aux utilisateurs de vCenter, que ces utilisateurs soient définis dans le domaine vSphere Single Sign-On par défaut ou dans un fournisseur d'identité tel qu'Active Directory.

Outre les rôles et les autorisations décrits dans la section Utilisation de rôles vCenter Server pour attribuer des privilèges, l'instance de vCenter Server de votre SDDC inclut les rôles prédéfinis suivants qui ne sont pas présents dans votre instance de vCenter sur site :

Rôle CloudAdmin

Le rôle CloudAdmin dispose des privilèges nécessaires pour créer et gérer des charges de travail de SDDC et des objets associés, tels que des stratégies de stockage, des bibliothèques de contenu, des balises vSphere et des pools de ressources. Ce rôle ne peut pas configurer les objets qui sont pris en charge et gérés par VMware, ni y accéder (par exemple, les hôtes, les clusters et les machines virtuelles de gestion). Le rôle CloudAdmin peut créer, cloner ou modifier des rôles autres que les rôles par défaut . Pour obtenir des informations détaillées sur les privilèges attribués à ce rôle, reportez-vous à la section Privilèges CloudAdmin.

Note L'utilisateur CloudAdmin peut accorder à d'autres utilisateurs ou groupes un accès en lecture seule aux objets de gestion vCenter VMware Cloud on AWS, tels que **Mgmt-ResourcePool**, le dossier **Machines virtuelles de gestion**, **Machines virtuelles découvertes**, **vmc-hostswitch** et **vsanDatastore**. Étant donné que cet accès en lecture seule ne se propage pas aux objets de gestion, vous ne pouvez pas l'accorder en tant qu'autorisation globale et devez l'accorder explicitement pour chaque objet de gestion. VMware Cloud on AWS exécute un script une fois par jour qui met à jour tous les objets de gestion récemment créés (tels que les objets d'un nouveau cluster) afin que le rôle mis à jour soit appliqué à l'utilisateur CloudAdmin et au groupe SSO CloudAdminGroup. Le script lui-même n'accorde pas d'accès supplémentaire à un utilisateur ou à un groupe. Vous devez donc attendre qu'il se termine avant que CloudAdmin puisse utiliser ce workflow pour accorder un accès en lecture seule à ces objets.

Seul, le rôle CloudAdmin n'attribue aucun accès aux objets de gestion. En tant que membre du CloudAdminGroup, le compte CloudAdmin@vmc.local hérite des autorisations de groupe, qui incluent un accès en lecture seule aux objets de gestion.

VMware Cloud on AWS définit également un ensemble de rôles de service que vous gérez dans la console VMware Cloud Services et un ensemble de rôles d'organisation attribués dans le cadre de l'invitation de nouveaux utilisateurs. Ces rôles peuvent restreindre davantage les droits dont disposent les membres de l'organisation pour accéder à des objets vSphere dans le SDDC. Reportez-vous aux sections Attribuer un rôle de service à un membre de l'organisation et Inviter un nouvel utilisateur.

Pour plus d'informations sur l'utilisation d'outils d'automatisation vSphere tels que PowerCLI ou vSphere Terraform Provider pour créer des rôles vCenter Server personnalisés, reportez-vous à la section Rôle vCenter Server personnalisé à l'aide de vSphere Terraform Provider sur VMware Cloud on AWS.

Procédure

1. Connectez-vous à VMware Cloud Services à l'adresse https://vmc.vmware.com.
2. Cliquez sur **Inventaire > SDDC**, puis choisissez une carte SDDC et cliquez sur **OUVRIR VCENTER**.
3. Utilisez vSphere Client pour sélectionner un objet dans la hiérarchie d'objets, par exemple un pool de ressources ou une machine virtuelle, puis cliquez sur **Autorisations**.
4. Vous pouvez ensuite afficher les privilèges associés à chaque groupe.
   a. Dans la page d'accueil de vSphere Client, cliquez sur **Administration**.
   b. Sous **Contrôle d'accès**, cliquez sur **Rôles**.
   c. Cliquez sur un nom de rôle (**CloudAdmin** , par exemple).
   d. Cliquez sur l'onglet **Privilèges** à droite.

Résultats

Vous pouvez faire défiler la liste pour afficher les privilèges accordés au rôle sélectionné. Pour afficher une liste détaillée de tous les privilèges de vSphere, reportez-vous à la section Privilèges définis.

Privilèges de CloudAdmin

Comme VMware effectue l'administration des hôtes et d'autres tâches, les administrateurs cloud n'ont pas besoin d'autant de privilèges que les administrateurs d'un centre de données sur site.

Le rôle CloudAdmin dispose d'un ensemble de privilèges généré de manière dynamique pour votre SDDC. Cet ensemble inclut la plupart des privilèges disponibles dans toutes les catégories. Pour afficher les privilèges accordés au rôle CloudAdmin, connectez-vous à vSphere Client dans le SDDC, cliquez sur **Administration > Rôles**, sélectionnez CloudAdmin dans la liste des rôles, puis cliquez sur **PRIVILÈGES**.

Vous pouvez également utiliser un extrait de code PowerShell tel que celui-ci pour récupérer la liste des privilèges du rôle CloudAdmin dans votre SDDC.

```
$vmcUserName = "CloudAdmin"

$authMgr = Get-View $global:DefaultVIServer.ExtensionData.Content.AuthorizationManager

Write-Host "vCenter Version: $($global:DefaultVIServer.ExtensionData.Content.About.Version)"
Write-Host "Build: $($global:DefaultVIServer.ExtensionData.Content.About.Build)"

($authMgr.RoleList | where {$_.Name -eq $vmcUserName}).Privilege
```

Le rôle CloudAdmin dispose des privilèges suivants dans SDDC version 1.18.

```
vCenter Version: 7.0.3, Build: 19584923
Alarm.Acknowledge
Alarm.Create
Alarm.Delete
Alarm.DisableActions
Alarm.Edit
Alarm.SetStatus
Authorization.ModifyPermissions
Authorization.ModifyRoles
CertificateManagement.Manage
Cns.Searchable
ComputePolicy.Manage
ContentLibrary.AddCertToTrustStore
ContentLibrary.AddLibraryItem
ContentLibrary.CheckInTemplate
ContentLibrary.CheckOutTemplate
ContentLibrary.CreateLocalLibrary
ContentLibrary.CreateSubscribedLibrary
ContentLibrary.DeleteCertFromTrustStore
ContentLibrary.DeleteLibraryItem
ContentLibrary.DeleteLocalLibrary
ContentLibrary.DeleteSubscribedLibrary
ContentLibrary.DownloadSession
ContentLibrary.EvictLibraryItem
ContentLibrary.EvictSubscribedLibrary
ContentLibrary.GetConfiguration
ContentLibrary.ImportStorage
ContentLibrary.ProbeSubscription
ContentLibrary.ReadStorage
ContentLibrary.SyncLibrary
ContentLibrary.SyncLibraryItem
ContentLibrary.TypeIntrospection
ContentLibrary.UpdateConfiguration
ContentLibrary.UpdateLibrary
ContentLibrary.UpdateLibraryItem
ContentLibrary.UpdateLocalLibrary
ContentLibrary.UpdateSession
ContentLibrary.UpdateSubscribedLibrary
Datastore.AllocateSpace
Datastore.Browse
```

```
Datastore.Config
Datastore.DeleteFile
Datastore.FileManagement
Datastore.UpdateVirtualMachineFiles
Datastore.UpdateVirtualMachineMetadata
Extension.Register
Extension.Unregister
Extension.Update
Folder.Create
Folder.Delete
Folder.Move
Folder.Rename
Global.CancelTask
Global.GlobalTag
Global.Health
Global.LogEvent
Global.ManageCustomFields
Global.ServiceManagers
Global.SetCustomField
Global.SystemTag
HLM.Manage
Host.Hbr.HbrManagement
InventoryService.Tagging.AttachTag
InventoryService.Tagging.CreateCategory
InventoryService.Tagging.CreateTag
InventoryService.Tagging.DeleteCategory
InventoryService.Tagging.DeleteTag
InventoryService.Tagging.EditCategory
InventoryService.Tagging.EditTag
InventoryService.Tagging.ModifyUsedByForCategory
InventoryService.Tagging.ModifyUsedByForTag
InventoryService.Tagging.ObjectAttachable
Namespaces.Configure
Namespaces.SelfServiceManage
Network.Assign
Resource.ApplyRecommendation
Resource.AssignVAppToPool
Resource.AssignVMToPool
Resource.ColdMigrate
Resource.CreatePool
Resource.DeletePool
Resource.EditPool
Resource.HotMigrate
Resource.MovePool
Resource.QueryVMotion
Resource.RenamePool
ScheduledTask.Create
ScheduledTask.Delete
ScheduledTask.Edit
ScheduledTask.Run
Sessions.GlobalMessage
Sessions.ValidateSession
StorageProfile.Update
StorageProfile.View
StorageViews.View
```

```
System.Anonymous
System.Read
System.View
Trust.Manage
VApp.ApplicationConfig
VApp.AssignResourcePool
VApp.AssignVApp
VApp.AssignVM
VApp.Clone
VApp.Create
VApp.Delete
VApp.Export
VApp.ExtractOvfEnvironment
VApp.Import
VApp.InstanceConfig
VApp.ManagedByConfig
VApp.Move
VApp.PowerOff
VApp.PowerOn
VApp.Rename
VApp.ResourceConfig
VApp.Suspend
VApp.Unregister
VirtualMachine.Config.AddExistingDisk
VirtualMachine.Config.AddNewDisk
VirtualMachine.Config.AddRemoveDevice
VirtualMachine.Config.AdvancedConfig
VirtualMachine.Config.Annotation
VirtualMachine.Config.CPUCount
VirtualMachine.Config.ChangeTracking
VirtualMachine.Config.DiskExtend
VirtualMachine.Config.DiskLease
VirtualMachine.Config.EditDevice
VirtualMachine.Config.HostUSBDevice
VirtualMachine.Config.ManagedBy
VirtualMachine.Config.Memory
VirtualMachine.Config.MksControl
VirtualMachine.Config.QueryFTCompatibility
VirtualMachine.Config.QueryUnownedFiles
VirtualMachine.Config.RawDevice
VirtualMachine.Config.ReloadFromPath
VirtualMachine.Config.RemoveDisk
VirtualMachine.Config.Rename
VirtualMachine.Config.ResetGuestInfo
VirtualMachine.Config.Resource
VirtualMachine.Config.Settings
VirtualMachine.Config.SwapPlacement
VirtualMachine.Config.UpgradeVirtualHardware
VirtualMachine.GuestOperations.Execute
VirtualMachine.GuestOperations.Modify
VirtualMachine.GuestOperations.ModifyAliases
VirtualMachine.GuestOperations.Query
VirtualMachine.GuestOperations.QueryAliases
VirtualMachine.Hbr.ConfigureReplication
VirtualMachine.Hbr.MonitorReplication
```

```
VirtualMachine.Hbr.ReplicaManagement
VirtualMachine.Interact.AnswerQuestion
VirtualMachine.Interact.Backup
VirtualMachine.Interact.ConsoleInteract
VirtualMachine.Interact.CreateScreenshot
VirtualMachine.Interact.DefragmentAllDisks
VirtualMachine.Interact.DeviceConnection
VirtualMachine.Interact.DnD
VirtualMachine.Interact.GuestControl
VirtualMachine.Interact.Pause
VirtualMachine.Interact.PowerOff
VirtualMachine.Interact.PowerOn
VirtualMachine.Interact.PutUsbScanCodes
VirtualMachine.Interact.Reset
VirtualMachine.Interact.SESparseMaintenance
VirtualMachine.Interact.SetCDMedia
VirtualMachine.Interact.SetFloppyMedia
VirtualMachine.Interact.Suspend
VirtualMachine.Interact.ToolsInstall
VirtualMachine.Inventory.Create
VirtualMachine.Inventory.CreateFromExisting
VirtualMachine.Inventory.Delete
VirtualMachine.Inventory.Move
VirtualMachine.Inventory.Register
VirtualMachine.Inventory.Unregister
VirtualMachine.Namespace.Event
VirtualMachine.Namespace.EventNotify
VirtualMachine.Namespace.Management
VirtualMachine.Namespace.ModifyContent
VirtualMachine.Namespace.Query
VirtualMachine.Namespace.ReadContent
VirtualMachine.Provisioning.Clone
VirtualMachine.Provisioning.CloneTemplate
VirtualMachine.Provisioning.CreateTemplateFromVM
VirtualMachine.Provisioning.Customize
VirtualMachine.Provisioning.DeployTemplate
VirtualMachine.Provisioning.DiskRandomAccess
VirtualMachine.Provisioning.DiskRandomRead
VirtualMachine.Provisioning.FileRandomAccess
VirtualMachine.Provisioning.GetVmFiles
VirtualMachine.Provisioning.MarkAsTemplate
VirtualMachine.Provisioning.MarkAsVM
VirtualMachine.Provisioning.ModifyCustSpecs
VirtualMachine.Provisioning.PromoteDisks
VirtualMachine.Provisioning.PutVmFiles
VirtualMachine.Provisioning.ReadCustSpecs
VirtualMachine.State.CreateSnapshot
VirtualMachine.State.RemoveSnapshot
VirtualMachine.State.RenameSnapshot
VirtualMachine.State.RevertToSnapshot
VirtualMachineClasses.Manage
Vsan.Cluster.ShallowRekey
vService.CreateDependency
vService.DestroyDependency
```

```
vService.ReconfigureDependency
vService.UpdateDependency
vSphereDataProtection.Protection
vSphereDataProtection.Recovery
```

Pour plus d'informations sur les autorisations accordées par chaque privilège, reportez-vous à la référence Privilèges définis de vSphere.

Fédération d'entreprise avec VMware Cloud Services

Les propriétaires d'organisation VMware Cloud on AWS peuvent tirer parti de la fédération d'entreprise avec VMware Cloud Services pour limiter l'accès à Console VMware Cloud aux comptes qui se connectent à VMware Cloud Services avec une identité fédérée.

À l'instar de la plupart des autres instances de VMware Cloud Services, VMware Cloud on AWS peut être configuré pour appliquer un ensemble unique d'identités dont les informations d'identification sont gérées via votre fournisseur d'identité d'entreprise basé sur SAML 2.0. Le workflow en libre-service pour la configuration de la fédération d'entreprise est décrit en détail dans la section Qu'est-ce que la fédération d'entreprise et comment fonctionne-t-elle ? et l'article 76201 de la base de connaissances de VMware.

Activer la connexion fédérée pour vCenter

La fédération de vCenter active Single Sign-On (SSO) afin que les utilisateurs puissent s'authentifier en toute sécurité sur leur SDDC vCenter Server sans avoir à entrer de nouveau leurs informations d'identification.

Lorsque vous activez la fonctionnalité de fédération vCenter dans votre SDDC, VMware Cloud on AWS remplace tous les fournisseurs d'identité externes (en utilisant le type de source AD sur LDAP et LDAP natif) par les fournisseurs d'identité (IDP) fédérés avec votre organisation VMware Cloud Services (avec le type source SSO). Le changement de fournisseurs d'identité modifie les moyens d'authentification, mais ne modifie en aucune manière l'autorisation. Aucun utilisateur ou groupe supplémentaire n'est autorisé à accéder à votre instance de vCenter Server.

Après avoir activé la connexion fédérée dans votre SDDC, vous pouvez constater quelques modifications comportementales dans votre SDDC vCenter Server :

- Message « Cette instance de vCenter est gérée par VMware Cloud Services » lors de l'affichage du **Fournisseur d'identité** dans la section **Single Sign-On > Configuration** de l'administration de vCenter. Cela est dû au fait qu'une fois la connexion fédérée activée, vCenter Single Sign-On est géré uniquement par VMware Cloud Services.
- Échecs d'activation pour les automatisations et les intégrations tierces. Si votre fournisseur d'identité ne prend pas en charge le recours à l'authentification par mot de passe ou requiert une authentification multifacteur, l'intégration par programme à vCenter échouera à l'étape d'authentification.

L'activation de la fédération modifie la source d'identité (authentification), mais n'a pas d'incidence sur les utilisateurs et les autorisations (autorisation). Le workflow supprime votre source d'identité LDAP et ajoute une source d'identité SSO.

La fédération de vCenter repose sur VMware Cloud Services pour activer SSO. Toute maintenance ou panne sur VMware Cloud Services peut affecter la disponibilité de SSO pour vCenter. Reportez-vous à Accès d'urgence à vCenter en cas d'échec de la connexion fédérée pour obtenir l'URL d'accès d'urgence et des instructions.

Si vous avez activé la connexion fédérée et que vous devez modifier votre source d'identité SSO ou en ajouter une nouvelle, vous devez configurer la fédération d'entreprise pour la nouvelle source d'identité SSO, puis désactiver et réactiver la connexion fédérée afin que votre instance de vCenter Server SDDC reconnaisse la nouvelle source d'identité, puis configure les autorisations pour la nouvelle source d'identité.

Pour plus d'informations sur la connexion fédérée, reportez-vous à l'article de la zone technique de VMware Cloud Présentation de la fonctionnalité : connexion fédérée de vCenter pour VMware Cloud on AWS.

Conditions préalables

- **Important** La fédération de vCenter ne prend pas en charge l'utilisation simultanée de sources d'identité SSO et AD/LDAP. Si vous disposez de plusieurs sources d'identité LDAP configurées dans vCenter et que vous devez authentifier les utilisateurs de ces domaines après avoir activé la connexion fédérée pour vCenter, les domaines doivent tous remplir les conditions préalables suivantes :

  Vous ne devez pas activer la connexion fédérée pour vCenter dans un SDDC configuré pour le renforcement de la conformité. Pour plus d'informations sur l'utilisation de cette configuration et ce dont elle a besoin, reportez-vous à la section Configurer le renforcement de la conformité du SDDC.

- Enregistrez votre configuration de source d'identité LDAP actuelle. Vous devrez restaurer manuellement cette configuration si vous décidez de désactiver la connexion fédérée à vCenter.
- Activez la fédération d'entreprise pour tous les domaines qui requièrent un accès à vCenter. Reportez-vous à la section Qu'est-ce que la fédération d'entreprise et comment fonctionne-t-elle ?
- Liez votre fournisseur d'identité à votre organisation VMware Cloud Services. Consultez la section Pourquoi faut-il lier mon fournisseur d'identité ?
- Désactiver la connexion fédérée pour vCenter

  La désactivation de la connexion fédérée pour vCenter n'est pas un workflow courant.

- Accès d'urgence à vCenter en cas d'échec de la connexion fédérée

  Si vous ne pouvez pas accéder à vCenter à l'aide de vos informations d'identification VMware Cloud Services dans un SDDC sur lequel la connexion fédérée a été activée, vous pouvez utiliser l'URL d'**Accès d'urgence à vCenter** sur la page **Paramètres** de votre SDDC.

Procédure

1. Connectez-vous à VMware Cloud Services à l'adresse https://vmc.vmware.com.

   Vous devez disposer du rôle VMware Cloud on AWS Administrateur pour activer la connexion fédérée pour vCenter.
2. Cliquez sur **Inventaire > SDDC**, puis choisissez une carte SDDC et cliquez sur **AFFICHER LES DÉTAILS**.
3. Ouvrez l'onglet **Paramètres** du SDDC.
4. Accédez à **Connexion fédérée** dans la section **Informations sur le système vCenter**, puis cliquez sur **ACTIVER**.

   Examinez les conditions préalables, puis cliquez sur **ACTIVER** lorsque vous êtes prêt à continuer. L'activation requiert VMware Cloud on AWS pour importer des données à partir de votre fournisseur d'identité fédéré. Le temps nécessaire pour terminer l'activation dépend de la quantité de données importées et de la bande passante réseau disponible.

Résultats

Une fois l'activation terminée, l'écran de connexion à vSphere Client demande aux utilisateurs de se connecter avec VMware Cloud Services.

Étape suivante

S'il s'agit d'un nouveau SDDC et qu'il n'a jamais activé la connexion fédérée, connectez-vous au SDDC vCenter Server à l'URL d'accès d'urgence en utilisant l'adresse cloudadmin@vmc.local et configurez les autorisations du domaine SSO. Si vous ne le faites pas, l'URL d'accès d'urgence ne fournira pas l'accès d'urgence.

Désactiver la connexion fédérée pour vCenter

La désactivation de la connexion fédérée pour vCenter n'est pas un workflow courant.

La connexion fédérée pour vCenter a été conçue pour remplacer à long terme le workflow de connexion de vCenter Server par défaut dans VMware Cloud on AWS. Vous devez désactiver la connexion fédérée pour vCenter si vous devez Configurer le renforcement de la conformité du SDDC dans un SDDC dans lequel elle a été activée. La désactivation de la connexion fédérée pour vCenter vous oblige à reconfigurer tous les paramètres Active Directory sur LDAP que vous souhaitez restaurer dans vCenter.

Procédure

1 Connectez-vous à VMware Cloud Services à l'adresse https://vmc.vmware.com.

   Vous devez disposer du rôle VMware Cloud Services Propriétaire d'organisation pour exécuter ce flux de travail.

2 Cliquez sur **Inventaire > SDDC**, puis choisissez une carte SDDC et cliquez sur **AFFICHER LES DÉTAILS**.

3 Ouvrez l'onglet **Paramètres** du SDDC.

4 Accédez à **Connexion fédérée** dans la section **Informations sur le système vCenter**. Vérifiez que la fonctionnalité est **Activée**, puis cliquez sur **DÉSACTIVER**.

   Vous pouvez cliquer sur **ACCÈS D'URGENCE À VCENTER** si vous souhaitez essayer l'accès d'urgence avant de désactiver la connexion fédérée. Si vous souhaitez toujours désactiver la connexion fédérée, confirmez que vous comprenez que vous allez devoir reconfigurer vos paramètres Active Directory via LDAP à la fin de la désactivation, puis cliquez sur **DÉSACTIVER**.

   Un message « Désactivation de la connexion fédérée pour vCenter » s'affiche lorsque la désactivation est en cours. Lorsque la fonctionnalité a été désactivée, le bouton **DÉSACTIVER** sous **Connexion fédérée** dans la section **Informations sur le système vCenter** passe à **ACTIVER**, et vSphere Client redemande une identité vmc.local.

Étape suivante

Une fois le workflow Désactiver la connexion fédérée terminé, reconfigurez les paramètres Active Directory sur LDAP pour cette organisation. Suivez les procédures décrites dans la section Ajouter ou modifier une source d'identité vCenter Single Sign-On pour restaurer la configuration qui était en place avant la configuration du SDDC pour la fédération d'entreprise.

Accès d'urgence à vCenter en cas d'échec de la connexion fédérée

Si vous ne pouvez pas accéder à vCenter à l'aide de vos informations d'identification VMware Cloud Services dans un SDDC sur lequel la connexion fédérée a été activée, vous pouvez utiliser l'URL d'**Accès d'urgence à vCenter** sur la page **Paramètres** de votre SDDC.

La connexion fédérée dépend de la configuration de la fédération d'entreprise de votre SDDC et requiert un accès réseau à votre fournisseur d'identité. Si l'une de ces dépendances rencontre une erreur qui vous empêche de vous connecter à vCenter à l'aide de vos informations d'identification VMware Cloud Services, vous pouvez utiliser l'URL d'**Accès d'urgence à vCenter** (`vcenter-url/ui/?idp=local`) pour vous connecter à un compte vmc.local, tel que cloudadmin@vmc.local.

Procédure

1 Connectez-vous à VMware Cloud Services à l'adresse https://vmc.vmware.com.

   Vous devez disposer du rôle VMware Cloud Services Propriétaire d'organisation pour exécuter ce flux de travail.

2 Cliquez sur **Inventaire > SDDC**, puis choisissez une carte SDDC et cliquez sur **AFFICHER LES DÉTAILS**.

3 Ouvrez l'onglet **Paramètres** du SDDC.

4 Accédez à **Accès d'urgence à vCenter** dans la section **Informations sur le système vCenter**, puis cliquez sur **URL d'accès d'urgence** pour ouvrir vSphere Client. Vous pouvez vous connecter en tant que cloudadmin@vmc.local ou tout autre compte vmc.local. Le mot de passe par défaut de cloudadmin@vmc.local, stocké dans Console VMware Cloud lors de la création du SDDC, n'est pas mis à jour si un administrateur vSphere le modifie. Reportez-vous à la section Impossible de copier le mot de passe modifié dans la page de connexion vCenter.

Configuration d'Hybrid Linked Mode

Hybrid Linked Mode vous permet de lier votre instance de cloud de vCenter Server à un domaine vCenter Single Sign-On sur site.

Important Avant de pouvoir utiliser Hybrid Linked Mode, vous devez configurer votre instance de vCenter sur site pour activer le Single Sign-On. Pour plus d'informations, consultez Authentification vSphere à l'aide de vCenter Single Sign-On.

Si vous liez votre vCenter Server de cloud à un domaine qui contient plusieurs instances de vCenter Server liées à l'aide d'Enhanced Linked Mode, toutes ces instances sont liées à votre SDDC de cloud.

À l'aide d'Hybrid Linked Mode, vous pouvez :

- Afficher et gérer les inventaires de vos centres de données sur site et dans le cloud à partir d'une seule interface vSphere Client accessible à l'aide de vos informations d'identification sur site.
- Migrer des charges de travail entre votre centre de données sur site et votre SDDC de cloud.
- Partager des balises et des catégories de balises à partir de votre instance de vCenter Server vers votre SDDC de cloud.

Hybrid Linked Mode prend en charge les systèmes vCenter Server sur site avec des systèmes Platform Services Controller intégrés ou externes (Windows et vCenter Server Appliance). Les systèmes vCenter Server avec des instances Platform Services Controller externes liées en mode Enhanced Linked Mode sont également pris en charge, jusqu'aux limites d'échelle fournies dans Valeurs maximales de configuration pour vSphere.

Vous avez deux options pour la configuration de Hybrid Linked Mode. Vous pouvez utiliser seulement une de ces options à la fois.

- Vous pouvez installer VMware Cloud Gateway et l'utiliser pour lier votre centre de données sur site à votre SDDC de cloud. Dans ce cas, les utilisateurs et les groupes SSO sont mappés depuis votre environnement sur site vers le SDDC et vous n'avez pas besoin d'ajouter une source d'identité au domaine LDAP du SDDC.

- Vous pouvez lier votre SDDC de cloud à votre instance de vCenter Server sur site. Dans ce cas, vous devez ajouter une source d'identité au domaine LDAP du SDDC.

Conditions préalables de Hybrid Linked Mode

Assurez-vous que vous respectez les conditions préalables suivantes avant de configurer Hybrid Linked Mode.

Conditions préalables communes

Les conditions préalables suivantes sont communes à la liaison depuis VMware Cloud Gateway et depuis le SDDC de cloud.

- Configurez une connexion entre votre centre de données sur site et le SDDC. Selon le service fournissant votre SDDC, vous pouvez être en mesure d'utiliser Direct Connect, un VPN ou les deux. Pour plus d'informations, reportez-vous à la documentation de mise en réseau de votre service.
- Quel que soit le type de connexion que vous choisissez, le nom de domaine complet de vCenter doit être résolu en adresse IP privée. Il ne s'agit pas de la configuration par défaut. Pour plus d'informations, reportez-vous à Définir l'adresse de résolution de nom de domaine complet de vCenter Server.
- Vérifiez que votre centre de données sur site et votre SDDC de cloud sont synchronisés sur un service NTP ou une autre source d'heure fiable. Le mode Hybrid Linked Mode peut tolérer un décalage horaire entre le centre de données sur site et le SDDC de cloud de dix minutes au maximum.
- La latence maximale entre votre SDDC de cloud et le centre de données sur site ne peut pas dépasser 100 ms A/R.
- Décidez quels utilisateurs de votre site disposeront des autorisations d'administrateur cloud. Ajoutez ces utilisateurs à un groupe au sein de votre source d'identité. Assurez-vous que ce groupe dispose d'un accès à votre environnement sur site.

Conditions préalables pour la liaison avec VMware Cloud Gateway

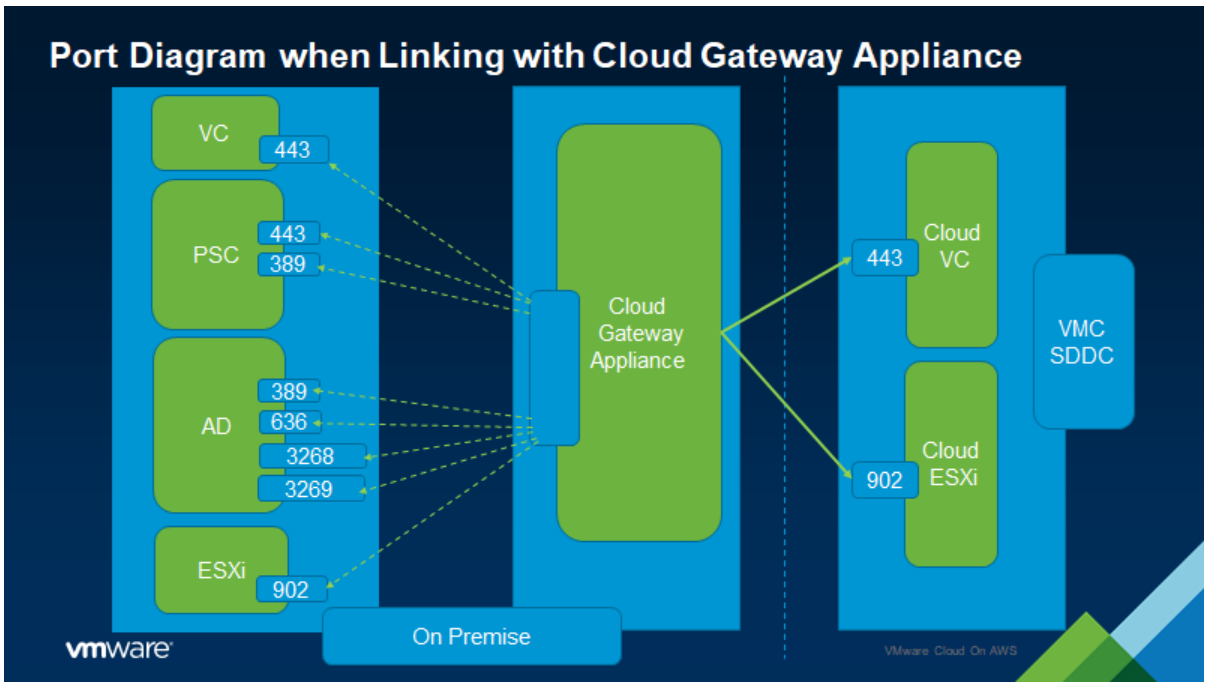
Les conditions préalables suivantes s'appliquent lors de la liaison avec VMware Cloud Gateway.

- Installez VMware Cloud Gateway. Reportez-vous à la section Installation et configuration de VMware Cloud Gateway.
- Votre environnement sur site doit exécuter vSphere 6.5 correctif d ou une version ultérieure.

- Pour vous assurer que les instances de VMware Cloud Gateway et de vCenter Server peuvent se joindre sur votre réseau, vérifiez que les ports de pare-feu suivants sont ouverts.

Source	Destination	Port	Objectif
Navigateur Web de l'utilisateur	VMware Cloud Gateway	5480	Générer un bundle de support
VMware Cloud Gateway	vCenter Server sur site	7444	Accéder à VMware Single Sign-On
VMware Cloud Gateway	vCenter Server sur site	443	Hybrid Linked Mode
VMware Cloud Gateway	Platform Services Controller sur site	443, 389	Hybrid Linked Mode
VMware Cloud Gateway	SDDC de cloud vCenter Server	443	Hybrid Linked Mode
VMware Cloud Gateway	Hôte ESXi de cloud	902	Console de machine virtuelle
VMware Cloud Gateway	Serveur Active Directory sur site (ports dépendant de votre utilisation)	389, 636, 3268, 3269	Source d'identité
VMware Cloud Gateway	https://vcgw-updates.vmware.com/	443	Liaison en mode Hybrid Linked Mode, mise à jour automatique de la passerelle de cloud

La figure suivante montre les ports qui doivent être ouverts pour la liaison avec le dispositif VMware Cloud Gateway.



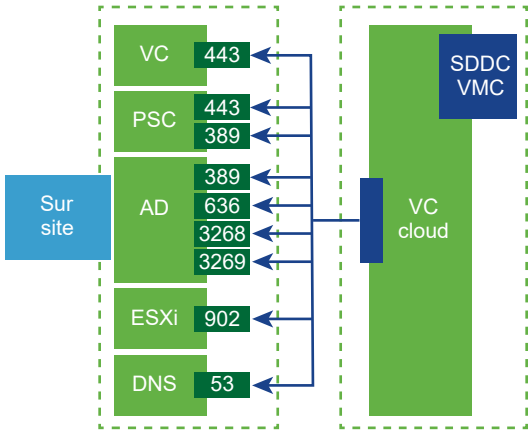
Conditions préalables pour la liaison depuis le SDDC de cloud

Les conditions préalables suivantes s'appliquent lors de la liaison depuis le SDDC de cloud.

- Votre système vCenter Server sur site exécute l'un des éléments suivants :
  - vSphere 6.0 Update 3 patch c et versions ultérieures.
  - vSphere 6.5 patch d et versions ultérieures.
- Assurez-vous d'avoir les informations d'identification de votre domaine SSO vSphere sur site.
- Vérifiez que vous disposez des informations d'identification pour un utilisateur disposant au moins d'un accès en lecture seule au nom unique de base pour les utilisateurs et les groupes de votre environnement sur site. Ceci est utilisé lors de l'ajout d'une source d'identité.
- Assurez-vous qu'un serveur DNS sur site est configuré pour votre passerelle de gestion afin qu'il puisse résoudre le nom de domaine complet de la source d'identité et des systèmes sur site.
- Assurez-vous que votre passerelle sur site ou pare-feu autorise l'accès aux ports nécessaires à partir de votre SDDC pour les services suivants.

Source	Destination	Ports	Objectif
SDDC de cloud	vCenter Server sur site	443	Hybrid Linked Mode
SDDC de cloud	Platform Services Controller sur site	389, 443	Hybrid Linked Mode
SDDC de cloud	Serveur Active Directory sur site (ports dépendant de votre utilisation)	389, 636, 3268, 3269	Source d'identité
SDDC de cloud	DNS sur site	53	Résolution du nom de domaine complet de vCenter Server sur site et du serveur Active Directory
SDDC de cloud	Hôte ESXi sur site	902	Console de machine virtuelle

La figure suivante montre les ports qui doivent être ouverts pour la liaison avec le SDDC de cloud.



- Si vous établissez une liaison vers une instance de vCenter Server sur site connectée à d'autres instances de vCenter Server sur site avec Enhanced Linked Mode, votre SDDC de cloud doit disposer d'une connectivité réseau à toutes les instances de vCenter Server sur site, pas seulement à celle avec laquelle vous établissez la liaison directe.
- Exécutez les tests du validateur de connectivité pour vérifier que la connectivité réseau est correctement établie pour Hybrid Linked Mode. Reportez-vous à la section Valider la connectivité réseau pour Hybrid Linked Mode.

Configuration de Hybrid Linked Mode à l'aide du dispositif VMware Cloud Gateway

Configurez VMware Cloud Gateway pour activer le mode Hybrid Linked Mode depuis votre environnement sur site.

Dans ce cas, vous vous connectez à VMware Cloud Gateway pour afficher et gérer à la fois vos environnements sur site et de cloud.

Pour plus d'informations, reportez-vous à la section Configuration de Hybrid Linked Mode à l'aide de VMware Cloud Gateway Appliance dans le document *Administration de VMware Cloud Gateway*.

Que lire ensuite ?

- Lier le dispositif VMware Cloud Gateway à votre SDDC cloud

  Utilisez cette procédure pour lier le dispositif VMware Cloud Gateway à votre SDDC de cloud à l'aide du mode Hybrid Linked Mode.
- Remplacer le certificat pour le dispositif VMware Cloud Gateway avec le mode Hybrid Linked Mode activé

  Vous pouvez remplacer le certificat du dispositif VMware Cloud Gateway lorsqu'il expire ou lorsque vous souhaitez utiliser un certificat d'un autre fournisseur de certificats.

Lier le dispositif VMware Cloud Gateway à votre SDDC cloud

Utilisez cette procédure pour lier le dispositif VMware Cloud Gateway à votre SDDC de cloud à l'aide du mode Hybrid Linked Mode.

Conditions préalables

- Vous devez disposer des privilèges d'administrateur dans votre environnement sur site pour effectuer cette tâche.

Procédure

1. Dans un navigateur Web, accédez à https://*gw-address*:5480/gw-platform/ où *gw-address* est l'adresse IP ou le nom de domaine complet du dispositif.
2. Sur la carte **Gestion hybride**, cliquez sur **Démarrer**.
3. Connectez-vous avec vos informations d'identification VMware Cloud Gateway.
4. Entrez les informations d'identification pour vCenter Server de cloud.

Option	Description
vCenter Server	Entrez le nom de domaine complet de l'instance de vCenter Server dans votre SDDC de cloud.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'administrateur cloud.
Mot de passe	Entrez le mot de passe de l'administrateur cloud.

5. Entrez vos paramètres SSO sur site.

Option	Description
Platform Services Controller	Entrez l'adresse IP ou le nom de domaine complet de l'instance de Platform Services Controller dans votre environnement sur site.
Port HTTPS	Entrez le port HTTPS utilisé par l'instance de Platform Services Controller.
Nom d'utilisateur Single Sign-On	Le nom d'utilisateur de l'administrateur Single Sign-On est « administrator ». L'application détermine le nom de domaine correct.
Mot de passe Single Sign-On	Entrez le mot de passe de l'administrateur Single Sign-On.

La configuration SSO dure environ 2 à 3 minutes.

6 Indiquez si vous souhaitez joindre VMware Cloud Gateway au domaine Active Directory.

Option	Description
Ignorer	Si vous utilisez Active Directory avec LDAP et que votre serveur Active Directory est déjà joint au vCenter Server sur site, sélectionnez **Ignorer** pour ignorer cette étape du processus. Si votre serveur Active Directory n'est pas joint au vCenter Server sur site ou si votre serveur Active Directory utilise IWA (qu'il soit joint ou non au vCenter Server sur site), sélectionnez **Joindre**.
Joindre	Entrez les paramètres suivants : a Dans la zone de texte **Domaine**, entrez un nom de domaine Active Directory. Par exemple, mydomain.com. b Dans la zone de texte **Unité d'organisation**, spécifiez éventuellement le nom de domaine complet LDAP de l'unité d'organisation. Par exemple, OU=Engineering,DC=mydomain,DC=com. c Dans la zone de texte **Nom d'utilisateur**, entrez le nom d'utilisateur de l'administrateur Active Directory au format UPN (User Principal Name, nom d'utilisateur principal). Par exemple, example@mydomain.com. d Dans le champ **Mot de passe**, entrez le mot de passe de l'administrateur Active Directory. Si votre serveur Active Directory utilise IWA, cliquez sur **Redémarrer la passerelle**. Après le redémarrage du dispositif, cliquez sur **Démarrer** sur la carte **Multi-vCenter Connect** et connectez-vous à nouveau avant de poursuivre.

7 Ajoutez les groupes que vous avez définis dans votre environnement sur site pour les utiliser comme groupes d'administrateurs cloud.

a Sélectionnez la source d'identité sur site.

b Entrez le nom du groupe d'administrateurs dans la zone de recherche et sélectionnez le groupe.

8 Cliquez sur **Configurer**.

Le processus de liaison peut prendre quelques minutes.

Étape suivante

Une fois le processus de liaison terminé, choisissez l'une des opérations suivantes :

- Cliquez sur **Lancer vSphere Client** pour afficher et gérer vos SDDC sur site et de cloud.

- Cliquez sur **Revenir à la passerelle de cloud** pour revenir à l'interface utilisateur de gestion de la passerelle de cloud.

Note La liaison depuis VMware Cloud Gateway accorde au(x) groupe(s) AD sélectionné(s) l'accès Administrateur cloud au SDDC. Si vous souhaitez configurer un utilisateur ou un groupe avec un niveau d'accès inférieur, vous devez ajouter la source d'identité directement à votre SDDC comme décrit dans Ajouter une source d'identité au domaine LDAP du SDDC.

Après avoir ajouté la source d'identité au SDDC, vous devez attribuer les autorisations que vous souhaitez accorder aux utilisateurs et/ou aux groupes, comme décrit dans la section Ajouter une autorisation à un objet d'inventaire. Une fois la source d'identité configurée dans le SDDC, les autorisations de l'utilisateur sont basées uniquement sur ce qui est configuré dans le SDDC. Si vous ne configurez pas les autorisations pour ces utilisateurs dans le SDDC, ces derniers rencontreront des problèmes lors de l'affichage de l'inventaire du SDDC depuis l'interface utilisateur de vSphere Client sur le VMware Cloud Gateway.

Remplacer le certificat pour le dispositif VMware Cloud Gateway avec le mode Hybrid Linked Mode activé

Vous pouvez remplacer le certificat du dispositif VMware Cloud Gateway lorsqu'il expire ou lorsque vous souhaitez utiliser un certificat d'un autre fournisseur de certificats.

Conditions préalables

Utilisez cette méthode pour remplacer le certificat uniquement après l'activation de Hybrid Linked Mode. Si vous devez remplacer le certificat sur un dispositif VMware Cloud Gateway sur lequel le mode Hybrid Linked Mode n'est pas activé, reportez-vous à la section Remplacer le certificat de VMware Cloud Gateway.

Générez des demandes de signature de certificat (CSR, Certificate Signing Request) pour chaque certificat que vous souhaitez remplacer. Fournissez la demande de signature de certificat à votre autorité de certification. Lorsque l'autorité de certification renvoie le certificat, placez-le dans un emplacement accessible à partir du dispositif VMware Cloud Gateway.

Procédure

1. Dans un navigateur Web, accédez à http://*adresse-cga*/ui où *adresse-cga* est l'adresse IP ou le nom de domaine complet de VMware Cloud Gateway.
2. Connectez-vous avec vos informations d'identification sur site.
3. Accédez à l'interface utilisateur de gestion de certificat.
   a. Dans le menu **Accueil**, sélectionnez **Administration**.
   b. Sous **Certificats**, cliquez sur **Gestion des certificats**.
4. Entrez vos informations d'identification et cliquez sur **Se connecter et gérer les certificats**.
5. Sur le certificat SSL de la machine, sélectionnez **Actions > Remplacer**.

6 Cliquez sur le bouton Parcourir de la chaîne de certificats et fournissez le chemin d'accès au fichier de chaîne de certificats.

   Ce fichier doit contenir le certificat SSL de la machine, le certificat de l'autorité de certification racine et l'intégralité de la chaîne d'approbation.

7 Cliquez sur le bouton Parcourir sur la clé privée et fournissez la clé privée du certificat.

8 Cliquez sur **Remplacer**.

Étape suivante

Une fois le certificat correctement remplacé, redémarrez tous les services sur le dispositif VMware Cloud Gateway. Reportez-vous à la section https://kb.vmware.com/s/article/2109887.

Configuration de Hybrid Linked Mode depuis le SDDC de cloud

Vous pouvez configurer Hybrid Linked Mode depuis le SDDC de cloud comme une alternative à l'utilisation de VMware Cloud Gateway.

Dans ce cas, vous utilisez l'instance de vSphere Client de votre SDDC de cloud pour afficher et gérer votre inventaire complet. Lorsque vous effectuez une liaison à partir du SDDC de cloud, vous ne pouvez lier qu'un seul domaine sur site.

Valider la connectivité réseau pour Hybrid Linked Mode

Le validateur de connectivité Console VMware Cloud permet de vérifier que l'ensemble de la connectivité réseau est en place pour Hybrid Linked Mode.

Lorsque vous fournissez les entrées requises au validateur de connectivité, il peut vérifier les connexions réseau requises pour Hybrid Linked Mode.

Procédure

1 Connectez-vous à la Console VMware Cloud à l'adresse https://vmc.vmware.com.

2 Cliquez sur **Afficher les détails** pour votre SDDC.

3 Cliquez sur l'onglet **Dépannage**.

4 Dans le menu déroulant **Cas d'utilisation**, sélectionnez **Hybrid Linked Mode**.

   Les tests de connectivité du mode Hybrid Linked Mode sont affichés. Les tests sont organisés en groupes en fonction de l'entrée nécessaire pour chaque groupe.

5 Dans la colonne **Entrée**, saisissez l'entrée requise pour chaque test que vous souhaitez exécuter.

6 Exécutez un ou plusieurs tests.

   - Pour exécuter tous les tests, cliquez sur **Exécuter tout**.
   - Pour exécuter un groupe de tests particulier, cliquez sur **Exécuter un groupe** à droite de la liste de groupes.

- Pour exécuter un test individuel, développez le groupe de tests et cliquez sur **Exécuter** en regard du test individuel.

Résultats

L'état de chaque test s'affiche au fur et à mesure de son exécution. Lorsqu'un test est terminé, vous pouvez le développer pour voir le détail de ses résultats.

Étape suivante

En cas de réussite de tous les tests, continuez à configurer Hybrid Linked Mode. Reportez-vous à la section Ajouter une source d'identité au domaine LDAP du SDDC.

Lier vers un centre de données sur site

Pour terminer la configuration du Hybrid Linked Mode depuis le SDDC de cloud, effectuez la liaison de votre centre de données sur site depuis votre vCenter Server en cloud.

Procédure

1. Si ce n'est déjà fait, connectez-vous à vSphere Client pour votre SDDC et accédez à la page Domaines liés.
   a. Sélectionnez **Menu > Administration** pour afficher la page Administration.
   b. Sous **Cloud hybride**, sélectionnez **Domaines liés**.
2. Connectez-vous à vCenter Server sur site.

Option	Description
Platform Services Controller	Entrez l'adresse IP ou le nom de domaine complet de l'instance de Platform Services Controller dans votre centre de données sur site.
Port HTTPS	Entrez le port HTTPS utilisé par Platform Services Controller.
Nom d'utilisateur	Entrez le nom d'utilisateur de l'administrateur SSO sur site.
Mot de passe	Entrez le mot de passe de l'administrateur SSO sur site.

3. Ajoutez les groupes que vous avez définis dans votre environnement sur site pour les utiliser comme groupes d'administrateurs cloud.
   a. Sélectionnez la source d'identité sur site.

      Si vous n'avez pas déjà ajouté la source d'identité sur site, suivez les instructions de Ajouter une source d'identité au domaine LDAP du SDDC.

   b. Entrez le nom du groupe d'administrateurs dans la zone de recherche et sélectionnez le groupe.
4. Cliquez sur **Lien**.

Ajouter une source d'identité au domaine LDAP du SDDC

La première étape de la configuration d'Hybrid Linked Mode depuis votre SDDC consiste à ajouter votre domaine LDAP sur site en tant que source d'identité pour l'instance de vCenter Server du SDDC.

Vous pouvez configurer Hybrid Linked Mode depuis votre SDDC si votre service LDAP sur site est fourni par un domaine Active Directory natif (authentification Windows intégrée) ou un service d'annuaire OpenLDAP.

Cette étape est facultative lors de la configuration du mode Hybrid Linked Mode à partir de VMware Cloud Gateway, mais l'ajout d'une source d'identité vous permet de configurer des utilisateurs ou des groupes avec un niveau d'accès inférieur à celui de l'administrateur de cloud.

Important Si vous utilisez OpenLDAP comme source d'identité, consultez l'article de la base de connaissances VMware accessible à l'adresse http://kb.vmware.com/kb/2064977 pour connaître les exigences supplémentaires.

Conditions préalables

Pour plus d'informations sur la configuration et l'utilisation des sources d'identité et des certificats, consultez la section Sources d'identité pour vCenter Server avec vCenter Single Sign-On dans la *documentation du produit VMware vSphere*.

Procédure

1. Connectez-vous à vSphere Client pour votre SDDC.

   Pour ajouter une source d'identité, vous devez être connecté en tant que cloudadmin@vmc.local ou un autre membre du groupe d'administrateurs Cloud.

2. Configurez Single Sign-on pour ajouter un fournisseur d'identité.

   Suivez les étapes décrites dans la section Ajouter ou modifier une source d'identité vCenter Single Sign-On de la *documentation du produit VMware vSphere*.

3. Configurez les paramètres de la source d'identité.

   Pour obtenir des informations détaillées sur les paramètres de configuration, reportez-vous à la section « Paramètres d'Active Directory sur LDAP et de la source d'identité du serveur OpenLDAP » dans Ajouter ou modifier une source d'identité vCenter Single Sign-On.

Résultats

Lorsque la source d'identité est ajoutée, les utilisateurs locaux peuvent s'authentifier sur le SDDC, mais disposent du rôle **Aucun accès**. Ajoutez des autorisations à un groupe d'utilisateurs pour leur accorder le rôle administrateur cloud.

Dépannage de la mise en réseau pour le mode Hybrid Linked Mode

Vous pouvez utiliser la fonctionnalité de dépannage réseau de la Console VMware Cloud ou la fonctionnalité faisant partie d'Hybrid Linked Mode dans VMware Cloud Gateway pour dépanner la connectivité réseau pour le mode Hybrid Linked Mode.

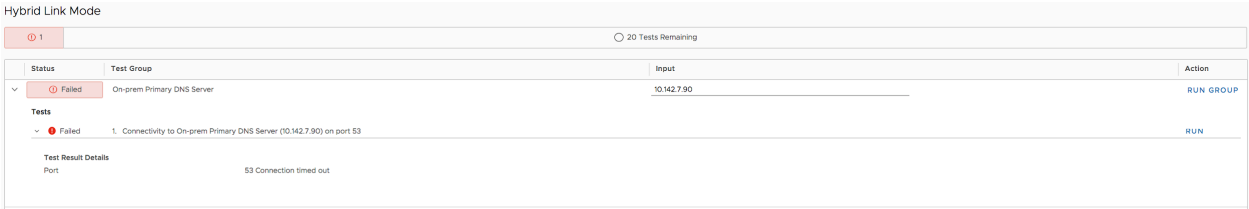
Validateur de connectivité : le serveur DNS est inaccessible.

Les tests du serveur DNS principal ou secondaire sur site échouent dans le validateur de connectivité.

Problème

Les tests **Connectivité au serveur DNS principal sur site sur le port 53** et/ou **Connectivité au serveur DNS secondaire sur site sur le port 53** dans le validateur de connectivité échouent avec un message indiquant que `la connexion au port 53 a expiré`.

Figure 1-1. Image d'un test de connectivité au serveur DNS ayant échoué



Cause

Les raisons de cet échec peuvent être les suivantes :

- La connexion VPN IPsec du SDDC de cloud vers le centre de données sur site ne fonctionne peut-être pas.
- Le port 53 du serveur DNS est bloqué par une règle de pare-feu sur le SDDC de cloud ou le centre de données sur site.
- Vous avez entré une adresse IP incorrecte pour le serveur DNS.
- Le serveur DNS est arrêté.

Solution

1. Vérifiez que le tunnel VPN du SDDC de cloud vers le serveur DNS sur site fonctionne. Reportez-vous à la section Afficher l'état et les statistiques du tunnel VPN.
2. Vérifiez les règles de pare-feu dans la Console VMware Cloud pour vous assurer que l'accès au port 53 sur le serveur DNS sur site n'est pas bloqué.
3. Vérifiez les règles de pare-feu dans votre environnement sur site pour vous assurer que l'accès au port 53 sur le serveur DNS sur site n'est pas bloqué.
4. Vérifiez que vous avez entré l'adresse IP correcte pour vos serveurs DNS sur site. Reportez-vous à la section Spécifier des serveurs DNS de passerelle de gestion.

5 Vérifiez que votre serveur DNS est en cours d'exécution ; si ce n'est pas le cas, exécutez-le.

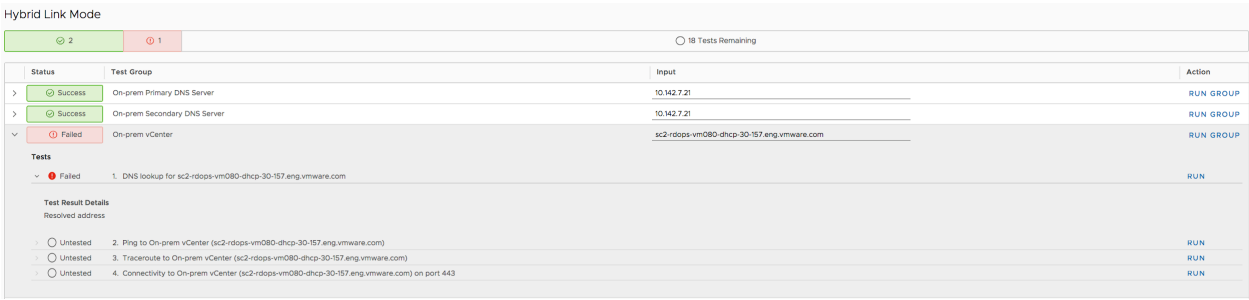
Validateur de connectivité : échec de la recherche DNS pour un nom de domaine complet donné

Le test de recherche DNS pour vCenter Server, Platform Services Controller, Active Directory, ou ESXi sur site échoue.

Problème

Un ou plusieurs tests de recherche DNS échouent. Le champ **Adresse résolue** dans les résultats du test n'affiche aucun résultat.

Figure 1-2. Exemple d'échec de test de recherche DNS



Cause

Si le test d'accessibilité au serveur DNS a réussi, mais que la recherche DNS pour un nom de domaine complet donné échoue, la raison peut être l'une des suivantes :

- Le serveur DNS sur site ne contient pas d'entrée pour le nom de domaine complet donné.
- Vous avez entré un nom de domaine complet incorrect pour le test.

Solution

1 Vérifiez que vous avez entré le nom de domaine complet correct.

2 Vérifiez que le serveur DNS sur site dispose d'une entrée pour le nom de domaine complet.

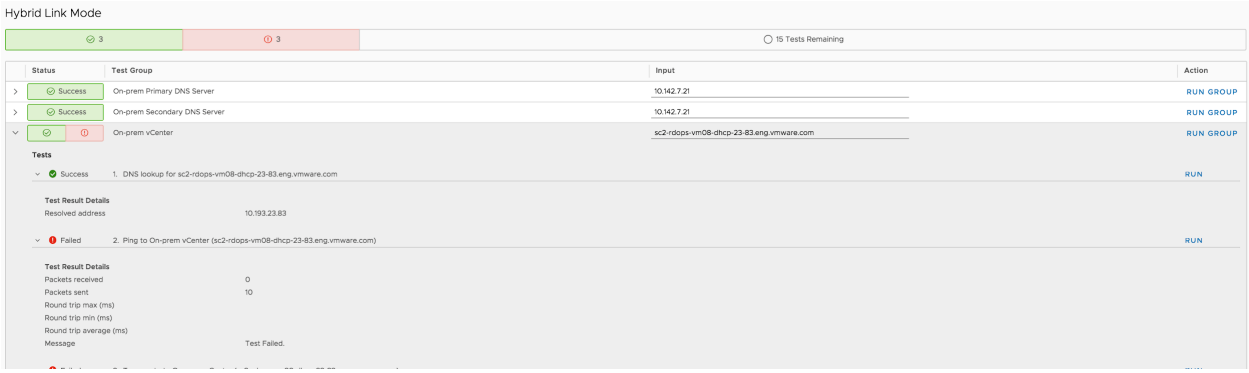
Validateur de connectivité : échec du test ping pour un nom de domaine complet donné

Le test ping sur vCenter Server, Platform Services Controller, Active Directory ou ESXi sur site échoue.

Problème

Un test ping pour un nom de domaine complet donné échoue. Les détails du test indiquent qu'aucune réponse aux paquets ICMP n'a été reçue.

Figure 1-3. Exemple d'échec de test ping



Cause

Les raisons de cet échec peuvent être les suivantes :

- Une règle de pare-fu dans le SDDC de cloud ou le centre de données sur site bloque peut-être le trafic ICMP.
- Le système distant avec le nom de domaine complet donnée est mis hors tension.

Solution

1. Vérifiez vos règles de pare-feu définies dans la Console VMware Cloud pour vous assurer qu'elles ne bloquent pas le trafic ICMP vers le nom de domaine complet donné.
2. Vérifiez vos règles de pare-feu sur site pour vous assurer qu'elles ne bloquent pas le trafic ICMP vers le nom de domaine complet donné.
3. Vérifiez que le système distant objet du test ping est sous tension et fonctionne ; si nécessaire, mettez-le sous tension ou redémarrez-le.

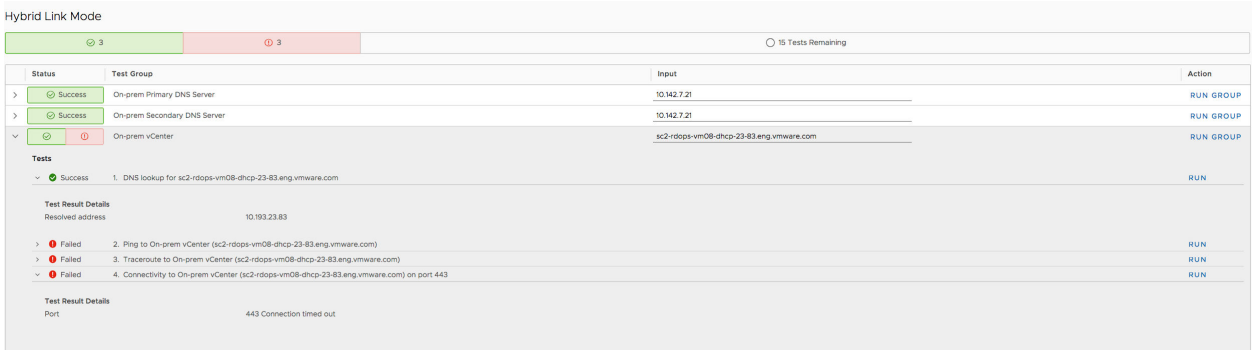
Validateur de connectivité : échec de l'accessibilité à un port pour un nom de domaine complet donné

Test d'accessibilité à un port spécifique

Problème

Un test de connectivité à un port particulier pour un nom de domaine complet donné échoue avec le message `Port port-number Connection timed out`.

Figure 1-4. Exemple d’échec de test de l'accessibilité du port



Cause

Les raisons de cet échec peuvent être les suivantes :

- Une règle de pare-feu dans le SDDC de cloud ou le centre de données sur site bloque peut-être l'accès au port.
- Le système distant avec le nom de domaine complet donnée est mis hors tension.

Solution

1. Vérifiez vos règles de pare-feu définies dans la Console VMware Cloud pour vous assurer qu'elles ne bloquent pas l'accès au port spécifié.
2. Vérifiez vos règles de pare-feu sur site pour vous assurer qu'elles ne bloquent pas l'accès au port spécifique.
3. Vérifiez que le système distant objet du test ping est sous tension et fonctionne ; si nécessaire, mettez-le sous tension ou redémarrez-le.

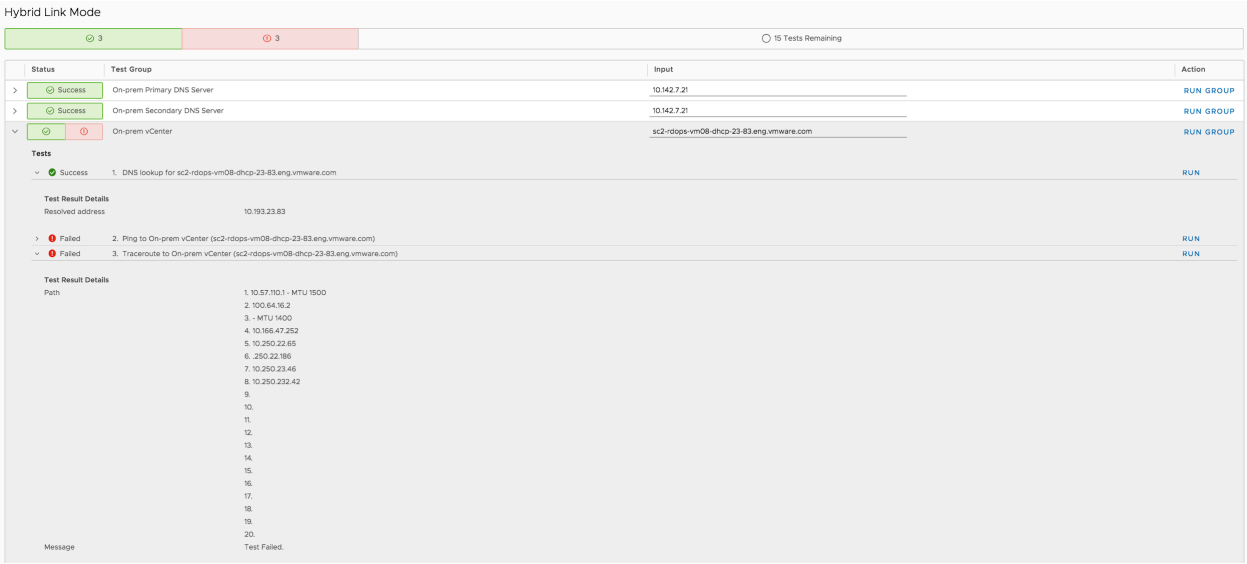
Validateur de connectivité : échec de détermination de route d'un nom de domaine complet donné

Un test de détermination de route pour un nom de domaine complet donné échoue.

Problème

Un test de détermination de route pour un nom de domaine complet échoue. Dans les résultats du test, vous pouvez observer des tronçons vers la destination répertoriés sans adresses IP.

Figure 1-5. Exemple d'échec du test de détermination de route



Cause

Les raisons de cet échec peuvent être les suivantes :

- Si le test ping sur le nom de domaine complet même réussit, une règle de pare-feu dans le SDDC de cloud ou le centre de données sur site est susceptible de bloquer le trafic ICMP sur l'un des tronçons du chemin du trafic.
- Le système distant avec le nom de domaine complet donnée est mis hors tension.

Solution

1. Vérifiez vos règles de pare-feu définies dans la Console VMware Cloud pour vous assurer qu'elles ne bloquent pas le trafic ICMP sur l'un des tronçons du chemin du trafic.
2. Vérifiez vos règles de pare-feu sur site pour vous assurer qu'elles ne bloquent pas le trafic ICMP sur l'un des tronçons du chemin du trafic.
3. Vérifiez que le système distant est mis sous tension et fonctionne ; si nécessaire, mettez-le sous tension ou redémarrez-le.

Validateur de connectivité : échec du test en raison d'une erreur interne

Un test échoue en raison d'une erreur interne.

Problème

Un test de validateur de connectivité peut échouer avec un message d'erreur commençant par `Internal Error:`.

Figure 1-6. Exemple d’échec de test en raison d'une erreur interne

Cause

Cette erreur se produit généralement lorsque le validateur de connectivité rencontre un problème de connectivité interne.

Solution

La plupart de ces pannes sont temporaires et se résolvent sans intervention de votre part. Toutefois, si l'erreur persiste, contactez le support technique de VMware.

Annuler le lien d'un SDDC de cloud

Vous pouvez annuler la liaison d'un SDDC de cloud en mode Hybrid Linked Mode lorsque vous ne souhaitez plus de liaison entre votre SDDC de cloud et un centre de données sur site particulier.

Par exemple, vous pourriez vouloir relier un centre de données sur site à votre SDDC afin de migrer les machines virtuelles vers le SDDC, puis annuler le lien du centre de données sur site. Si vous prévoyez de désactiver un centre de données sur site lié, annuler le avant de le faire.

Note L'annulation du lien d'un centre de données sur site au SDDC de cloud ne supprime pas la source d'identité ou les autorisations associées que vous avez ajoutées avant de lier le domaine. Les utilisateurs peuvent toujours utiliser leurs informations d'identification sur site pour s'authentifier auprès de votre SDDC et conserver les autorisations qui leur ont été accordées. Cependant, ils ne peuvent pas visualiser l'inventaire sur place après avoir annulé le lien du domaine. Lorsque vous annulez le lien d'un SDDC de cloud au dispositif VMware Cloud Gateway, les utilisateurs ne peuvent pas utiliser leurs informations d'identification sur site pour se connecter au SDDC de cloud.

L'annulation du lien laisse également des balises et des catégories en place, car les machines virtuelles dans votre SDDC de cloud peuvent encore utiliser ces balises.

Conditions préalables

Assurez-vous de disposer d'une connectivité réseau entre votre passerelle de gestion SDDC et votre domaine SSO.

Procédure

1 Connectez-vous au système approprié.

- Si vous avez lié votre SDDC de cloud et votre centre de données sur site à partir du dispositif VMware Cloud Gateway, connectez-vous à l'interface utilisateur de VMware Cloud Gateway.
- Si vous avez lié votre SDDC de cloud et votre centre de données sur site à partir du vCenter Server cloud, connectez-vous à l'instance de vSphere Client pour votre SDDC.

2 Accédez à la page Domaines liés.

a Sélectionnez **Menu > Administration** pour afficher la page Administration.

b Sous **Cloud hybride**, sélectionnez **Domaines liés**.

3 Sous le nom du domaine lié, cliquez sur **Annuler le lien**.

Une boîte de dialogue s'affiche vous demandant de confirmer l'annulation du lien. Notez que toutes les sessions actives sont déconnectées lorsque vous annulez le lien avec un domaine.

4 Cliquez sur **OK**.

Lorsque l'annulation du lien est terminée, vous êtes invité à vous déconnecter.

5 Cliquez sur **OK** pour vous déconnecter.

Résultats

Le domaine SSO n'est pas lié. Si vous souhaitez continuer à utiliser le hybrid linked mode, vous pouvez créer un lien vers un autre domaine SSO ou rétablir le lien vers le même domaine.

Note Une fois que vous avez annulé le lien au SDDC de cloud, les nouvelles connexions au SDDC de cloud vSphere Client ne peuvent pas voir les ressources sur site préalablement liées ni interagir avec elles. Les sessions actuellement actives dans le SDDC de cloud vSphere Client continuent à afficher et interagir avec des ressources dans les instances de vCenter Server précédemment liées jusqu'à ce que les utilisateurs de ces sessions se déconnectent du SDDC de cloud vSphere Client ou que les sessions expirent. Si nécessaire, connectez-vous à chacune des instances vCenter Server précédemment liées et fermez ces sessions de force.

Une fois que vous avez annulé le lien au dispositif VMware Cloud Gateway, les nouvelles connexions au dispositif VMware Cloud Gateway ne peuvent pas voir les ressources de cloud précédemment liées ni interagir avec elles. Les sessions actuellement actives dans le dispositif VMware Cloud Gateway peuvent toujours voir les ressources dans le SDDC de cloud et interagir avec elles jusqu'à la déconnexion ou l'expiration des sessions. Si nécessaire, connectez-vous au dispositif VMware Cloud Gateway et forcez la fin de ces sessions.

Clusters et pools de ressources dans VMware Cloud on AWS

2

Dans un environnement vSphere sur site, vous configurez des clusters pour regrouper des hôtes ESXi et pour configurer vSphere HA, vSphere DRS et d'autres fonctions de cluster. Vous utilisez des ressources de groupes de pools de ressources. Dans un environnement VMware Cloud on AWS, VMware crée un cluster unique avec une configuration prédéfinie. VMware crée un pool de ressources pour les machines virtuelles de calcul et un second pool de ressources pour les machines virtuelles de gestion. Vous pouvez afficher les paramètres de cluster et de pool de ressources, ainsi que créer et configurer des pools de ressources enfants.

Vos possibilités dans VMware Cloud on AWS dépendent de vos sélections.

Tableau 2-1. Tâches prises en charge sur les clusters et pools de ressources dans VMware Cloud on AWS

Objet	Tâches prises en charge
Cluster	Un environnement VMware Cloud on AWS dispose d'un cluster qui inclut tous les hôtes ESXi faisant partie de votre SDDC. ■ Afficher la configuration du cluster, y compris vSphere DRS et vSphere HA. L'utilisateur administrateur de cloud ne peut pas modifier la configuration du cluster. ■ Renommez un cluster. ■ Examiner tous les hôtes et tous les pools de ressources qui sont associés au cluster. Vous pouvez afficher la mémoire consommée et la CPU, l'état de HA et le temps d'activité. ■ Examiner toutes les machines virtuelles, toutes les banques de données et tous les réseaux qui sont associés au cluster. ■ Définir des balises et des attributs. Reportez-vous à la section Balises et attributs personnalisés vSphere.
Pool de ressources	Un environnement VMware Cloud on AWS comporte deux pools de ressources prédéfinis. Vous pouvez effectuer les tâches suivantes : ■ Créer des machines virtuelles et des pools de ressources enfants. ■ Modifier les paramètres d'allocation des ressources sur les pools de ressources enfants. ■ Renommer les pools de ressources pour qu'ils correspondent mieux à la stratégie d'entreprise. ■ Surveiller le pool de ressources, ses machines virtuelles et ses pools de ressources enfants, ainsi qu'examiner l'utilisation de pool de ressources. ■ Définir des balises et des attributs. Reportez-vous à la section Balises et attributs personnalisés vSphere.

Note Certaines options de menu, telles que **Supprimer**, sont disponibles sur les pools de ressources de niveau supérieur, mais n'ont aucun effet. En tant que cloudadmin@vmc.local, vous ne disposez pas des autorisations nécessaires pour effectuer ces tâches. Un avertissement s'affiche dans la fenêtre Alarmes.

Lisez les sections suivantes :

- Clusters et pools de ressources prédéfinis
- Examiner les machines virtuelles et les hôtes du cluster
- Examiner et surveiller vSphere DRS
- Examiner et surveiller vSphere HA
- Examiner la configuration du cluster

- Créer et gérer des pools de ressources enfants

Clusters et pools de ressources prédéfinis

Votre SDDC VMware Cloud on AWS inclut initialement un cluster unique, nommé Cluster-1, qui contient deux pools de ressources. Les clusters supplémentaires que vous créez sont numérotés dans l'ordre : Cluster-2, Cluster-3 et ainsi de suite.

Un cluster vSphere organise et gère toutes les ressources de CPU, de mémoire et de stockage d'un ensemble d'hôtes. Chaque cluster prend en charge plusieurs pools de ressources. Un pool de ressources est une abstraction logique pour une gestion flexible des ressources. Les pools de ressources peuvent être regroupés en hiérarchies et utilisés pour partitionner hiérarchiquement les ressources CPU et mémoire disponibles. Reportez-vous à la section Gestion des pools de ressources dans la documentation du produit vSphere pour obtenir plus d'informations.

Lors de la création, Cluster-1 dispose de deux pools de ressources prédéfinis. Ils partagent le même matériel physique, mais sont dédiés à différentes utilisations.

Gestion - Pool de ressources

Ce pool de ressources est toujours créé dans cluster-1 et ne consomme jamais les ressources d'autres clusters. Les ressources de ce pool sont réservées aux machines virtuelles de gestion afin qu'elles puissent fonctionner sans consommer les ressources de Calcul - Pool de ressources. Pour obtenir un résumé des ressources consommées par les machines virtuelles de gestion, reportez-vous au nombre de vCPU de SDDC et aux valeurs de RAM de SDDC dans Valeurs maximales de configuration VMware.

Calculer - Pool de ressources

Ce pool de ressources est initialement créé dans Cluster-1. Par défaut, toutes les machines virtuelles de charge de travail sont créées dans Calcul - Pool de ressources de niveau supérieur (racine). Chaque cluster supplémentaire que vous créez commence par son propre Calcul - Pool de ressources de niveau supérieur. Vous pouvez créer des pools de ressources enfants de n'importe quel pool Calcul - Pool de ressources pour disposer de plus de contrôle sur l'allocation fine des ressources de calcul.

Examiner les machines virtuelles et les hôtes du cluster

Dans un environnement VMware Cloud on AWS, vous pouvez examiner les machines virtuelles et les hôtes dans un cluster.

Procédure

1. Dans vSphere Client, cliquez sur **Menu** et sélectionnez **Hôtes et clusters**.
2. Sélectionnez **Cluster-1**.

   Dans VMware Cloud on AWS, le **Cluster-1** contient les paramètres de configuration de tous les clusters SDDC.

3 Cliquez sur **VM** pour examiner les machines virtuelles et les vApp.

   a Vérifiez la quantité de CPU et de mémoire consommée par machine virtuelle, ainsi que le stockage alloué et utilisé.

   b Cliquez avec le bouton droit sur une flèche vers le bas dans la barre de titre pour afficher ou masquer les colonnes dans cet affichage.

   c Si vous souhaitez apporter des modifications à une machine virtuelle ou à un vApp, sélectionnez-le, cliquez avec le bouton droit sur la machine virtuelle dans la hiérarchie d'objets, cliquez sur **Paramètres** et effectuez la modification.

      Pour plus de détails, consultez la documentation **Gestion des machines virtuelles** de VMware Cloud on AWS.

4 Cliquez sur **Hôtes** pour afficher la ressource que consomment les hôtes du cluster.

   Vous pouvez demander des hôtes supplémentaires si l'utilisation actuelle des ressources indique que vous en aurez bientôt besoin.

Examiner et surveiller vSphere DRS

vSphere DRS garantit l'allocation optimale des ressources dans les machines virtuelles de votre SDDC. Dans un environnement sur site, vous pouvez configurer plusieurs options comme l'utilisation d'un DRS entièrement automatisé ou le choix de recevoir des recommandations. Dans un SDDC VMware Cloud on AWS, VMware a préconfiguré les options vSphere DRS pour le cluster d'hôtes.

VMware a sélectionné des paramètres qui garantissent une distribution optimale des ressources tout en minimisant le nombre de migrations qui se produisent, et pour empêcher les migrations des composants de gestion, y compris NSX Edge, pour l'équilibrage de charge. Bien que vous ne puissiez pas modifier ces sélections, leur affichage peut vous aider à comprendre comment DRS est appliqué dans votre SDDC.

Note Pour une expérience utilisateur harmonieuse, les écrans de configuration, de surveillance et d'examen des clusters et des pools de ressources sont les mêmes dans un SDDC sur site et dans un SDDC VMware Cloud on AWS. Toutefois, le bouton **Modifier** est grisé pour VMware Cloud on AWS.

Procédure

1 Dans vSphere Client, cliquez sur **Menu** et sélectionnez **Hôtes et clusters**.

2 Sélectionnez **Cluster-1**.

   Dans VMware Cloud on AWS, le **Cluster-1** contient les paramètres de configuration de tous les clusters SDDC.

3 Examinez les paramètres DRS qui automatisent entièrement l'allocation des ressources au sein du cluster.

   Pour plus d'informations sur DRS, reportez-vous à la section À propos de la gestion des ressources vSphere dans la *Documentation de VMware vSphere*.

Examiner et surveiller vSphere HA

vSphere High Availability (HA) garantit la disponibilité des machines virtuelles dans votre SDDC. Si un hôte tombe en panne, vSphere HA redémarre ses machines virtuelles sur un hôte différent. Tous les clusters d'un SDDC VMware Cloud on AWS doivent être configurés pour utiliser vSphere HA. Ce paramètre ne peut pas être reconfiguré.

Pour garantir la disponibilité de toutes les charges de travail et de toutes les machines virtuelles de gestion dans votre SDDC, VMware Cloud on AWS doit conserver une capacité suffisante pour les alimenter en cas de panne de l'hôte. Le contrôle d'admission HA est le mécanisme principal de la maintenance de la capacité. Le contrôle d'admission impose des contraintes sur l'utilisation des ressources et peut empêcher toute action qui consomme plus de ressources que le cluster ne peut en prendre en charge lors d'un basculement. Ces contraintes s'appliquent à des actions telles que la mise sous tension ou la migration d'une machine virtuelle, ou la réservation de ressources de CPU ou de mémoire supplémentaires pour une machine virtuelles. Elles limitent efficacement la disponibilité des ressources de l'hôte, comme indiqué ici :

- Dans un cluster de SDDC i3.metal à deux hôtes, le contrôle d'admission vous empêche de mettre sous tension plus de 36 machines virtuelles ou d'attribuer plus de 1 152 MHz de réservation de CPU à une seule machine virtuelle.
- Dans les clusters SDDC comptant de trois à cinq hôtes, le contrôle d'admission réserve un hôte au basculement.

Pour plus d'informations sur les limites du système, reportez-vous à la section Valeurs maximales de configuration VMware.

Pour une présentation détaillée de vSphere HA et d'autres fonctionnalités qui garantissent la disponibilité vSphere, reportez-vous à la section Mode de fonctionnement de vSphere HA dans la *documentation du produit VMware vSphere*. Bien que la plupart des paramètres HA dans VMware Cloud on AWS soient gérés pour vous par VMware et ne puissent pas être modifiés dans le vCenter Server de votre SDDC, il est important de comprendre les concepts fondamentaux de vSphere HA et la manière dont ils s'appliquent au déploiement de la charge de travail dans votre SDDC.

Procédure

1 Dans vSphere Client, cliquez sur **Menu** et sélectionnez **Hôtes et clusters**.

2 Sélectionnez **Cluster-1**.

   Dans VMware Cloud on AWS, le **Cluster-1** contient les paramètres de configuration de tous les clusters SDDC.

3 (Facultatif) Examinez les paramètres vSphere HA, qui sont optimisées pour VMware Cloud on AWS.

   Même si ces paramètres ne sont pas modifiables, en vous familiarisant avec eux vous comprendrez plus facilement comment les machines virtuelles sont déployées dans les clusters de votre SDDC.

4 Pour plus d'informations sur les événements vSphere HA, cliquez sur le lien de **Surveillance de vSphere HA**.

Examiner la configuration du cluster

Dans votre SDDC VMware Cloud on AWS, vous pouvez examiner tous les détails de configuration du cluster que vous pouvez afficher et modifier dans un déploiement sur site.

Note Pour une expérience utilisateur harmonieuse, les écrans de configuration, de surveillance et d'examen des clusters et des pools de ressources sont les mêmes dans un SDDC sur site et dans un SDDC VMware Cloud on AWS. Toutefois, le bouton **Modifier** est grisé pour VMware Cloud on AWS.

Procédure

1 Dans vSphere Client, cliquez sur **Menu** et sélectionnez **Hôtes et clusters**.

2 Sélectionnez **Cluster-1**.

   Dans VMware Cloud on AWS, le **Cluster-1** contient les paramètres de configuration de tous les clusters SDDC.

3 Examinez les paramètres suivants.

Paramètre de configuration	Description
Général	Affiche l'emplacement du fichier d'échange prédéfini et les paramètres de compatibilité de machine virtuelle.
VMware EVC	VMware Enhanced vMotion Compatibility n'est pas requis dans VMware Cloud on AWS. Les hôtes sont uniformes, les problèmes avec vMotion Compatibility ne surviennent pas.
Groupes de machines virtuelles/hôtes	
Règles de machines virtuelles/hôtes	Les administrateurs de votre environnement VMware Cloud on AWS créent des règles pour vous assurer que certaines machines virtuelles ne s'exécutent jamais avec les mêmes règles. Vous pouvez afficher ces règles, mais vous ne pouvez pas créer de règles.

Paramètre de configuration	Description
Substitutions de machines virtuelles	Les substitutions des machines virtuelles modifient le comportement de certaines machines virtuelles. Par exemple, la machine virtuelle vCenter a la priorité de redémarrage vSphere HA la plus élevée. Vous pouvez afficher les substitutions que l'administrateur VMware Cloud on AWS définit pour certaines machines virtuelles du système. Vous ne pouvez pas spécifier les substitutions pour vos propres machines virtuelles.
Options d'hôte	Affiche les options de l'hôte, y compris des informations sur l'hôte.
Profil d'hôte	Tous les hôtes ESXi sont gérés par VMware et sont configurés de manière uniforme. Les profils d'hôte ne sont pas requis.

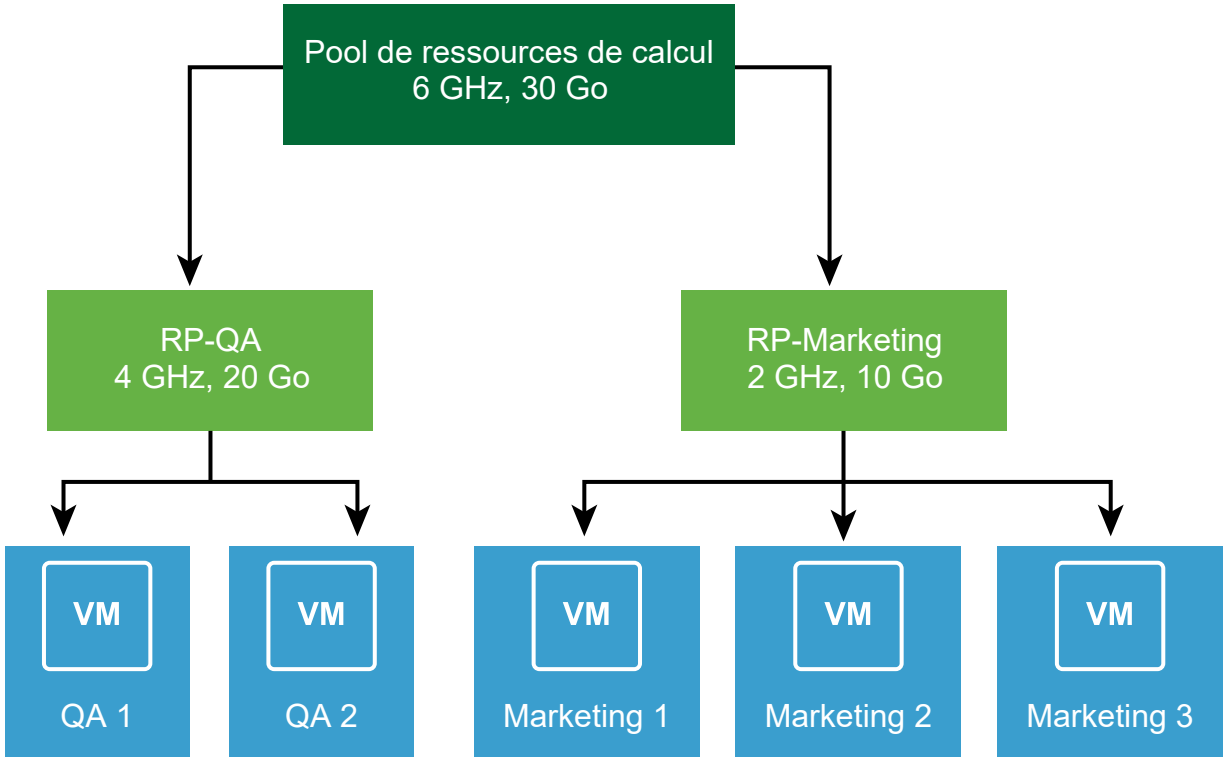
Créer et gérer des pools de ressources enfants

Les pools de ressources vous permettent d'effectuer une allocation de ressources en fonction des besoins des différents groupes . Vous pouvez créer une hiérarchie de pools de ressources enfant pour le pool de ressources de calcul de niveau supérieur, appelée Calcul - Pool de ressources par défaut. Vous pouvez spécifier les paramètres de ressources à la création d'un pool de ressources, et vous pouvez modifier ces paramètres ultérieurement.

Par exemple, supposons qu'un hôte dispose d'un certain nombre de machines virtuelles. Le service Marketing utilise trois des machines virtuelles et le service Assurance de la qualité utilise deux machines virtuelles. Le service Assurance de la qualité nécessite de plus grandes quantités de CPU et de mémoire ; l'administrateur crée donc un pool de ressources pour chaque groupe. L'administrateur définit l'option **Partages CPU** sur **Élevée** pour le pool du service Assurance de la qualité et sur **Normal** pour le pool du service Marketing afin que les utilisateurs du service Assurance de la qualité puissent exécuter des tests automatisés. Le second pool de ressources, possédant moins de ressources CPU et mémoire, est suffisant pour la charge plus légère du personnel du service Marketing. Lorsque le service Assurance de la qualité n'utilise pas complètement son allocation, le service Marketing peut utiliser les ressources disponibles.

Les nombres de la figure qui suit indiquent les allocations effectives des pools de ressources.

Figure 2-1. Pools de ressources parents et pools de ressources enfants



Procédure

1 Démarrez la tâche.

Tâche	Étapes
Créer un pool de ressources	Cliquez avec le bouton droit sur le pool de ressources parent et sélectionnez **Nouveau pool de ressources**.
Modifier les paramètres du pool de ressources	Cliquez avec le bouton droit sur un pool de ressources et sélectionnez **Modifier les paramètres des ressources**. **Note** Si vous modifiez les paramètres des pools de ressources définis par le système, les modifications ne prennent pas effet.

2 Indiquez comment allouer des ressources CPU et de mémoire.

Option	Description
Nom	Nom de ce pool de ressources.
Parts	Définissez les parts du pool de ressources par rapport aux ressources totales du parent. Les pools de ressources frères partagent des ressources selon leurs valeurs de part relatives limitées par la réservation et la limite. ■ Sélectionnez **Faible**, **Normal** ou **Haut** pour définir des valeurs de part dans un rapport 1/2/4. ■ Sélectionnez **Personnalisé** pour donner à chaque machine virtuelle un nombre spécifique de parts, qui exprime un poids proportionnel.
Réservation	Spécifiez une allocation de CPU ou de mémoire garantie pour ce pool de ressources. La valeur par défaut est 0. Une réservation supérieure à zéro est soustraite des ressources non réservées du parent (hôte ou pool de ressources). Les ressources sont considérées comme réservées, que des machines virtuelles soient ou non associées au pool de ressources.
Réservation extensible	Si vous cochez la case (elle l'est par défaut), des réservations extensibles sont prises en compte au cours du contrôle d'admission. Si vous mettez sous tension une machine virtuelle dans le pool de ressources et que les réservations combinées des machines virtuelles sont supérieures à la réservation du pool de ressources, le pool de ressources peut utiliser les ressources de son parent ou de ses ancêtres.
Limite	Spécifiez la limite maximale d'allocation CPU ou de mémoire du pool de ressources. Généralement, vous pouvez accepter la valeur par défaut (**Illimité**). Pour spécifier une limite, décochez la case **Illimité**.

3 Cliquez sur **OK**.

Stockage vSAN dans VMware Cloud on AWS

3

VMware Cloud on AWS fournit deux banques de données vSAN dans chaque cluster SDDC : WorkloadDatastore, gérée par l'administrateur de cloud et vsanDatastore, gérée par VMware.

Ces banques de données sont des entités logiques qui partagent un pool de capacités commun. Chaque banque de données indique l'espace libre disponible total dans le cluster comme étant sa **Capacité**. La capacité consommée dans l'une des deux banques de données met à jour la valeur **Libre** pour les deux banques de données.

vsanDatastore

Cette banque de données fournit un stockage pour les machines virtuelles de gestion dans votre SDDC, tels que vCenter Server, NSX Controller, etc.

La gestion et le dépannage du stockage vSAN dans votre SDDC sont gérés par VMware. Pour cette raison, vous ne pouvez pas modifier les paramètres du cluster vSAN ou surveiller le cluster vSAN. Vous n'avez pas non plus l'autorisation de parcourir cette banque de données, d'y télécharger des fichiers ou d'en supprimer des fichiers.

WorkloadDatastore

Cette banque de données fournit un stockage pour vos machines virtuelles, modèles, images ISO de charge de travail et tout autre fichier que vous choisissez de télécharger sur votre SDDC. Vous avez la totale autorisation de parcourir cette banque de données, créer des dossiers, télécharger des fichiers, supprimer des fichiers et effectuer toutes les autres opérations nécessaires pour consommer ce stockage.

Les banques de données de votre SDDC se voient attribuer la stratégie de stockage des machines virtuelles par défaut. Vous pouvez définir des stratégies de stockage supplémentaires et les attribuer à l'une des deux banques de données. Pour plus d'informations sur les stratégies de stockage vSAN, reportez-vous à Utilisation des stratégies vSAN.

Lisez les sections suivantes :

- Capacité de stockage et redondance des données
- vSAN Déduplication et compression
- Activation des commandes TRIM/UNMAP pour les clusters VMware Cloud on AWS

- Chiffrement vSAN dans VMware Cloud on AWS
- Stratégies vSAN
- Prise en charge du matériel virtuel dans le SDDC VMware Cloud on AWS
- Clusters de stockage partagé sur vSAN

Capacité de stockage et redondance des données

La capacité de stockage et la redondance des données des SDDC dépendent du nombre de nœuds présents dans un SDDC.

Les SDDC ne comprenant qu'un seul nœud ne fournissent aucune redondance de données. Les SDDC comprenant plusieurs nœuds prennent en charge la redondance des données via différentes configurations RAID. Tous les espaces de stockage d'un SDDC fournissent la déduplication des données, la compression des données ou les deux. La redondance des données dans les SDDC comprenant plusieurs hôtes est exprimée sous forme de nombre de pannes à tolérer (FTT, Failures To Tolerate). Une panne peut être la perte d'un hôte dans un cluster ou d'un périphérique de stockage dans une baie.

Toutes les configurations RAID consomment des données pour prendre en charge la redondance. Vous pouvez calculer les besoins en capacité prévus pour vos charges de travail en fonction du type d'instance hôte, de la configuration du cluster et des paramètres de tolérance de panne à l'aide de l'outil VMware Cloud on AWS Sizer et TCO disponibles à l'adresse https://vmc.vmware.com/sizer/workload-profiles.

vSAN Déduplication et compression

vSAN effectue une déduplication et une compression au niveau des blocs pour économiser l'espace de stockage. Cela vous permet d'utiliser de manière plus efficace et rentable le stockage votre SDDC VMware Cloud on AWS.

La déduplication supprime les blocs de données redondants. La compression supprime les données redondantes supplémentaires au sein de chaque bloc de données. Ces techniques fonctionnent en synergie ou séparément pour réduire la quantité de stockage physique requise pour stocker les données. VMware vSAN applique la déduplication, puis la compression lorsqu'il déplace les données du niveau cache au niveau capacité.

La déduplication et la compression sont automatiquement activées pour les clusters VMware Cloud on AWS contenant des hôtes i3 et ne peuvent pas être désactivées. Les clusters contenant des hôtes i3en ou i4i sont automatiquement activés pour la compression uniquement. L'activation de la compression sans déduplication améliore les performances. Elle permet également d'améliorer la disponibilité, car le domaine de pannes peut être limité à un seul disque plutôt qu'à un groupe de disques.

La déduplication a lieu en ligne lors de la réécriture des données du niveau cache au niveau capacité. L'algorithme de déduplication utilise une taille de bloc fixe et est appliqué au sein de chaque groupe de disques. Les copies redondantes d'un bloc dans le même groupe de disques sont dédupliquées.

Les économies de stockage résultant de la déduplication et de la compression dépendent fortement des données de la charge de travail. En moyenne, les économies d'espace de stockage vont de 1,5X à 2X.

Activation des commandes TRIM/UNMAP pour les clusters VMware Cloud on AWS

La prise en charge des commandes TRIM/UNMAP permet aux clusters vSAN de récupérer de l'espace lorsque des fichiers sont supprimés dans une machine virtuelle ou lorsque l'espace est alloué pour plusieurs écritures dans le même fichier.

Le provisionnement des machines virtuelles avec des disques à provisionnement dynamique vous permet de conserver de l'espace de stockage. Le disque démarre à petite taille et s'étend pour accueillir l'espace de stockage requis par le système d'exploitation invité, jusqu'à la taille de disque maximale allouée.

Malgré le provisionnement dynamique, il existe des obstacles à une utilisation optimale de l'espace de stockage des disques de la machine virtuelle. Par défaut, le disque de machine virtuelle ne réduit pas lorsque des fichiers sont supprimés dans le système d'exploitation invité. En outre, de nombreux systèmes d'exploitation invités redirigent toujours les nouvelles écritures vers des blocs de disque libres. Cela peut entraîner l'augmentation de la taille d'un petit fichier dans lequel des données sont fréquemment écrites, tel qu'un fichier journal, et la consommation une grande quantité d'espace disque.

Le système d'exploitation invité peut envoyer des commandes TRIM/UNMAP pour permettre au disque de machine virtuelle de récupérer l'espace précédemment utilisé comme espace disque libre.

Par défaut, la prise en charge de ces commandes n'est pas activée. Pour demander que cette fonctionnalité soit activée pour votre SDDC, contactez l'équipe VMware responsable de votre compte. L'activation de cette fonctionnalité est effectuée par cluster. Vous devez redémarrer les machines virtuelles de charge de travail du cluster pour leur permettre d'utiliser cette fonctionnalité après son activation.

Lors de la suppression de fichiers volumineux ou de l'exécution d'une tâche de récupération d'espace planifiée pour récupérer un grand bloc de capacité, le processus de récupération d'espace peut affecter les charges de travail de production. Cela se manifeste le plus souvent par des latences accrues. Lorsque cela est possible, planifiez des tâches de récupération d'espace importantes pendant les heures de faible activité afin de réduire tout impact potentiel. Après l'activation de cette fonctionnalité, le système peut traiter des suppressions en ligne sans pénalités graves.

Chiffrement vSAN dans VMware Cloud on AWS

vSAN chiffre toutes les données utilisateur stockées dans VMware Cloud on AWS.

Le chiffrement est activé par défaut sur chaque cluster déployé sur votre SDDC et ne peut pas être désactivé.

Lorsque vous déployez un cluster, vSAN utilise le service AWS KMS (AWS Key Management Service) pour générer une clé principale de client (CMK, Customer Master Key), qui est stockée par AWS KMS. vSAN génère une clé de chiffrement de clé (KEK, Key Encryption Key) et la chiffre en utilisant la clé CMK. La clé KEK est à son tour utilisée pour chiffrer les clés de chiffrement de disque (DEK, Disk Encryption Key) générées pour chaque disque vSAN.

Vous pouvez modifier les clés KEK à l'aide de l'API vSAN ou de l'interface utilisateur de vSphere Client. Ce processus est appelé un renouvellement de clés superficiel. La modification de la CMK ou de la DEK n'est pas prise en charge. Si vous devez modifier la CMK ou la DEK, créez un cluster et migrez vos machines virtuelles et vos données vers celle-ci.

Générer de nouvelles clés de chiffrement dans VMware Cloud on AWS

Vous pouvez générer de nouvelles clés de chiffrement de clé (KEK, Key Encryption Key) pour votre cluster VMware Cloud on AWS si nécessaire.

Ce processus est appelé un renouvellement de clés superficiel. La modification de la CMK ou de la DEK n'est pas prise en charge. Si vous devez modifier la CMK ou la DEK, créez un cluster et migrez vos machines virtuelles et vos données vers celle-ci

Procédure

1. Connectez-vous à vSphere Client pour votre SDDC de cloud.
2. Accédez au cluster vSAN.
3. Cliquez sur l'onglet **Configurer**.
4. Sous vSAN, sélectionnez **Services**.
5. Cliquez sur **Générer de nouvelles clés de chiffrement**.
6. Cliquez sur **Appliquer** pour générer de nouvelles clés KEK.

   Les clés de chiffrement de disque (DEK, Disk Encryption Key) sont rechiffrées avec les nouvelles clés KEK.

Exemple : Utilisation de VMware PowerCLI pour cette tâche

Si vous connaissez le mot de passe cloudadmin, vous pouvez utiliser une commande PowerCLI comme celle-ci pour effectuer un renouvellement de clés superficiel pour le service vSAN. Cet exemple, basé sur le modèle de code `Vsan-EncryptionRekey.psl` que vous pouvez télécharger à partir de https://code.vmware.com/samples/2200#code, génère une nouvelle clé du service vSAN qui s'exécute sur le `Cluster-1` de l'instance de vCenter du SDDC`vcenter.sddc-54-200-165-35.vmwarevmc.com` :

```
PS > ./Vsan-EncryptionRekey.psl -vCenter vcenter.sddc-54-200-165-35.vmwarevmc.com -User
      cloudadmin@vmc.local -Password cloudadmin-password -ReKey shallow -ClusterName Cluster-1
```

Stratégies vSAN

Les stratégies de stockage vSAN définissent les conditions de stockage requises pour vos machines virtuelles. Ces stratégies déterminent la manière dont le stockage est alloué aux machines virtuelles de gestion et de charge de travail.

Le premier cluster créé dans votre SDDC VMware Cloud on AWS inclut deux banques de données vSAN : l'une pour les machines virtuelles de gestion (vsanDatastore) et l'autre pour les machines virtuelles de charge de travail (WorkloadDatastore). Les deux banques de données partagent les mêmes périphériques de stockage sous-jacents et consomment les ressources du même pool d'espace libre. Les clusters supplémentaires créés dans le SDDC incluent uniquement un WorkloadDatastore.

Chaque machine virtuelle déployée dans une banque de données vSAN se voit attribuer au moins une stratégie de stockage de machine virtuelle. Vous pouvez attribuer des stratégies de stockage lorsque vous créez ou reconfigurez des machines virtuelles.

Pour plus d'informations sur les stockage, consultez le Designlet VMware Profils de stratégie de stockage gérée.

Attributs de disponibilité pour les stratégies de stockage VM vSAN

Tolérance aux sinistres de site

Définit la méthode de redondance des données utilisée par les clusters étendus pour gérer la défaillance d'un site. Cet attribut s'applique aux clusters étendus. Si vous disposez d'un cluster vSAN standard, choisissez Aucun (cluster standard).

Les options sont :

- Aucun (cluster standard)
- Mise en miroir double-site (cluster étendu)
- Aucun - Conserver les données sur le dispositif primaire (cluster étendu)

- Aucun - Conserver les données sur le dispositif secondaire (cluster étendu)

Pannes à tolérer

Définit le nombre de pannes d'hôte et de périphérique qu'une machine virtuelle peut tolérer. Vous pouvez choisir de n'avoir aucune redondance de données ou sélectionner une configuration RAID optimisée pour les performances (mise en miroir) ou la capacité (codage d'effacement).

- RAID-1 utilise plus d'espace disque, mais offre de meilleures performances.
- RAID-5/6 (codage d'effacement) utilise moins d'espace disque, mais les performances sont réduites.

Tableau 3-1. Configurations RAID, FTT et conditions requises de l'hôte

Configuration RAID	Pannes à tolérer (FTT)	Nombre minimal d'hôtes requis
RAID-1 (mise en miroir) Il s'agit du paramètre par défaut. RAID-1	1	2
RAID-5 (codage d'effacement)	1	4
RAID-1 (mise en miroir)	2	5
RAID-6 (codage d'effacement)	2	6
RAID-1 (mise en miroir)	3	7

Important L'utilisation d'une stratégie de stockage de machine virtuelle avec FTT = 0 (aucune redondance de données) n'est pas recommandée et peut entraîner une perte de données en cas de panne de l'hôte ou si la machine virtuelle cesse de répondre.

Le profil de stratégie de stockage gérée détermine la configuration RAID initiale d'un cluster. Lorsqu'un profil de stratégie de stockage gérée est appliqué au cluster, la configuration RAID est automatiquement mise à jour lorsque la taille du cluster est modifiée. Reportez-vous à Profils de stratégie de stockage gérée par VMware Cloud on AWS pour plus de détails.

Attributs avancés pour les stratégies de stockage VM vSAN

Nombre de bandes de disque par objet

Définit le nombre minimal de périphériques de stockage sur lesquels chaque réplica d'un objet de machine virtuelle est agrégé par bandes. Une valeur supérieure à 1 peut donner de meilleures performances, mais peut également engendrer une plus grande utilisation des ressources système. La valeur par défaut est 1. La valeur maximale est 12. Modifiez la valeur par défaut uniquement lorsque le support VMware le recommande.

Limite d'IOPS pour un objet

Définit la limite IOPS pour un objet, tel qu'un VMDK. IOPS sont calculées comme le nombre d'opérations d'E/S, en utilisant une taille pondérée. Si le système utilise la taille de base par défaut de 32 Ko, une E/S de 64 Ko représente deux opérations d'E/S.

Lors du calcul d'IOPS, la lecture et l'écriture sont considérées équivalentes, mais le taux de réussite du cache et la séquentialité ne sont pas pris en compte. Si l'IOPS d'un disque dépasse la limite, les opérations d'E/S sont limitées. Si la **Limite IOPS pour un objet** est définie sur 0, les limites IOPS ne sont pas appliquées.

vSAN permet à l'objet de doubler le taux de la limite IOPS pendant la première seconde d'une opération ou après une période d'inactivité.

Réservation d'espace de l'objet

Ce paramètre définit le pourcentage de la taille logique du disque de machine virtuelle (vmdk) devant être réservé (provisionné) lors du déploiement de machines virtuelles. La valeur de réservation par défaut dans VMware Cloud on AWS est de 0 % (**Provisionnement dynamique**). Vous pouvez spécifier **Provisionnement statique** pour réserver de la capacité pour des écritures vSAN plus volumineuses qu'attendues, mais la structure vmdk sous-jacente reste la même que celle de la configuration **Provisionnement dynamique** et n'est pas la même que le modèle de provisionnement statique immédiatement mis à zéro disponible sur site.

Comme indiqué dans la section Ressources de stockage, vous devez envisager de définir le paramètre de stratégie avancée **Réservation d'espace de l'objet** (OSR) sur **Provisionnement dynamique**. L'OSR contrôle uniquement la réservation d'espace et n'a aucun impact sur les performances. Bien que la gestion de la capacité soit souvent critique pour les centres de données sur site, l'utilisation de VMware Cloud on AWS Elastic DRS permet de s'assurer que le cluster ne manquera pas d'espace libre.

Réservation de Flash Read Cache

Ce paramètre est ignoré dans VMware Cloud on AWS. Dans les déploiements vSAN hybride, il désigne la capacité de mémoire flash réservée en tant que cache de lecture.

Désactiver le total de contrôle de l'objet

Si l'option est définie sur **Non**, l'objet calcule les informations de total de contrôle pour garantir l'intégrité de ses données. Si cette option est définie sur **Oui**, l'objet ne calcule pas les informations de total de contrôle.

vSAN utilise un total de contrôle de bout en bout pour garantir l'intégrité des données en confirmant que chaque copie d'un fichier est exactement la même que le fichier source. Le système vérifie la validité des données pendant les opérations de lecture/écriture et si une erreur est détectée, vSAN répare les données ou signale l'erreur.

Si une non-correspondance de total de contrôle est détectée, vSAN répare automatiquement les données en remplaçant les données incorrectes par les données correctes. Le calcul du total de contrôle et la correction d'erreur sont effectués en arrière-plan.

La valeur par défaut pour tous les objets du cluster est **Non**, ce qui signifie que le total de contrôle est activé.

Forcer le provisionnement

Si l'option est définie sur **Oui**, l'objet est provisionné, même si les stratégies **Niveau primaire de pannes à tolérer**, **Nombre de bandes de disque par objet** et **Réservation de Flash Read Cache** spécifiées dans la stratégie de stockage ne peuvent pas être satisfaites par la banque de données. Utilisez ce paramètre dans les scénarios d'amorçage ou lors d'une coupure lorsque le provisionnement standard n'est plus possible.

La valeur par défaut **Non** est acceptable pour la plupart des environnements de production. vSAN ne parvient pas à provisionner une machine virtuelle lorsque les conditions requises de la stratégie ne sont pas respectées, mais crée avec succès la stratégie de stockage définie par l'utilisateur.

Profils de stratégie de stockage gérée par VMware Cloud on AWS

Lorsque vous créez un cluster dans votre SDDC, VMware Cloud on AWS crée un profil de stratégie de stockage gérée qui est appliqué par défaut aux machines virtuelles que vous créez dans le cluster. Ce profil de stratégie de stockage est nommé « stratégie de stockage de charge de travail VMC - *nom du cluster* ». Les paramètres de stratégie veillent à ce que le cluster respecte les exigences décrites dans le Contrat de niveau de service pour VMware Cloud on AWS (le SLA). Lorsque vous migrez une machine virtuelle vers un cluster différent dans le même SDDC, vous devez également modifier la stratégie de stockage de machine virtuelle. Reportez-vous à la section Attribuer des stratégies de stockage à des machines virtuelles.

Les paramètres de stratégie de stockage géré sont basés sur la configuration du cluster :

- Les SDDC à hôte unique ne sont pas couverts par le SLA. Ils utilisent une stratégie **Aucune redondance de données**.
- Les clusters à une seule zone de disponibilité utilisent le provisionnement fin et définissent une valeur de tolérance de panne basée sur la taille du cluster et le type d'instance de l'hôte :
  - Les clusters contenant entre deux et cinq hôtes utilisent la stratégie **1 panne - RAID-1 (mise en miroir)**.
  - Les clusters contenant six hôtes ou plus utilisent la stratégie **2 pannes : RAID-6 (codage d'effacement)**.
- Les clusters étendus incluant quatre hôtes ou moins utilisent **Pas de redondance de données** et **Tolérance aux sinistres de site** défini sur **Double mise en miroir du site**.
- Les clusters étendus comportant six hôtes ou plus utilisent la stratégie **1 panne - RAID-1 (mise en miroir)**, mais disposent également d'un niveau de **Tolérance aux sinistres de site** défini sur **Double mise en miroir du site**.

Comme la stratégie de stockage gérée varie en fonction de la taille du cluster, l'ajout ou la suppression d'hôtes déclenche une reconfiguration de la stratégie de stockage si elle modifie la taille du cluster afin qu'elle nécessite une stratégie différente. Par exemple, si vous ajoutez un hôte supplémentaire à un cluster contenant cinq hôtes, la stratégie de stockage pour ce cluster est reconfigurée pour passer de **1 panne - RAID-1 (mise en miroir)** à **2 pannes - RAID-6 (codage de suppression)**. L'inverse se produit si l'hôte supplémentaire est supprimé et que le nombre d'hôtes est réduit de six à cinq.

Note Lorsque vous apportez une modification à un cluster qui déclenche une reconfiguration de la stratégie de stockage gérée, la reconfiguration nécessite un stockage supplémentaire de manière temporaire. Si la capacité de stockage du cluster est proche de 79%, un événement de montée en charge EDRS peut se déclencher et ajouter un hôte au cluster. Une fois la reconfiguration terminée, EDRS peut ne pas supprimer l'hôte supplémentaire. Vérifiez vos clusters après la reconfiguration du stockage et supprimez l'hôte supplémentaire si nécessaire.

Dans un cluster étendu à six hôtes, vous ne pouvez pas supprimer des hôtes. Dans un cluster standard à six hôtes ou plus, vous ne pouvez pas supprimer un hôte si l'utilisation du stockage du cluster est supérieure à 40 % de la capacité totale de stockage. Pour tous les autres types de clusters, VMware recommande vivement de ne pas supprimer un hôte si l'utilisation du stockage du cluster est supérieure à 40 % de la capacité de stockage totale.

Si la suppression d'un ou de plusieurs hôtes d'un cluster déclenche une reconfiguration de la stratégie de stockage gérée, la reconfiguration doit se terminer avant la suppression du ou des hôtes. Si vos charges de travail utilisent une quantité de stockage importante, cette reconfiguration peut prendre de quelques heures à plusieurs jours. Pendant ce temps, tous les hôtes que vous avez désignés pour être supprimés restent utilisables et vous êtes toujours facturé pour l'utilisation de ces hôtes. Une fois la reconfiguration de la stratégie de stockage terminée, l'hôte ou les hôtes sont supprimés et vous n'êtes plus facturé pour l'utilisation de ceux-ci.

Note Ne modifiez pas les stratégies de stockage gérées que VMware Cloud on AWS crée pour vos clusters. Si vous renommez la stratégie, celle-ci n'est plus gérée par VMware Cloud on AWS. Si vous modifiez les paramètres de la stratégie de stockage gérée, vos modifications sont écrasées lors de la prochaine reconfiguration de la stratégie de stockage.

Si vous ne souhaitez pas utiliser la stratégie de stockage gérée, vous pouvez définir votre propre stratégie de stockage et l'attribuer comme valeur par défaut pour la banque de données de charge de travail. Reportez-vous à la section Utilisation des stratégies vSAN dans *Administration de VMware vSAN*.

Modèles de VM et stratégies de stockage gérées

Si un modèle de machine virtuelle est associé à une stratégie de stockage gérée par VMware Cloud on AWS, la stratégie du modèle n'est pas automatiquement mise à jour si la stratégie du cluster est reconfigurée. Une fois la stratégie de stockage du cluster reconfigurée, l'état de conformité du modèle de machine virtuelle est « Obsolète ». Pour rendre l'état de la stratégie du modèle « Conforme », vous devez convertir le modèle en machine virtuelle, réappliquer la stratégie de stockage de machine virtuelle, puis reconvertir la machine virtuelle en modèle.

Lorsque vous déployez une machine virtuelle à partir d'un modèle, VMware vous recommande de sélectionner **Banque de données par défaut** pour la stratégie de stockage de machine virtuelle afin de garantir que la machine virtuelle est déployée avec la stratégie de stockage gérée du cluster actuel.

Stratégies de stockage et conditions SLA

Lorsque vous utilisez des stratégies de stockage de machine virtuelle, il est important de comprendre comment elles affectent la consommation de la capacité de stockage dans le cluster vSAN et si elles répondent aux conditions requises définies dans le contrat de niveau de service (SLA) pour VMware Cloud sur AWS.

La stratégie de stockage gérée est initialement configurée en fonction du nombre d'hôtes dans le cluster. Par exemple, un cluster à trois hôtes est défini par défaut sur FTT=1 à l'aide de la stratégie de mise en miroir RAID-1. Les clusters disposant de plus de six hôtes dans une seule zone de disponibilité sont définis par défaut sur **2 pannes : RAID-6 (codage de suppression)**. Vous pouvez créer des stratégies personnalisées qui alignent la disponibilité des données avec les besoins de vos données sous-jacentes, mais les machines virtuelles de charge de travail avec des stratégies de stockage qui ne répondent pas aux exigences définies dans le contrat de niveau de service peuvent ne pas être éligibles aux crédits SLA. La stratégie de stockage de machine virtuelle doit être configurée avec le niveau de protection approprié. Les charges de travail éphémères peuvent utiliser la stratégie Aucune redondance de données pour économiser de la capacité, conformément aux garanties suivantes de disponibilité du SLA.

Important Lors de la montée en puissance d'un cluster de cinq à six hôtes, la tolérance de panne de la stratégie sous-jacente doit être mise à jour en **2 pannes : RAID-6 (codage de suppression)** ou **2 pannes : RAID-1 (mise en miroir)** afin de compenser le plus grand pool de pannes. Les clusters utilisant la stratégie de stockage gérée seront reconfigurés automatiquement, mais vous devrez mettre à jour manuellement tous les clusters qui utilisent des stratégies personnalisées. L'utilisation continue d'une tolérance de panne égale à 1 pour cette configuration d'hôte signifie que VMware ne peut pas garantir la disponibilité conformément au guide de définition de service.

VMware vérifie régulièrement la conformité des stratégies de stockage de vos machines virtuelles aux exigences du SLA et envoie des notifications en cas de stratégies non conformes.

Pour plus d'informations sur les considérations de conception et de dimensionnement à prendre en compte dans les stratégies de stockage, reportez-vous à Administration de VMware vSAN.

Définir une stratégie de stockage de machine virtuelle pour vSAN

Vous pouvez créer une stratégie de stockage qui définit des conditions de stockage pour une machine virtuelle et ses disques virtuels. Dans cette stratégie, vous faites référence aux capacités de stockage prises en charge par la banque de données vSAN.

Procédure

1. Dans vSphere Client, cliquez sur **Menu > Stratégies et profils**, puis sur **Règles de stockage VM**.
2. Cliquez sur **Créer une stratégie de stockage VM**.
3. Sur la page Nom et description :
   a. Laissez le vCenter Server sélectionné.
   b. Entrez un nom et une description pour la stratégie de stockage et cliquez sur **Suivant**.
4. Sur la page vSAN, spécifiez les attributs **Disponibilité** et **Avancés**, et cliquez sur **Suivant**.

   Les valeurs par défaut conviennent à de nombreuses situations. Pour plus d'informations sur chaque attribut, reportez-vous à la section Stratégies vSAN.
5. Dans la page Compatibilité de stockage, vérifiez la liste des banques de données qui correspondent à cette stratégie, puis cliquez sur **Suivant**.

   Pour être admissible, une banque de données ne doit pas nécessairement être conforme à tous les ensembles de règles qui constituent la stratégie. Elle doit être conforme à au moins un ensemble de règles et à l'intégralité des règles de cet ensemble. Vérifiez que la banque de données de WorkloadDatastore répond aux conditions requises définies dans la stratégie de stockage et qu'elle figure dans la liste de banques de données compatibles.
6. Dans la page Prêt à terminer, vérifiez les paramètres de la stratégie, puis cliquez sur **Terminer**.

Étape suivante

Attribuez cette stratégie à une machine virtuelle et à ses disques virtuels. vSAN place les objets de machine virtuelle selon les conditions spécifiées dans la stratégie. Pour plus d'informations sur l'application des stratégies de stockage aux objets de machine virtuelle, reportez-vous à la documentation de *Stockage vSphere*.

Attribuer des stratégies de stockage à des machines virtuelles

Vous pouvez attribuer une stratégie de stockage VM lors du déploiement initial d'une machine virtuelle ou alors que vous effectuez d'autres opérations de machine virtuelle telles qu'un clonage ou une migration.

Cette rubrique explique comment attribuer une stratégie de stockage VM lorsque vous créez une machine virtuelle. Pour plus d'informations sur les autres méthodes de déploiement, parmi lesquelles le clonage, le déploiement à partir d'un modèle, etc., reportez-vous à la documentation *Administration d'une machine virtuelle vSphere*.

Vous pouvez appliquer la même stratégie de stockage au fichier de configuration de la machine virtuelle et à tous ses disques virtuels. Si les besoins en stockage de vos disques virtuels et du fichier de configuration sont différents, vous pouvez associer différentes stratégies de stockage au fichier de configuration de machine virtuelle et aux disques virtuels sélectionnés.

Important Lorsque vous faites migrer des machines virtuelles entre des clusters dans le même SDDC, vous devez également transformer la stratégie de stockage de machine virtuelle en stratégie gérée du cluster de destination. L'option par défaut, à savoir Conserver les stratégies de stockage de machine virtuelle existantes, n'est appropriée que si vous utilisez une stratégie personnalisée. Sinon, sélectionnez la stratégie attribuée au cluster de destination.

Procédure

1. Dans vSphere Client, démarrez le processus de provisionnement de la machine virtuelle et suivez la procédure appropriée.
2. Attribuez la même stratégie de stockage à tous les disques et les fichiers de machine virtuelle.
   a. Sur la page **Sélectionner un stockage**, sélectionnez une stratégie de stockage dans le menu déroulant **Stratégie de stockage VM**.

      Selon sa configuration, la stratégie de stockage sépare toutes les banques de données en ensembles compatibles et incompatibles. Si la stratégie fait référence à des services de données proposés par une entité de stockage spécifique (Virtual Volumes, par exemple), la liste des ensembles compatibles inclut les banques de données représentant uniquement ce type de stockage.

   b. Sélectionnez une banque de données appropriée dans la liste des banques de données compatibles.

      Cette banque de données devient la ressource de stockage de destination pour le fichier de configuration de la machine virtuelle et pour tous les disques virtuels.
3. Modifiez la stratégie de stockage VM du disque virtuel.

   Utilisez cette option si les besoins en matière de placement de stockage sont différents pour les disques virtuels. Vous pouvez également utiliser cette option pour activer des services de filtre d'E/S (par exemple, la mise en mémoire cache et la réplication) pour vos disques virtuels.
   a. Sur la page **Personnaliser le matériel**, développez le volet **Nouveau disque dur**.
   b. Dans le menu déroulant **Stratégie de stockage VM**, sélectionnez la stratégie de stockage à attribuer au disque virtuel.
4. Terminez le processus de provisionnement de la machine virtuelle.

Résultats

Une fois la machine virtuelle créée, les stratégies de stockage attribuées et leur état de conformité s'affichent dans l'onglet **Résumé**.

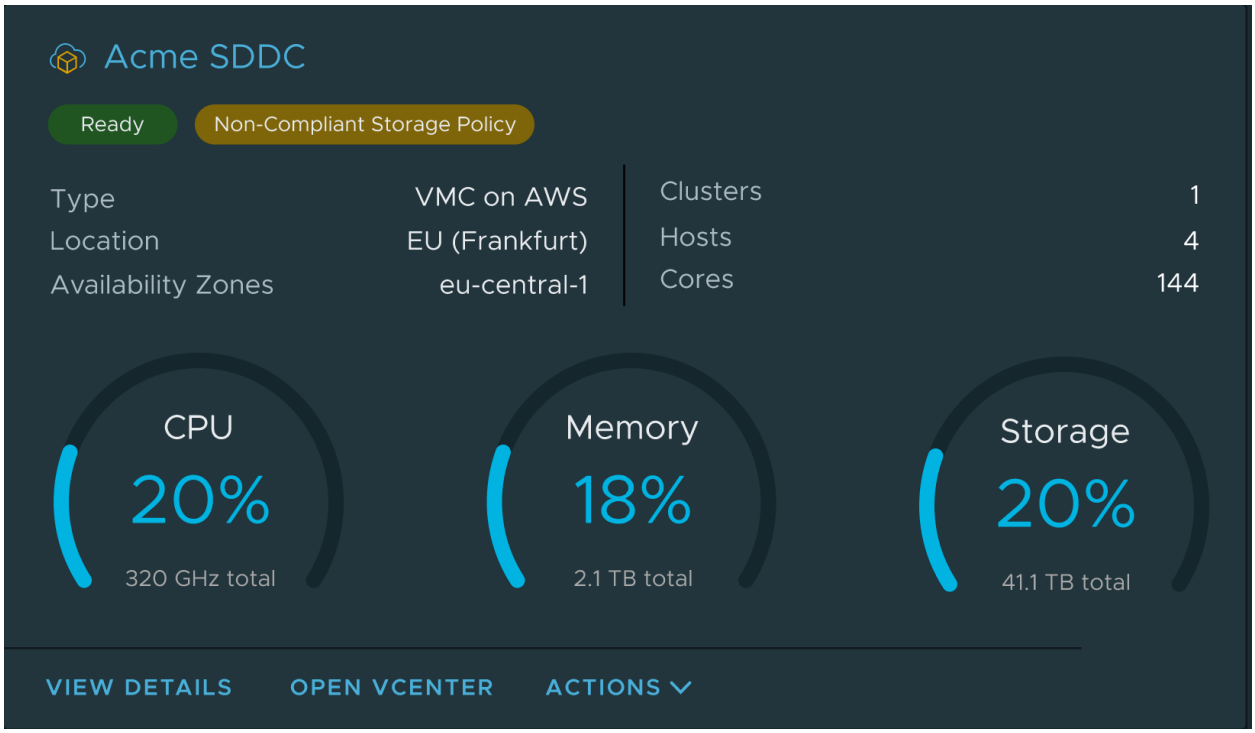
Étape suivante

En cas de changement des conditions requises en matière de placement de stockage pour le fichier de configuration ou les disques virtuels, vous pourrez modifier ultérieurement l'attribution de stratégie de machine virtuelle.

Appliquer une stratégie de stockage gérée aux machines virtuelles non conformes

VMware Cloud on AWS vérifie régulièrement vos SDDC pour détecter les machines virtuelles dont les stratégies de stockage ne sont pas conformes aux exigences du SLA.

S'il y a des machines virtuelles non conformes dans votre organisation, vous recevez des notifications dans la bannière de la Console VMware Cloud. Les cartes de SDDC et les clusters qui contiennent des machines virtuelles non conformes présentent un indicateur **Stratégie de stockage non conforme**.



Vous pouvez utiliser la Console VMware Cloud pour mettre à jour les machines virtuelles non conformes vers une stratégie de stockage gérée, ce qui permettra d'en maintenir la conformité. Si vous souhaitez conserver une stratégie de stockage personnalisée pour ces machines virtuelles, connectez-vous à vSphere Client et modifiez la stratégie comme indiqué dans la section Utilisation de stratégies vSAN.

Procédure

1 Connectez-vous à la Console VMware Cloud à l'adresse https://vmc.vmware.com.

2 Sur la carte d'un SDDC ayant un indicateur **Stratégie de stockage non conforme**, cliquez sur **Afficher les détails**, puis sur l'onglet **Stockage**.

   Une liste des clusters du SDDC s'affiche, avec une colonne **État** indiquant s'il y a des machines virtuelles non conformes.

3 Pour afficher les machines virtuelles non conformes, développez un cluster.

4 Sélectionnez une ou plusieurs machines virtuelles non conformes, puis cliquez sur **Mettre à jour vers la stratégie de stockage gérée**.

Résultats

Les machines virtuelles sélectionnées sont mises à jour pour utiliser la stratégie de stockage gérée.

Mettre à jour la stratégie de stockage par défaut pour un cluster ayant une stratégie non conforme

La Console VMware Cloud affiche une alerte si des clusters dans vos SDDC ont une stratégie de stockage par défaut qui n'est pas conforme.

Il est recommandé de maintenir la conformité des stratégies de stockage du cluster. Une stratégie de stockage non conforme peut avoir un impact négatif sur les exigences du SLA.

Vous pouvez corriger ce problème en mettant à jour vos clusters pour utiliser une stratégie de stockage gérée par VMware, ce qui rend la stratégie de stockage par défaut conforme en fonction de l'évolution du SLA. Vous pouvez également modifier le cluster pour appliquer une stratégie de stockage personnalisée conforme aux conditions du SLA. Pour plus d'informations sur les stratégies de stockage gérées et les exigences du SLA, reportez-vous à la section Profils de stratégie de stockage gérée par VMware Cloud on AWS.

Procédure

1 Sélectionnez le cluster à mettre à jour.

   a Cliquez sur la fiche du SDDC.

   b Sur la fiche du cluster que vous souhaitez mettre à jour, sélectionnez **Actions > Définir la stratégie de stockage par défaut**

2 Mettez à jour la stratégie de stockage.

   - Cliquez sur **Mettre à jour vers la stratégie de stockage gérée** pour mettre à jour le cluster vers la stratégie de stockage gérée.
   - Cliquez sur **Connexion à vCenter Server** pour mettre à jour manuellement la stratégie.

Prise en charge du matériel virtuel dans le SDDC VMware Cloud on AWS

La compatibilité de machine virtuelle dans VMware Cloud on AWS peut être mise en corrélation avec la version du SDDC.

Pour savoir quelles versions de ESXi et de vCenter Server s'exécutent dans votre SDDC, ainsi que les versions du matériel virtuel qu'elles prennent en charge, reportez-vous à la section Mise en corrélation de VMware Cloud on AWS avec les versions des composants. Pour obtenir des informations détaillées sur les versions du matériel virtuel et les fonctionnalités associées prises en charge par les versions d'ESXi et de vCenter Server, reportez-vous à la section Fonctionnalités matérielles disponibles dans les paramètres de compatibilité des machines virtuelles de la *documentation du produit VMware vSphere*.

Note La prise en charge du matériel virtuel pour un ensemble donné de composants peut ne pas être la même dans VMware Cloud on AWS, car elle est mise en œuvre dans votre centre de données sur site.

Reportez-vous à Configurations de machines virtuelles ayant une prise en charge limitée ou nulle dans le SDDC de cloud pour obtenir un résumé des configurations de machines virtuelles qui ne sont pas prises en charge ou qui sont prises en charge avec des limitations dans le SDDC.

Clusters de stockage partagé sur vSAN

VMware Cloud on AWS prend en charge les réservations persistantes SCSI-3 pour les machines virtuelles de charge de travail. Vous devez utiliser cette capacité lors de la configuration d'un cluster de basculement Windows Server (WSFC) dans votre SDDC.

La plus grande partie de ce que vous devez savoir pour configurer les machines virtuelles de charge de travail pour prendre en charge WSFC est expliquée dans la section À propos de la configuration du clustering de basculement Windows Server sur VMware vSphere dans la documentation du produit vSphere. Cette rubrique ajoute quelques étapes que vous devrez suivre si vous souhaitez configurer WSFC pour utiliser le stockage vSAN dans votre SDDC.

VMware Cloud on AWS prend en charge WSFC sur les clusters conventionnels et étendus.

Un cluster de basculement Windows Server utilise les réservations persistantes SCSI-3 pour arbitrer l'accès partagé aux ressources de disque en cluster. Pour que cela fonctionne, les machines virtuelles du cluster doivent respecter plusieurs exigences de configuration :

- Pour activer l'utilisation des réservations persistantes SCSI-3, les disques partagés doivent être accessibles via un contrôleur SCSI pour lequel le **partage de bus SCSI** est configuré sur **Physique**.
- Pour empêcher les opérations de snapshots non prises en charge sur les disques partagés, le **mode Disque** de tous les disques du cluster doit être défini sur **Indépendant – Persistant**.

Dans un SDDC VMware Cloud on AWS, vSAN prend en charge les réservations persistantes SCSI-3 sur six nœuds d'applications au maximum par cluster invité avec jusqu'à 64 disques partagés.

Note Lorsqu'un VMDK est partagé à l'aide de réservations persistantes SCSI-3, les opérations des machines virtuelles telles que les snapshots, Storage vMotion vers ou depuis une banque de données vSAN, le clonage, l'extension à chaud d'un disque dur et la réplication via vSphere Replication ne sont pas prises en charge. Consultez l'article 79616 de la base de connaissances VMware pour obtenir des informations détaillées sur les configurations prises en charge.

Vous ne devez pas activer le mode multi-écriture VMDK sur les ressources de disque WSFC.

Pour obtenir des directives complètes sur les considérations architecturales et des procédures détaillées de configuration et de migration des charges de travail WSFC sur VMware Cloud on AWS, consultez l'article technique de VMware intitulé Charges de travail Microsoft SQL Server et VMware Cloud on AWS : conception, migration et configuration et l'article de blog VMware Prise en charge native du cluster SQL Server sur vSAN.

Procédure

1 Configurez le premier nœud du cluster.

   Suivez les étapes décrites dans Ajouter des disques durs au premier nœud pour un cluster entre hôtes physiques avec des VMDK en cluster sur des banques de données VMFS avec les ajouts suivants :

   a Définissez le mode **Disque** sur **Indépendant – Persistant**.

   b (Facultatif) Attribuez au disque une stratégie de stockage de machine virtuelle personnalisée.

      Bien que cela ne soit pas une exigence, il est probable que toutes les données que vous devez protéger avec WSFC auraient avantage à utiliser une stratégie de stockage dédiée.

2 Configurez des nœuds supplémentaires.

   Suivez les étapes décrites dans la section Ajouter des disques durs à des nœuds supplémentaires pour les clusters entre hôtes physiques avec les ajouts suivants :

   a Définissez le mode **Disque** sur **Indépendant – Persistant**.

   b (Facultatif) Attribuez au disque une stratégie de stockage de machine virtuelle personnalisée.

3 Utilisez l'assistant Création d'un cluster de Microsoft pour valider le cluster.

   Note Pendant la validation, l'assistant affiche un avertissement dans la catégorie **Stockage** et la sous-catégorie **Valider la réservation persistante d'espaces de stockage**. Cet avertissement ne s'applique pas lors de la configuration d'un cluster de basculement Windows Server dans votre SDDC et il peut être ignoré en toute sécurité.

Gestion des machines virtuelles dans VMware Cloud on AWS

Votre SDDC de cloud VMware Cloud on AWS fournit tous les outils dont vous avez besoin pour déployer et personnaliser les machines virtuelles (VM) VMware.

Comme il s'agit d'un service, VMware Cloud on AWS impose quelques contraintes pour les opérations de machine virtuelle, en particulier celles qui nécessitent un accès physique au matériel hôte ou un accès racine au système d'exploitation hôte. En dehors de quelques exceptions (que nous abordons dans ce document), les opérations sur site décrites dans la section À propos de l'administration d'une machine virtuelle vSphere fonctionnent de la même manière dans votre SDDC VMware Cloud on AWS.

Tableau 4-1. Points clés de l'*Administration d'une machine virtuelle vSphere*

Rubriques	Points clés du contenu
Introduction aux machines virtuelles vSphere	■ Présentation du cycle de vie et des composants des machines virtuelles. ■ Liste des fichiers de machine virtuelle et leur objet. ■ Présentation du matériel de machine virtuelle et d'autres options.
Déploiement des machines virtuelles	Instructions détaillées pour la création de machines virtuelles. Vous disposez de nombreuses options, notamment : ■ Le déploiement d'une machine virtuelle à partir de zéro. ■ Le clonage de machines virtuelles ou de modèles existants ■ Le déploiement d'un modèle OVF ou OVA ■ Le déploiement d'une machine virtuelle à partir d'un fichier OVF ou OVA téléchargé
Utilisation des bibliothèques de contenu	Les bibliothèques de contenu sont des objets conteneurs pour les modèles de machine virtuelle, les modèles de vApp et les autres types de fichiers, tels que des images ISO, des fichiers texte, etc. Vous pouvez utiliser les modèles de la bibliothèque pour déployer des machines virtuelles et des vApp dans l'inventaire vSphere. Vous pouvez également utiliser des bibliothèques de contenu pour partager du contenu entre votre infrastructure sur site et votre SDDC.

Tableau 4-1. Points clés de l'*Administration d'une machine virtuelle vSphere* (suite)

Rubriques	Points clés du contenu
Configuration du matériel d'une machine virtuelle	Des informations détaillées sur les possibilités de configuration des différentes options matérielles, comme les CPU, la mémoire et les périphériques. Vous pouvez modifier des périphériques virtuels existants ou ajouter de nouveaux périphériques. Cependant, comme nous l'avons précisé, certaines contraintes peuvent s'appliquer dans VMware Cloud on AWS par rapport à ce que vous pouvez faire dans votre environnement vCenter sur site.
Configuration des options des machines virtuelles	Détaille les options des machines virtuelles et comment les modifier. ■ Paramètres de gestion de l'alimentation ■ Démarrage sécurisé UEFI pour les machines virtuelles ■ Options de démarrage des machines virtuelles ■ Options avancées, telles que la journalisation, le débogage et la sensibilité de la latence
Personnalisation des machines virtuelles	Instructions sur l'exécution de tâches de personnalisation post-déploiement, notamment : ■ Les options d'installation d'un système d'exploitation invité ■ La personnalisation du système d'exploitation invité avec une spécification de personnalisation ■ L'utilisation d'une console de machine virtuelle ■ L'utilisation de snapshots ■ La mise à niveau de VMware Tools ou du paramètre de compatibilité du matériel.
Gestion de la configuration du proxy VMware Remote Console	Le proxy de VMware Remote Console pour vSphere (proxy VMRC) est un service du système SDDC vCenter Server qui simplifie l'établissement des connexions VMRC aux machines virtuelles de charge de travail.

Configurations de machines virtuelles ayant une prise en charge limitée ou nulle dans le SDDC de cloud

Certaines configurations de machines virtuelles que vous pouvez utiliser dans votre centre de données sur site ne sont pas prises en charge dans le SDDC. D'autres sont prises en charge avec des limitations.

Utilisez Administration d'une machine virtuelle vSphere dans la Documentation de VMware vSphere en tant que guide de création, de configuration et de gestion des machines virtuelles de charge de travail dans VMware Cloud on AWS. Comme VMware Cloud on AWS est un service, certaines options de configuration de machines virtuelles documentées dans Administration d'une machine virtuelle vSphere ne peuvent pas être utilisées dans un SDDC de cloud, même si elles peuvent être mentionnées dans une rubrique d'aide ou répertoriées dans vSphere

Client lorsque vous cliquez avec le bouton droit sur une machine virtuelle de charge de travail et choisissez **Modifier les paramètres**. Mais en dehors de quelques exceptions, que nous documentons ici, vous pouvez utiliser les conseils fournis dans ce document lorsque vous configurez, déployez et gérez des machines virtuelles de charge de travail dans le SDDC.

Pour connaître les autres limites imposées par VMware Cloud on AWS, reportez-vous à la section Valeurs maximales de configuration VMware.

Tableau 4-2. Options de configuration de machines virtuelles sur site non disponibles dans un SDDC

Option de configuration	Références	Commentaires
Activez l'hyperthreading dans un CPU virtuel.	Configuration de CPU virtuel et autres rubriques.	Pour atténuer les vulnérabilités de sécurité, y compris celles décrites dans l'article 55806 de la base de connaissances VMware et dans l'article 55808 de la base de connaissances VMware, VMware Cloud on AWS gère l'hyperthreading de CPU sur les hôtes i3.metal.
Modifiez les masques d'identification de CPU.	Configuration matérielle de la machine virtuelle disponible pour les machines virtuelles vSphere	Vous ne pouvez pas modifier le masque de CPUID d'une machine virtuelle dans votre SDDC.
Modifiez le type de disque virtuel.	Changer la configuration de disque virtuel	Le type de disque de machine virtuelle est géré par la stratégie de stockage VMware Cloud on AWS. Le provisionnement dynamique est le provisionnement par défaut. Les formats de disque Thick et EagerZeroedThick ne sont pas pris en charge. Pour plus d'informations, reportez-vous à la section Utilisation des stratégies vSAN.
Configurez le matériel virtuel.	Configuration matérielle de la machine virtuelle disponible pour les machines virtuelles vSphere	Vous ne pouvez pas créer une machine virtuelle qui inclut un périphérique matériel virtuel nécessitant une modification physique de l'hôte. Cela inclut des choses telles que les ports série, les lecteurs USB et les lecteurs de disquette.
Ajoutez un contrôleur SCSI.	Configuration des contrôleurs de machines virtuelles dans VMware Host Client	Vous pouvez ajouter un contrôleur SCSI mais ne pouvez pas utiliser le partage de bus SCSI virtuel.
Mappez un LUN ou un disque logique brut.	Mappage de périphérique brut	VMware Cloud on AWS ne prend pas en charge le stockage de blocs externes. Vous ne pouvez pas déployer une machine virtuelle qui utilise un disque RDM dans un SDDC de cloud.
Ajoutez un adaptateur réseau.	Notions de base des adaptateurs réseau	VMware Cloud on AWS prend uniquement en charge les adaptateurs E1000E, VMXNET3 et PVRDMA.
Configurez un périphérique de relais PCI ou DirectPath I/O.	DirectPath I/O	Cette fonctionnalité n'est pas prise en charge dans VMware Cloud on AWS.

Tableau 4-2. Options de configuration de machines virtuelles sur site non disponibles dans un SDDC (suite)

Option de configuration	Références	Commentaires
VM chiffrées	Chiffrement des machines virtuelles	Cette fonctionnalité n'est pas prise en charge dans VMware Cloud on AWS.
VM sur lesquelles plusieurs adresses MAC sont configurées pour une vNIC unique.	Comprendre la détection MAC	Étant donné que VMware Cloud on AWS configure la stratégie d'apprentissage MAC NSX sans l'apprentissage MAC, les machines virtuelles ne peuvent pas avoir plusieurs adresses MAC sur la même vNIC.

Configurations de machines virtuelles sur site bloquées ou limitées dans un SDDC de cloud

Certaines options de configuration de machine virtuelle peuvent empêcher l'hôte de passer en mode de maintenance, interférer avec vMotion ou également empêcher VMware d'effectuer des mises à niveau de service. Ces configurations, qui sont autorisées sur site, ont une prise en charge limitée ou ne prennent pas en charge le SDDC de cloud. Si vous téléchargez un modèle avec une configuration non prise en charge à partir de votre bibliothèque de contenu sur site vers votre SDDC de cloud, les machines virtuelles créées à partir du modèle ne seront pas mises sous tension dans le SDDC.

Tableau 4-3. Configurations de machines virtuelles ayant une prise en charge limitée ou nulle dans le SDDC de cloud

Option de configuration	Support	Commentaires
La machine virtuelle inclut un port série avec sortie réseau	Aucun	Cette configuration est bloquée dans le SDDC de cloud
Le disque de machine virtuelle active le multi-lecteur et le service CBT (Changed Block Tracking)	Aucun	Cette configuration est bloquée dans le SDDC de cloud.
La machine virtuelle inclut un adaptateur SR-IOV	Aucun	Cette configuration n'est pas prise en charge dans le SDDC de cloud.
La machine virtuelle inclut un port parallèle	Aucun	Les ports parallèles ne sont pas pris en charge pour le périphérique physique ou la sortie de fichier.
La machine virtuelle utilise le partage de bus virtuel ou physique	Limitée	Les configurations de partage de bus physique sont prises en charge par la version matérielle 11 et versions ultérieures.

Tableau 4-3. Configurations de machines virtuelles ayant une prise en charge limitée ou nulle dans le SDDC de cloud (suite)

Option de configuration	Support	Commentaires
La machine virtuelle monte une image ISO de VMware Tools et débute l'installation ou la mise à niveau des outils.	Limitée	vMotion n'est pas autorisé durant l'installation ou la mise à niveau de VMware Tools. Si le vMotion requis par la maintenance de SDDC est bloqué par une machine virtuelle dans cet état, le système prend quelques minutes pour permettre à l'opération de terminer. Si l'opération ne se termine pas correctement, le système met fin à la mise à niveau ou à l'installation et démonte l'image ISO afin de débloquer l'événement de maintenance. Vous devrez redémarrer manuellement le processus d'installation ou de mise à niveau une fois la maintenance terminée.
Sécurisation des machines virtuelles avec le vTPM (Virtual Trusted Platform Module)	Limitée	■ Requiert I3.en ou des types d'instances plus récents. ■ Aucune mobilité de VM vers d'autres SDDC. Une machine virtuelle disposant d'une configuration vTPM définie dans un SDDC perd cette configuration et ne pourra pas démarrer si elle est déplacée vers un autre SDDC ou migrée vers une instance de vCenter sur site. ■ VMware Cloud on AWS ne peut pas sauvegarder ou restaurer les clés d'un vSphere Native Key Provider vers ou depuis une autre instance de vSphere Native Key Provider. ■ Vous ne pouvez pas cloner une machine virtuelle dans VMware Cloud on AWS si elle dispose d'un périphérique vTPM.

Utilisation de PowerCLI et de l'API des opérations du système invité

Vous pouvez utiliser l'API des opérations du système invité vSphere ou les applets de commande PowerCLI `Invoke-VMScript` et `Copy-VMGuestFile` dans vos workflows de personnalisation pour les machines virtuelles de SDDC.

Conditions préalables

- Configurez l'une de ces connexions ou les deux entre votre environnement sur site et votre SDDC.
  - VPN de gestion
  - Connexion Direct Connect via une interface virtuelle privée (VIF)

  Reportez-vous aux sections Démarrage de VMware Cloud on AWS et Mise en réseau et sécurité de VMware Cloud on AWS.
- Créez une règle de pare-feu de réseau de gestion qui autorise l'accès de votre réseau sur site au port 443 de vos hôtes SDDC. Reportez-vous à la section Ajouter ou modifier des règles de pare-feu de passerelle de gestion.

Procédure

1 Vérifiez que la machine virtuelle exécute la dernière version de VMware Tools.

2 Vérifiez que vous pouvez accéder à l'API des opérations du système invité, directement ou via une applet de commande PowerCLI simple.

Vous pouvez utiliser une applet de commande semblable à celle-ci pour tester la possibilité d'atteindre le port 443 sur l'hôte ESXi à l'adresse IP 10.100.1.1.

```
PS C:\Users\admin>Test-NetConnection -Port 443 -ComputerName 10.100.1.1
```

Une réponse `True` ou `TcpTestSucceeded` confirme la réussite du test.

Exemple : Utilisation de l'applet de commande PowerCLI Invoke-VMScript Cmdlet

Après l'établissement d'une connexion réseau qui autorise le trafic vers le port 443 sur vos hôtes, vous pouvez utiliser l'API des opérations du système invité, directement ou via PowerCLI comme indiqué ici. Les demandes de l'API et de l'applet de commande sont adressées au port 443 sur l'hôte sur lequel s'exécute la machine virtuelle concernée (ici Win10-Example). VMware Tools en cours d'exécution sur la machine virtuelle gère les opérations du système invité demandées.

```
PS C:\Users\admin> $vm = Get-VM Win10-Example
PS C:\Users\admin> Invoke-VMScript -ScriptText "dir C:\" -VM $vm -GuestUser admin
-GuestPassword $passwd"

ScriptOutput
-----------------------------------------------------
|
| Directory: C:\
|
| ...
```

Déployer une machine virtuelle à partir d'un modèle OVF dans une bibliothèque de contenu

Vous pouvez déployer une machine virtuelle à partir d'un modèle OVF dans une bibliothèque de contenu locale ou avec abonnement.

Conditions préalables

Vous devez disposer d'une bibliothèque de contenu contenant le modèle OVF que vous souhaitez utiliser.

- Pour plus d'informations sur la création de bibliothèques de contenu, reportez-vous à la section Créer et modifier une bibliothèque de contenu.
- Pour plus d'informations sur l'importation de contenu dans une bibliothèque de contenu, reportez-vous à la section Comment ajouter du contenu aux bibliothèques.

Procédure

1. Dans la vue VM et modèles de vSphere Client, cliquez avec le bouton droit sur un objet parent valide d'une machine virtuelle, tel que le dossier **Charges de travail**, puis sélectionnez **Nouvelle machine virtuelle**.
2. Sélectionnez **Déployer à partir d'un modèle** et cliquez sur **Suivant**.
3. Sélectionnez le modèle à déployer.
4. Suivez les étapes de l'assistant Nouvelle machine virtuelle, en utilisant les paramètres suivants.
   a. Pour le dossier de machine virtuelle, sélectionnez **Charges de travail**, **Modèles** ou un autre dossier pour lequel vous disposez d'autorisations en écriture.
   b. Pour la ressource de calcul, sélectionnez **Calculer - Pool de ressources**.
   c. Pour la banque de données, sélectionnez **workloadDatastore**.
5. Sur la page Sélectionner les réseaux, entrez une adresse IP dans le champ **Adresse IP**.

   Les **Paramètres d'allocation d'IP** sur cette page affichent uniquement l'option IP statique, même si le réseau logique que vous avez sélectionné utilise le protocole DHCP. Vous devez saisir une valeur dans le champ **Adresse IP** pour passer à l'étape suivante de l'assistant. Si le protocole DHCP est activé, la machine virtuelle est déployée avec DHCP.
6. Vérifiez les paramètres de la machine virtuelle et cliquez sur **Terminer**.