Installation et configuration de VMware Workspace Portal

Workspace Portal 2.1

Ce document prend en charge la version de chacun des produits répertoriés, ainsi que toutes les versions publiées par la suite jusqu'au remplacement dudit document par une nouvelle édition. Pour rechercher des éditions plus récentes de ce document, rendez-vous sur : http://www.vmware.com/fr/support/pubs.

FR-001538-02

vmware®

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

http://www.vmware.com/fr/support/

Le site Web de VMware propose également les dernières mises à jour des produits.

N'hésitez pas à nous transmettre tous vos commentaires concernant cette documentation à l'adresse suivante :

docfeedback@vmware.com

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

VMware, Inc.
100-101 Quartier Boieldieu
92042 Paris La Défense
France
www.vmware.com/fr

Table des matières

À propos de l'installation et de la configuration de VMware Workspace Portal

1

Le *Guide d'installation et de configuration de VMware Workspace Portal* vous présente le processus d'installation et de configuration du dispositif Workspace. Une fois l'installation terminée, vous pouvez utiliser VMware Workspace™ Portal pour octroyer aux utilisateurs un accès géré et multi-périphériques aux applications de votre organisation, notamment aux applications Windows, aux applications SaaS (software as a service) et aux postes de travail View.

Public concerné

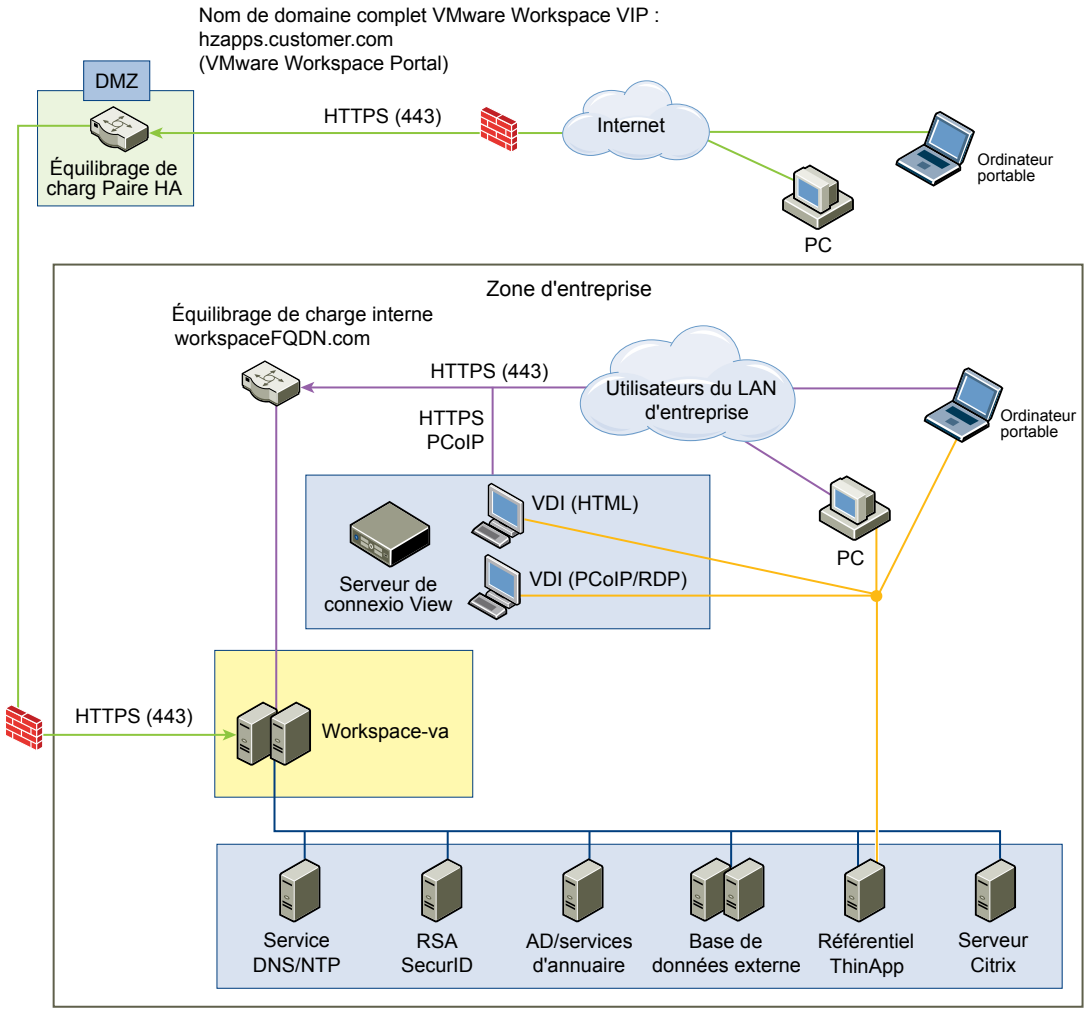
Ces informations sont destinées aux administrateurs système et fonctionnels de VMware Workspace™ Portal. Elles ont été rédigées à l'intention d'administrateurs système Windows et Linux expérimentés et connaissant bien les technologies vCenter™, ESX™, vSphere® et View™, les concepts de mise en réseau, les serveurs Active Directory, le protocole SMTP (Simple Mail Transfer Protocol) et les serveurs NTP. SUSE Linux 11 est le système d'exploitation sous-jacent du dispositif virtuel. La connaissance d'autres technologies, telles que VMware ThinApp®, RSA SecurID et Active Directory est utile si vous prévoyez de mettre en œuvre ces fonctionnalités.

Préparation de l'installation de VMware Workspace Portal

2

Les tâches de déploiement et de configuration de VMware Workspace Portal vous obligent à exécuter les opérations préalables requises, à déployer le fichier Workspace et à effectuer la configuration à partir de l'assistant de configuration de Workspace.

Figure 2-1. Diagramme de l'architecture de VMware Workspace Portal pour des déploiements standards



Ce chapitre aborde les rubriques suivantes :

Exigences de configuration du système et du réseau Workspace

Considérez l'intégralité de votre déploiement Workspace, y compris votre façon d'intégrer Workspace à vos décisions concernant les exigences en matériel, en ressources et en matière de réseau.

Configuration requise du dispositif virtuel Workspace

Assurez-vous que les ressources allouées au dispositif virtuel Workspace répondent aux exigences minimales.

Tableau 2-1. Configuration requise du dispositif virtuel VMware Workspace Portal (workspace-va)

Composant	Exigences minimales
CPU	2
RAM	6 Go
Espace disque	36 Go
Remarques additionnelles	■ Une base de données PostgreSQL est incluse dans la configuration workspace-va et vous pouvez utiliser un serveur de base de données externe. Pour plus d'informations sur les versions de base de données et configurations de Service Pack spécifiques prises en charge par Workspace, consultez les matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. ■ Informations sur le dimensionnement de la base de données externe : 64 Go pour les 100 000 premiers utilisateurs Ajoutez 20 Go pour chaque tranche de 10 000 utilisateurs supplémentaires. ■ Stockage : 32 Go

Exigences de configuration réseau

Le serveur Workspace doit joindre le domaine Windows si les fonctions Kerberos, View ou ThinApp sont activées. Dans ce cas, le nom d'hôte Workspace doit se situer dans le même domaine que le domaine Active Directory auquel il se joint.

Tableau 2-2. Exigences de configuration réseau

Composant	Exigences minimales
Enregistrement DNS et adresse IP	Adresse IP et enregistrement DNS
Port du pare-feu	Assurez-vous que le port entrant 443 du pare-feu est ouvert aux utilisateurs hors du réseau de l'entreprise qui accèdent à Workspace.

Exigences du port

Les ports utilisés dans Workspace sont décrits ci-dessous. Votre déploiement peut inclure uniquement un sous-ensemble de ceux-ci. Voici deux scénarios potentiels :

- Pour synchroniser les utilisateurs et les groupes, le dispositif virtuel Workspace doit se connecter à Active Directory.
- Pour se synchroniser sur ThinApp, la machine virtuelle Workspace doit joindre le domaine Active Directory et se connecter au partage de référentiel ThinApp.

Tableau 2-3. Ports utilisés par Workspace

Port	Source	Cible	Description
443	Équilibrage de charge	Workspace-va	HTTPS (Hypertext Transport Protocol over SSL)
443	Workspace-va	Workspace-va 2, 3, etc.	HTTPS (Hypertext Transport Protocol over SSL)
443	Navigateurs	Workspace-va	HTTPS (Hypertext Transport Protocol over SSL)
8443	Navigateurs	Workspace-va	Port administrateur HTTPS (Hypertext Transport Protocol over SSL)
25	Workspace-va	SMTP	Port TCP pour le relais du courrier sortant
389, 636, 3268, 3269	Workspace-va	Active Directory	Les valeurs par défaut sont affichées. Ces ports sont configurables.
5432	Workspace-va	Base de données	Le port PostgreSQL par défaut est 5432. Le port Oracle par défaut est 1521.
389, 443	Workspace-va	View Server	Accès à View Server
443	Workspace-va	Référentiel ThinApp VMware	Accès au référentiel ThinApp
5500	Workspace-va	Système RSA SecurID	La valeur par défaut est affichée. Ce port est configurable
53	Workspace-va	Serveur DNS	TCP/UDP Chaque workspace-va doit avoir accès au serveur DNS sur le port 53 et autoriser le trafic SSH entrant sur le port 22
88, 465, 135	Workspace-va	Contrôleur de domaine	TCP/UDP
TCP : 9300 à 9400 UDP : 54328	Workspace-va	Workspace-va	Besoins d'audit

Exigences matérielles d'ESX Server

Assurez-vous que l'environnement de l'hôte et de l'instance vSphere qui exécute le dispositif virtuel Workspace répond aux exigences matérielles minimales. Les exigences de stockage varient selon le déploiement, en fonction du nombre d'utilisateurs.

Remarque Vous devez activer la synchronisation horaire au niveau de l'hôte ESX à l'aide d'un serveur NTP. Sinon, une dérive horaire se produira entre les dispositifs virtuels.

Tableau 2-4. Exigences matérielles minimales d' Workspace

Composant	Exigences minimales
Processeur	2 Intel à quatre cœurs, 3.0 GHz, 4 Mo de cache
RAM	16 Go DDR2 1066 MHz, ECC et enregistrée
LAN embarqué	Un port 10/100/1000Base-TX
Stockage	500 Go

Navigateurs Web pris en charge pour Workspace

La console d'administration de Workspace est une application Web installée lors de l'installation de Workspace. Vous pouvez accéder à la Console d'administration Workspace à partir des navigateurs suivants.

- Internet Explorer 10 et 11 pour les systèmes Windows
- Google Chrome 34.0 ou version ultérieure pour les systèmes Windows et Mac
- Mozilla Firefox 28 ou version ultérieure pour les systèmes Windows et Mac
- Safari 6.1.3 et version ultérieure pour les systèmes Mac

Préparation au déploiement d' Workspace

Avant de déployer Workspace, vous devez préparer votre environnement. Cette préparation inclut le téléchargement du fichier OVF de Workspace, ainsi que la création d'enregistrements DNS et d'adresses IP.

Prérequis

Avant de commencer à installer Workspace, effectuez les tâches préalables.

- Un ou plusieurs serveurs ESX pour déployer le dispositif virtuel Workspace.

  REMARQUE Pour obtenir des informations sur les versions des serveurs vSphere et ESX prises en charge, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.

- VMware vSphere Client ou vSphere Web Client est requis pour déployer le fichier OVF et pour accéder au dispositif virtuel déployé à distance afin de configurer la mise en réseau.
- Fichier OVF de Workspace provenant du site Web de VMware.
- Créer des enregistrements DNS et des adresses IP page 11

  Le dispositif Workspace doit disposer d'une entrée DNS et d'une adresse IP statique . Du fait que chaque entreprise administre ses adresses IP et ses enregistrements DNS de manière différente, avant de commencer l'installation, demandez l'enregistrement DNS et les adresses IP à utiliser.

- Options de base de données dans Workspace page 11

  Workspace peut être configuré avec une base de données interne ou externe. Une base de données vPostgres est intégrée au dispositif Workspace. Par défaut, la base de données est interne. Vous pouvez choisir de vous connecter à une base de données externe lorsque vous configurez l'assistant Configuration de Workspace.

- Se connecter à Active Directory page 12

  Workspace utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour synchroniser les utilisateurs et les groupes, le dispositif virtuel Workspace doit se connecter à Active Directory.

- Listes de vérification de déploiement page 12

  Vous pouvez utiliser les listes de vérification de déploiement d'Workspace pour collecter les informations nécessaires à son installationWorkspace.

Créer des enregistrements DNS et des adresses IP

Le dispositif Workspace doit disposer d'une entrée DNS et d'une adresse IP statique . Du fait que chaque entreprise administre ses adresses IP et ses enregistrements DNS de manière différente, avant de commencer l'installation, demandez l'enregistrement DNS et les adresses IP à utiliser.

(Facultatif) Recherche inversée et adresses IP

La configuration de la recherche inversée est facultative dans Workspace. Lorsque vous implémentez la recherche inversée, vous devez définir un enregistrement PTR sur le serveur DNS afin que le dispositif virtuel utilise la configuration réseau adéquate.

Vous pouvez utiliser l'exemple de liste d'enregistrements DNS suivant lorsque vous parlez avec votre administrateur réseau. Remplacez les informations de l'exemple par les informations de votre environnement. Cet exemple montre des enregistrements DNS et des adresses IP qui utilisent la résolution.

Tableau 2-5. Exemples d'enregistrements DNS et d'adresses IP qui utilisent la résolution

Nom de domaine	Type de ressource	Adresse IP
my-workspace-va.company.com	Aoû	10.28.128.3

Cet exemple montre des enregistrements DNS et des adresses IP qui utilisent la résolution inverse

Tableau 2-6. Exemples d'enregistrements DNS et d'adresses IP qui utilisent la résolution inverse

Adresse IP	Type de ressource	Nom de domaine
128.28.10.in-addr.arpa.	IN	PTR my-workspace-va.company.com

Après avoir terminé la configuration DNS, vérifiez que la résolution DNS inverse est configurée correctement. Par exemple, la commande de dispositif virtuel *host IP_address* doit être résolue en recherche de nom DNS.

Utilisation d'un serveur DNS basé sur Unix/Linux

Si vous utilisez un serveur DNS basé sur Unix/Linux et prévoyez de joindre Workspace au domaine Active Directory, assurez-vous que les enregistrements de la ressource de service (SRV) appropriée sont créés pour chaque contrôleur de domaine Active Directory.

Options de base de données dans Workspace

Workspace peut être configuré avec une base de données interne ou externe. Une base de données vPostgres est intégrée au dispositif Workspace. Par défaut, la base de données est interne. Vous pouvez choisir de vous connecter à une base de données externe lorsque vous configurez l'assistant Configuration de Workspace.

La configuration de la base de données vPostgres intégrée est utile pour les petits déploiements et elle peut être utilisée par défaut. La base de données interne ne nécessite aucune configuration supplémentaire en dehors de Workspace, mais nous vous recommandons de configurer la base de données interne pour la haute disponibilité. Consultez l'article 2094258 de la base de connaissances, Utilisation d'une base de données vPostgres intégrée pour VMware Workspace Portal 2.1.

Pour utiliser une base de données externe, votre administrateur de base de données doit préparer une base de données et un schéma externes et vides avant de se connecter à la base de données externe. Les utilisateurs sous licence peuvent utiliser un dispositif virtuel vPostgres ou une base de données Oracle externe pour configurer un environnement de base de données externe à haute disponibilité. Voir « Connexion à une base de données externe », page 24.

Se connecter à Active Directory

Workspace utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Pour synchroniser les utilisateurs et les groupes, le dispositif virtuel Workspace doit se connecter à Active Directory.

Votre annuaire Active Directory doit être accessible sur le même réseau local que celui du dispositif virtuel Workspace. Voir « Établissement d'une connexion à Active Directory », page 36

Listes de vérification de déploiement

Vous pouvez utiliser les listes de vérification de déploiement d'Workspace pour collecter les informations nécessaires à son installationWorkspace.

En fonction de votre déploiement, vous pouvez n'avoir besoin que d'une partie des informations réseau pour vos dispositifs virtuels lorsque vous créez les adresses IP statiques dans le DNS avant et pendant l'installation de Workspace.

Informations sur le nom de domaine complet

Voir « Utilisation d'un équilibrage de charge pour activer l'accès externe à Workspace », page 43 pour plus d'informations.

Tableau 2-7. Liste de vérification des informations sur le nom de domaine complet (FQDN) de Workspace

Informations à collecter	Afficher les informations
FQDN d'Workspace	

Informations réseau sur le dispositif virtuel Workspace

Tableau 2-8. Liste de vérification des informations réseau d' Workspace

Informations à collecter	Afficher les informations
adresse IP	
Nom DNS de ce dispositif virtuel	
Adresse de la passerelle par défaut	
Masque réseau ou préfixe	

contrôleur de domaine Active Directory

Tableau 2-9. Liste de vérification des informations du contrôleur de domaine Active Directory

Informations à collecter	Afficher les informations
Nom du serveur Active Directory	
Nom du domaine Active Directory	
Nom d'utilisateur et mot de passe ND Bind	
ND de base	
Nom d'utilisateur et mot de passe Active Directory (doit avoir les privilèges nécessaires pour ajouter des ordinateurs au domaine)	

Certificat SSL (facultatif)

Tableau 2-10. Liste de vérification des informations du certificat SSL

Informations à collecter	Afficher les informations
certificat SSL	
Clé privée	

REMARQUE Le certificat SSL est facultatif. Vous pouvez ajouter un certificat SSL après le déploiement d'Workspace.

Clé de licence Workspace

Tableau 2-11. Liste de vérification des informations de la clé de licence Workspace

Informations à collecter	Afficher les informations
Clé de licence	

REMARQUE Les informations sur la clé de licence sont entrées dans la console d'administration Workspace dans l'onglet Paramètres > Paramètres globaux une fois l'installation terminée.

Base de données externe

Tableau 2-12. Liste de vérification des informations de la base de données externe

Informations à collecter	Afficher les informations
Nom d'hôte de la base de données	
Port	
Nom d'utilisateur	
Mot de passe	

Mots de passe Workspace

Tableau 2-13. Mot de passe d'administration utilisé dans Workspace

Informations à collecter	Afficher les informations
Mot de passe du compte d'administrateur Workspace	
Mot de passe du compte racine du dispositif virtuel	
Mot de passe du compte Sshuser pour une connexion à distance	

Déploiement d' Workspace 3

Les tâches visant à déployer et à configurer Workspace à l'aide de vSphere Client ou de vSphere Web Client inclut le déploiement du modèle OVF, le démarrage du dispositif virtuel Workspace et la configuration de Workspace.

Une fois le dispositif virtuel Workspace déployé, vous utilisez l'assistant de configuration de Workspace pour configurer l'environnement de Workspace.

Utilisez les informations des listes de contrôle du déploiement pour terminer l'installation. Voir « Listes de vérification de déploiement », page 12.

Ce chapitre aborde les rubriques suivantes :

Installer le fichier OVF de Workspace

Pour commencer l'installation de Workspace, vous devez déployer le fichier OVF à l'aide de VMware vSphere Client ou de vSphere Web Client. Vous pouvez télécharger et déployer le fichier OVF à partir d'un fichier local accessible à vSphere Client ou à partir d'une URL Web.

Prérequis

- Avec vSphere Web Client, utilisez les navigateurs Firefox ou Chrome. N'utilisez pas Internet Explorer pour déployer les fichiers OVF.
- Téléchargez le fichier OVF de Workspace.

Procédure

1 À partir de vSphere Client ou de vSphere Web Client, sélectionnez **Modèle OVF** pour déployer le fichier OVF de Workspace.

2 Dans les pages Déployer le modèle OVF, entrez les informations spécifiques de votre déploiement de Workspace.

Page	Description
Source	Localisez l'emplacement du module OVF ou entrez une URL spécifique.
Détails du modèle OVF	Vérifiez que vous avez sélectionné la version correcte de Workspace.
Licence	Lisez l'accord de licence d'utilisateur final et cliquez sur **Accepter**.
Nom et emplacement	Entrez le nom identifiant ce dispositif virtuel Workspace. Il doit être unique dans le dossier de la machine virtuelle. Les noms sont sensibles à la casse.
Hôte / Cluster	Sélectionnez l'hôte ou le cluster pour exécuter le modèle déployé.
Pool de ressources	Sélectionnez le pool de ressources.
Stockage	Sélectionnez l'emplacement de stockage des fichiers des machines virtuelles.
Format du disque	Sélectionnez le format du disque sur lequel stocker les fichiers Workspace. Pour les environnements de production, sélectionnez le format de provisionnement épais. Utilisez le format de provisionnement fin pour les évaluations et les tests.
Mappage réseau	Mappez les réseaux utilisés dans Workspace aux réseaux de votre inventaire.
Propriétés	**Remarque** Pour déployer Workspace, laissez la case Section d'application non cochée. Dans le champ du Paramètre de fuseau horaire, sélectionnez le fuseau horaire correspondant. Le Programme d'amélioration du produit est activé par défaut. VMware collecte des données anonymes sur votre déploiement afin d'améliorer la réponse de VMware aux exigences des utilisateurs. Dans le champ Nom de l'hôte, entrez le nom d'hôte à utiliser. Si ce champ est vide, le DNS inversé est utilisé pour rechercher le nom d'hôte. Pour configurer l'adresse IP statique de Workspace, entrez l'adresse de chacun des champs suivants : Passerelle par défaut, DNS, Adresse IP et Masque réseau. **Important** Si l'un des quatre champs d'adresse, y compris le nom d'hôte, sont vides, le protocole DHCP est utilisé. Pour configurer le protocole DHCP, laissez les champs d'adresse vides. (Facultatif) Une fois Workspace installé, vous pouvez configurer les pools d'adresses IP. Voir « (Facultatif) Ajouter des pools IP dans Workspace », page 17.
Prêt à terminer	Vérifiez les options que vous avez sélectionnées. Si les informations sont correctes, cliquez sur **Terminer**.

Une barre de progression s'affiche. Selon la vitesse de votre réseau, ce déploiement peut nécessiter plusieurs minutes.

3 Une fois le déploiement terminé, cliquez sur **Fermer** dans la barre de progression.

4 Sélectionnez le dispositif virtuel Workspace que vous venez de déployer et cliquez sur **Mettre la machine virtuelle sous tension**.

Le dispositif virtuel Workspace est initialisé. Vous pouvez accéder à l'onglet Console pour voir les détails. Une fois l'initialisation du dispositif virtuel terminée, l'écran de la console affiche la version de Workspace et les URL pour vous connecter à l'interface Web de Workspace et terminer la configuration de Workspace.

Suivant

Configurez les paramètres de Workspace, notamment la connexion à Active Directory et la sélection d'utilisateurs et de groupes à synchroniser avec Workspace.

(Facultatif) Ajouter des pools IP dans Workspace

La configuration réseau avec un pool IP est facultative dans Workspace. Vous pouvez ajouter manuellement des pools IP à Workspace une fois Workspace installé. Vous modifiez les propriétés de mise en réseau du dispositif virtuel workspace-va afin de changer les propriétés en propriétés dynamiques et configurez les paramètres de masque réseau, de passerelle et DNS.

Les pools d'adresses IP agissent comme des serveurs DHCP (Dynamic Host Configuration Protocol) pour attribuer des adresses IP du pool au dispositif virtuel workspace-va. Pour permettre au dispositif Workspace d'utiliser des pools IP, vous devez modifier ses propriétés OVF.

Prérequis

Le dispositif virtuel workspace-va doit être mis hors tension pour ajouter les paramètres de pools IP.

Procédure

1 Dans vSphere Client ou vSphere Web Client, cliquez avec le bouton droit sur le dispositif virtuel que vous configurez pour les pools IP, puis sélectionnez **Modifier les paramètres**.

2 Cliquez sur **Propriétés** dans la section Propriétés de la page.

3 Sur la page Configuration avancée des propriétés, configurez les étiquettes de clé suivantes : vami.DNS.WorkspacePortal, vami.netmask0.WorkspacePortal et vami.gateway.WorkspacePortal.

   a Sur la page Configuration avancée des propriétés, sélectionnez l'une des étiquettes de clé et cliquez sur **Modifier**.

   b Sur la page Modifier les paramètres de propriété, en regard du champ Type, cliquez sur **Modifier**.

   c Sur la page Modifier le type de propriété, sélectionnez **Propriété dynamique** puis choisissez dans le menu déroulant la valeur appropriée au masque réseau, à la passerelle et aux serveurs DNS, respectivement.

   d Cliquez sur **OK** jusqu'à ce que toutes les pages soient fermées.

4 Mettez sous tension le dispositif virtuel.

Les propriétés sont configurées pour effectuer une sélection à partir des pools IP.

Configurer les paramètres de Workspace

Une fois le fichier OVF de Workspace déployé et installé, vous exécutez l'assistant de configuration de Workspace pour configurer les informations de connexion à votre annuaire Active Directory ; créez une base de données externe ou sélectionnez une base de données externe si vous en utilisez une, puis sélectionnez les utilisateurs et les groupes à synchroniser avec Workspace.

Prérequis

- Dispositif virtuel Workspace sous tension.
- Liste des mots de passe à utiliser pour l'administrateur de Workspace, le compte root de Workspace et le compte Sshuser de Workspace.
- Si vous utilisez une base de données externe, celle-ci doit être configurée et ses informations de connexion disponibles.
- Informations de connexion à Active Directory.

- Lorsqu'une instance d'Active Directory à forêts multiples est configurée et que le groupe local du domaine contient des membres de domaines situés dans différentes forêts, l'utilisateur Bind DN utilisé sur la page Workspace Directory doit être ajouté au groupe d'administrateurs du domaine dans lequel réside le groupe local du domaine. Sinon, ces membres ne seront pas présents dans le groupe local du domaine.
- Liste des attributs utilisateur Active Directory à utiliser comme filtres et liste des groupes à ajouter à Workspace.

Procédure

1 Pour configurer Workspace une fois le fichier OVF déployé, accéder à l'URL de Workspace, `https://workspacehostname.com`.

Sur l'écran d'accueil, cliquez sur **Continuer**.

2 Sur la page Définir des mots de passe, créez des mots de passe pour les comptes d'administrateurs suivants.

- Administrateur du dispositif. Créez le mot de passe administrateur de Workspace. Le nom d'utilisateur est admin et ne peut pas être modifié. Ce compte a été créé pendant l'installation initiale de Workspace.
- Compte root. Un mot de passe racine VMware par défaut a été utilisé pour configurer Workspace. Créez un nouveau mot de passe racine.
- Compte Sshuser. Créez le mot de passe à utiliser pour accéder à distance au dispositif virtuel workspace-va.

Cliquez sur **Continuer**.

3 Sélectionnez la base de données à utiliser.

- Si vous utilisez une base de données interne, cliquez sur **Continuer**.
- Si vous utilisez une base de données externe, sélectionnez **Base de données externe** et entrez les informations de connexion à la base de données externe, le nom d'utilisateur et le mot de passe, du serveur de base de données que vous avez configuré précédemment. Pour vérifier que Workspace peut se connecter à la base de données, cliquez sur **Tester la connexion**.

Cliquez sur **Continuer**.

La connexion à la base de données est configurée et la base de données est initialisée.

4 Sur la page Annuaire, entrez vos informations Active Directory et cliquez sur **Vérifier**.

Type d'informations	Description
Type de dossier	Laissez-le sur Active Directory.
Utiliser SSL	Cochez cette case si vous utilisez SSL pour vous connecter au dossier.
Utiliser l'emplacement du service DNS	Cochez cette case si l'emplacement du service DNS est utilisé pour vous connecter au dossier.
Hôte du serveur	Entrez l'adresse de l'hôte Active Directory. N'utilisez pas de caractères non-ASCII lorsque vous entrez le nom d'hôte.
Port du serveur	Entrez le numéro de port de l'hôte Active Directory. Pour un domaine Active Directory unique, le port par défaut est 389. Lorsque SSL est sélectionné, le port par défaut est 636.
Attribut de recherche	Entrez l'attribut du compte Active Directory contenant le nom d'utilisateur. Pour la plupart des déploiements, sélectionnez **`sAMAccouontName`**.
ND de base	Entrez le nom unique (DN) qui est le point de départ pour les recherches sur le serveur d'annuaire. Par exemple, OU-myunit,DC=mycompany,DC=com.

Type d'informations	Description
ND Bind	Entrez le nom unique ND Bind, incluant le nom commun (NC), du compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. Cet utilisateur devient un administrateur de votre déploiement de Workspace.
Mot de passe Bind	Entrez le mot de passe Active Directory du compte ND Bind.

Les informations ND Bind sont confirmées et le compte de l'administrateur est ajouté en tant qu'utilisateur dans Workspace.

Cliquez sur **Continuer**.

5 Sur la page Association des attributs utilisateur, sélectionnez les attributs utilisés dans Active Directory qu correspondent aux attributs de l'annuaire Workspace.

Si vous prévoyez d'intégrer View, sélectionnez **Requis** situé en regard de l'attribut userPrincipal Name. Si vous prévoyez d'intégrer Horizon DaaS, sélectionnez **Requis** situé en regard de l'attribut distinguishedName. Vous pouvez également le faire ultérieurement à partir des page de Administrateur de Connector Services.

6 Sur la page Sélectionner les utilisateurs, sélectionnez les attributs utilisateur dans le menu déroulant pour créer des filtres visant à restreindre le type d'utilisateurs se synchronisant avec Workspace. Cliquez sur **Continuer**.

7 Les groupes d'Active Directory ne se synchronisent pas automatiquement avec Workspace. Sur la page Groupes sélectionnés, cliquez sur **Ajouter** situé en regard d'une description DN du groupe pour ajouter le groupe. Cliquez sur **Continuer**.

La Page Transmettre à Workspace affiche des informations sur le nombre d'utilisateurs et de groupes à synchroniser avec Workspace.

Cliquez sur **Transmettre à Workspace** pour commencer la synchronisation.

8 Lorsque la page Configuration complète s'affiche, cliquez sur **Se connecter à Workspace** pour vous connecter à la console d'administration.

L'écran de connexion de Workspace s'affiche. Entrez le nom d'utilisateur et le mot de passe ND Bind que vous avez entrés quand vous avez configuré la connexion à Active Directory. Dans le Console d'administration Workspace, vous pouvez configurer les ressources pour utiliser Workspace et attribuer des utilisateurs à ces ressources.

Remarque Si une erreur de mise en réseau se produit et si le nom d'hôte ne peut pas être résolu de manière unique à l'aide de la résolution DNS inverse, le processus du Programme de configuration s'arrête. Vous devez corriger les problèmes de mise en réseau et redémarrer le dispositif virtuel workspace-va. Vous pouvez ensuite poursuivre le processus de déploiement. Les nouveaux paramètres réseau ne seront disponibles qu'après le redémarrage du dispositif virtuel workspace-va.

Suivant

Connectez-vous à la console d'administration de Workspace pour personnaliser un catalogue de ressources pour les applications de votre entreprise et autorisez les utilisateurs à y accéder.

Configurez les autres ressources, notamment les applications View, ThinApp, Horizon DaaS et Citrix. Reportez-vous à *Configuration des ressources dans le Guide de VMware Workspace Portal* .

Définir des paramètres de serveur proxy pour Workspace

Le dispositif virtuel Workspace accède au catalogue d'applications Cloud et à d'autres services Web via Internet. Si votre configuration réseau fournit un accès à Internet via un proxy HTTP, vous devez régler les paramètres de votre proxy sur chaque dispositif Workspace.

Autorisez uniquement la gestion du trafic Internet sur votre serveur proxy. Pour vous assurer que le serveur proxy est correctement configuré, définissez le paramètre du trafic interne sur `no–proxy` dans le domaine.

Procédure

1 Dans vSphere Client, connectez-vous en tant qu'utilisateur root au dispositif virtuel workspace-va.

2 Tapez **YaST2**.

3 Sélectionnez **Services réseau**, puis sélectionnez la page **Proxy**.

4 Entrez l'URL de proxy appropriée dans le champ HTTP.

http://proxy.example.com:3128

5 Entrez l'URL de proxy appropriée dans le champ HTTPS.

https://proxy.example.com:3128

6 Redémarrez le serveur Tomcat sur la machine virtuelle workspace-va pour utiliser les nouveaux paramètres de proxy.

```
#service horizon–workspace restart
```

Le catalogue d'applications Cloud et autres services Web sont désormais disponibles dans Workspace.

Services administratifs de Workspace

Vous gérez les utilisateurs, les groupes, les ressources, l'authentification, la configuration de la synchronisation et la connexion de la base de données de Workspace à partir de différents services administratifs de Workspace.

Service	Description
Console d'administration Workspace	Dans l'interface de la console d'administration de Workspace, vous configurez le catalogue de ressources et administrez vos utilisateurs et vos groupes, les droits d'accès et les rapports. Vous vous connectez sous le rôle d'utilisateur administrateur attribué depuis Active Directory. L'URL permettant de se connecter directement à la console d'administration est https://*WorkspaceFQDN*/SAAS/admin.
Administrateur de Connector Services	Sur les pages Administrateur des services de connecteur, vous configurez le répertoire et vos adaptateurs d'authentification, et vous administrez d'autres intégrations d'entreprise, comme les postes de travail virtuels et les applications distantes. Cela inclut la configuration de l'intégration au serveur de connexion View, au référentiel ThinApp et aux ressources d'application publiées Citrix. À partir de ces pages, vous pouvez également vérifier l'état de synchronisation et les alertes des annuaires. Vous vous connectez en tant qu'administrateur de Workspace, en utilisant le nom d'utilisateur **`admin`** et le mot de passe admin que vous avez créés lors de la configuration de Workspace. Vous trouverez un lien vers les pages Administrateur des services de connecteur à l'adresse https://*Workspace_FQDN*.com:8443.
Configurateur de dispositifs	Sur les pages Programme de configuration du dispositif, vous pouvez gérer la base de données de Workspace, mettre à jour les certificats, activer Syslog, modifier les mots de passe Workspace et système et gérer d'autres fonctions d'infrastructure. Vous vous connectez en tant qu'administrateur de Workspace, en utilisant le nom d'utilisateur **`admin`** et le mot de passe admin que vous avez créés lors de la configuration de Workspace. Un lien vers les pages Configurateur de dispositifs est accessible à l'adresse https://*Workspace_FQDN*.com:8443. Vous pouvez également accéder aux pages de Configurateur de dispositifs à partir de Console d'administration Workspace, page Paramètres > Configuration système du dispositif virtuel.

Programme d'amélioration du produit

Lorsque vous installez Workspace, vous pouvez choisir de participer au Programme d'amélioration du produit de VMware.

Si vous participez au programme, VMware collecte des données anonymes sur votre déploiement afin d'améliorer sa réponse aux exigences du client. Aucune donnée identifiant votre organisation n'est collectée.

Avant de collecter les données, VMware rend anonymes tous les champs contenant des informations propres à votre organisation.

Remarque Si la configuration de votre réseau prévoit un accès Internet via un proxy HTTP, pour envoyer ces informations vous devez ajuster vos paramètres de proxy sur le dispositif Workspace. Voir « Définir des paramètres de serveur proxy pour Workspace », page 20

Gérer les paramètres de configuration du dispositif Workspace

4

Après avoir configuré Workspace, vous pouvez accéder aux pages Programme de configuration du dispositif pour mettre à jour la configuration actuelle et surveiller les informations système du dispositif virtuel.

Vous pouvez mettre à jour ou modifier les paramètres de votre base de données, le FQDN et les certificats SSL, et plus encore sur les pages de Configurateur de dispositifs.

Tableau 4-1. Paramètres du Programme de configuration du dispositif

Nom de la page	Paramètre Description
Connexion à la base de données	Le paramètre de connexion à la base de données, interne ou externe, est activé. Vous pouvez modifier le type de la base de données. Lorsque vous sélectionnez la base de données externe, vous entrez son URL, son nom d'utilisateur et son mot de passe. Pour configurer une base de données externe, reportez-vous à « Connexion à une base de données externe », page 24.
Installer le certificat	Dans cette page, vous installez un certificat personnalisé ou auto-signé pour Workspace et, si Workspace est configuré avec un équilibrage de charge, vous pouvez installer le certificat racine de l'équilibrage de charge. L'emplacement du certificat de l'autorité de certification racine de Workspace s'affiche également sur cette page. Voir « Utilisation des certificats SSL dans Workspace », page 29.
FQDN de Workspace	Le FQDN de Workspace s'affiche sur cette page. Vous pouvez le modifier. Le FQDN de Workspace correspond à l'URL que les utilisateurs utilisent pour accéder à Workspace.
Configurer Syslog	Sur cette page, vous pouvez activer un serveur syslog externe. Les journaux de Workspace sont envoyés à ce serveur externe. Voir « Activation du serveur Syslog », page 28.
Changer le mot de passe	Sur cette page, vous pouvez changer le mot de passe administrateur de Workspace.
Sécurité du système	Sur cette page, vous pouvez changer le mot de passe root du dispositif Workspace et le mot de passe utilisé pour se connecter à distance en tant qu'administrateur.
Emplacements des fichiers journaux	Cette page affiche une liste des fichiers journaux de Workspace et les emplacements de leurs répertoires. Vous pouvez rassembler les fichiers journaux dans un fichier tar.zip et le télécharger depuis cette page. Voir « Informations sur le fichier journal », page 30.

Ce chapitre aborde les rubriques suivantes :

Modifier les paramètres de configuration du dispositif Workspace

Après avoir configuré Workspace, vous pouvez accéder aux pages Programme de configuration du dispositif pour mettre à jour la configuration actuelle et surveiller les informations système du dispositif virtuel.

Procédure

1 Pour accéder aux pages programme de configuration du dispositif, connectez-vous à Console d'administration Workspace.

2 Ouvrez l'onglet Paramètres et cliquez sur **Configuration système du dispositif virtuel**.

3 Connectez-vous à Configurateur de dispositifs avec le mot de passe administrateur de Workspace.

4 Utilisez le volet de navigation gauche pour sélectionner la page à consulter.

Suivant

Vérifiez que les paramètres que vous définissez ou les mises à jour que vous effectuez sont maintenant appliqués.

Connexion à une base de données externe

Une base de données PostgreSQL interne est intégrée au dispositif Workspace. Pour utiliser une base de données externe avec Workspace, votre administrateur de base de données doit préparer une base de données et un schéma Oracle ou PostgreSQL externes et vides avant de se connecter à la base de données dans Workspace.

Vous pouvez vous connecter à la base de données externe lorsque vous exécutez l'assistant de configuration de Workspace. Vous pouvez également accéder à la page Connexion à la base de données Configurateur de dispositifs pour configurer la connexion à la base de données externe.

Les utilisateurs sous licence peuvent utiliser un dispositif virtuel vPostgres ou une base de données Oracle externe pour configurer un environnement à haute disponibilité.

Remarque Pour configurer votre base de données interne pour la haute disponibilité, consultez l'article 2094258 de la base de connaissances, Utilisation d'une base de données vPostgres intégrée pour VMware Workspace Portal 2.1.

Configuration d'une base de données Oracle

Pendant l'installation d'Oracle, vous devez spécifier certaines configurations Oracle pour optimiser les performances avec Workspace.

Prérequis

Workspace nécessite des identificateurs Oracle entre guillemets pour le nom d'utilisateur et le schéma. Par conséquent, vous devez utiliser des guillemets doubles lors de la création du nom d'utilisateur et du schéma `saas` Oracle.

Procédure

1 Spécifiez les paramètres suivants lors de la création d'une base de données Oracle.

   a Sélectionnez l'option de configuration **General Purpose/Transaction Processing Database**.

   b Cliquez sur **Use Unicode > UTF8**.

   c Utilisez le jeu de caractères national.

2 Connectez-vous à la base de données Oracle une fois l'installation terminée.

3 Connectez-vous à la base de données Oracle en tant qu'utilisateur sys.

4 Augmentez le nombre de connexions de processus. Chaque machine virtuelle workspace-va supplémentaire nécessite la connexion d'au minimum 300 processus pour fonctionner avec Workspace. Par exemple, si votre environnement dispose de deux machines virtuelles workspace-va, exécutez la commande `alter` en tant qu'utilisateur sys ou système.

   a Augmentez le nombre de connexions de processus à l'aide de la commande `alter`.

   ```
   alter system set processes=600 scope=spfile
   ```

   b Redémarrez la base de données.

5 Créez un déclencheur de base de données que tous les utilisateurs peuvent utiliser.

Exemple de code SQL de création d'un déclencheur de base de données

```
CREATE OR REPLACE
TRIGGER CASE_INSENSITIVE_ONLOGON
AFTER LOGON ON DATABASE
DECLARE
username VARCHAR2(30);
BEGIN
username:=SYS_CONTEXT('USERENV','SESSION_USER');
IF username = 'saas' THEN
execute immediate 'alter session set NLS_SORT=BINARY_CI';
execute immediate 'alter session set NLS_COMP=LINGUISTIC';
END IF;
EXCEPTION
WHEN OTHERS THEN
NULL;
END;
```

6 Exécutez les commandes Oracle pour créer un schéma d'utilisateur.

Exemple de code SQL de création d'un utilisateur

```
CREATE USER "saas"
IDENTIFIED BY <password>
DEFAULT TABLESPACE USERS
TEMPORARY TABLESPACE TEMP
PROFILE DEFAULT
ACCOUNT UNLOCK;
GRANT RESOURCE TO "saas" ;
GRANT CONNECT TO "saas" ;
ALTER USER "saas" DEFAULT ROLE ALL;
GRANT UNLIMITED TABLESPACE TO "saas";
```

Si vous utilisez une base de données Oracle en cluster, consultez la documentation VMware sur l'installation de RAC.

Configuration d'une base de données PostgreSQL

Pendant l'installation de PostgreSQL, vous devez spécifier certaines configurations PostgreSQL pour optimiser les performances avec Workspace.

REMARQUE Workspace ne prend actuellement pas en charge PostgreSQL générique.

Prérequis

- Installez et configurez une version prise en charge de VMware vFabric PostgreSQL en tant que serveur de base de données externe avec l'un des modules d'installation, par exemple OVA, OVF ou RPM, le module citext étant installé. Le module citext prend en charge le type de données CITEXT, un type de texte insensible à la casse. Vérifiez que la version de VMware vFabric PostgreSQL que vous utilisez est compatible avec la version d'Workspace. Pour obtenir des informations sur les versions de VMware vFabric PostgreSQL prises en charge, reportez-vous aux matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Installez et configurez l'implémentation de l'équilibrage de charge.
- Vérifiez que votre environnement remplit les conditions suivantes :
  - Vous utilisez le serveur de base de données PostgreSQL.
  - Le nom d'utilisateur et le mot de passe de l'administrateur de la base de données sont disponibles.
  - Vous devez entrer un nom d'utilisateur et un mot de passe pour créer un utilisateur disposant d'un droit d'accès au schéma `saas`. Cet utilisateur est requis lorsque vous connectez une instance de machine virtuelle workspace-va à la base de données.

    REMARQUE La machine virtuelle workspace-va utilise le nom de base de données `saas`. Pendant le processus d'initialisation, toute base de données existante nommée `saas` est supprimée, puis recréée.

Procédure

1 Connectez-vous en tant qu'utilisateur root.

2 Modifiez le fichier `postgresql.conf`.

Par exemple, la base de données VMware vFabric PostgreSQL se trouve à l'emplacement `/var/vmware/vpostgres/current/pgdata/`.

3 Augmentez le paramètre `max_connections`. Chaque machine virtuelle workspace-va supplémentaire nécessite au moins`300` connexions pour fonctionner correctement avec Workspace.

4 Définissez la valeur du paramètre `max_connections` sur **`600`** pour les deux machines virtuelles workspace-va.

5 Redémarrez la base de données.

6 Ajoutez une nouvelle ligne au fichier `postgresql.conf.auto` qui inclut le paramètre `search_path='saas'`.

7 Exécutez les commandes PostgresSQL pour créer un schéma de base de données PostgresSQL.

Tableau 4-2. Créer un code SQL de schéma de base de données

Exemple de code SQL pour créer un schéma de base de données
CREATE ROLE horizon LOGIN PASSWORD `yourpassword` NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION; ALTER ROLE horizon SET search_path = saas; CREATE DATABASE saas WITH OWNER = postgres ENCODING = 'UTF8' TABLESPACE = pg_default CONNECTION LIMIT = -1; GRANT CONNECT, TEMPORARY ON DATABASE saas TO public; GRANT ALL ON DATABASE saas TO postgres; GRANT ALL ON DATABASE saas TO horizon; \connect saas; CREATE SCHEMA saas AUTHORIZATION horizon; CREATE EXTENSION citext SCHEMA saas;

Transfert de données à partir de la base de données interne

Si votre déploiement utilise une base de données interne et que vous prévoyez de passer à une base de données externe, vous pouvez extraire les données existantes de la base de données pour les ajouter à une nouvelle base de données externe.

Prérequis

Préparez le serveur de la base de données externe. Voir « Configuration d'une base de données PostgreSQL », page 26.

Procédure

1 Connectez-vous en tant qu'utilisateur root.

2 Accédez au répertoire `/opt/vmware/vpostgres/current/bin`.

3 Exécutez la commande `./pg_dump –U postgres –w ––clean –f /tmp/db_dump.data saas`.

4 Copiez le fichier `db_dump.data` dans le serveur de base de données externe que vous venez de préparer.

```
scp /tmp/db_dump.data
```

5 Connectez-vous en tant qu'utilisateur root sur le serveur de base de données externe.

6 Accédez au répertoire `/opt/vmware/vpostgres/current/bin`.

7 Exécutez la commande `db_dump.data`.

```
./psql –U postgres –w –d saas –f /tmp/db_dump.data
```

Il est possible que vous voyiez les commandes `DROP` et `ALTER` pendant l'exécution de la commande `db_dump.data`.

Ajouter une base de données externe au dispositif Workspace

Après l'exécution de l'assistant Configuration d'Workspace, vous pouvez configurer Workspace afin d'utiliser une autre base de données.

Vous devez faire pointer Workspace vers une base de données initialisée et peuplée. Par exemple, vous pouvez utiliser une base de données configurée après une exécution réussie de l'assistant Configuration d'Workspace, une base de donnée provenant d'une sauvegarde ou une base de données existante provenant d'un snapshot restauré.

Prérequis

- Installez et configurez VMware vFabric PostgreSQL ou Oracle en tant que serveur de base de données externe. Pour obtenir des informations sur la configuration d'une base de données PostgreSQL pour Workspace, reportez-vous à « Configuration d'une base de données PostgreSQL », page 26. Pour plus d'informations sur les versions Oracle spécifiques prises en charge par Workspace, consultez les matrices d'interopérabilité des produits VMware à l'adresse http://www.vmware.com/resources/compatibility/sim/interop_matrix.php.
- Transférez les données depuis la base de données interne, si vous en utilisez une.

Procédure

1 Dans Console d'administration Workspace, cliquez sur **Paramètres** et sélectionnez **Configuration VA**.

2 Cliquez sur **Gérer la configuration**.

3 Connectez-vous à Configurateur de dispositifs avec le mot de passe de l'administrateur de Workspace.

4 Sur la page Configuration de la connexion à la base de données, sélectionnez **Base de données externe** comme type de base de données.

5 Entrez les informations de connexion de la base de données.

a Tapez l'URL JDBC du serveur de base de données.

PostgreSQL	`jdbc:postgresql://IP_address/saas?stringtype=unspecified`
Oracle	`jdbc:oracle:thin:@//IP_address:port/sid`

b Tapez le nom de l'utilisateur disposant de privilèges de lecture et d'écriture sur la base de données.

PostgreSQL	`horizon`
Oracle	“`saas`”

c Tapez le mot de passe de l'utilisateur que vous avez créé lors de la configuration de votre base de données Oracle ou PostgreSQL.

6 Cliquez sur **Tester la connexion** pour vérifier puis enregistrer les informations.

Activation du serveur Syslog

Workspace exporte les événements de niveau application vers le serveur syslog externe. Les événements du système d'exploitation ne sont pas exportés.

Comme la plupart des entreprises ne disposent pas d'un espace disque illimité, Workspace n'enregistre pas l'intégralité de l'historique de journalisation de chaque machine virtuelle. Si vous souhaitez enregistrer davantage d'historique ou créer un emplacement centralisé pour votre historique de journalisation, vous pouvez configurer un serveur syslog externe.

Si vous ne configurez pas de serveur syslog pendant la configuration initiale, vous pouvez le configurer ultérieurement à partir de la page Configuration de Syslog de Configurateur de dispositifs.

Prérequis

Configurez un serveur syslog externe. Vous pouvez utiliser n'importe quel serveur syslog standard disponible. Plusieurs serveurs syslog incluent des fonctions de recherche avancées.

Procédure

1 Dans Console d'administration Workspace, cliquez sur **Paramètres** et sélectionnez **Configuration VA**.

2 Cliquez sur **Gérer la configuration**.

3 Connectez-vous à Configurateur de dispositifs.

4 Cliquez sur **Configurer Syslog** dans le volet de navigation de gauche.

5 Cliquez sur **Activer**.

6 Entrez l'adresse IP ou le nom de domaine complet du serveur à l'emplacement sur lequel vous souhaitez stocker les journaux.

7 Cliquez sur **Enregistrer.**

Workspace envoie une copie de vos journaux au serveur syslog.

Utilisation des certificats SSL dans Workspace

Lorsque le dispositif Workspace est installé, un certificat de serveur SSL par défaut est généré automatiquement. Vous pouvez utiliser ce certificat auto-signé pour tester Workspace. VMware recommande vivement que vous génériez et installiez des certificats SSL commerciaux lorsque Workspace est utilisé dans un environnement de production.

Une autorité de certification est une entité approuvée qui garantit l'identité du certificat et de son créateur. Lorsqu'un certificat est signé par une autorité de certification de confiance, les utilisateurs ne reçoivent plus les messages leur demandant de vérifier le certificat.

Si vous déployez Workspace avec le certificat SSL auto-signé, le certificat de l'autorité de certification racine de Workspace doit être disponible en tant qu'autorité de certification de confiance pour les clients qui accèdent à Workspace. Les clients peuvent inclure les machines des utilisateurs finaux, les équilibreurs de charge, les proxys, etc. Vous pod'identification à Kerberosd'identification à Kerberosuvez télécharger l'autorité de certification racine de Workspace à l'adresse *https://workspacehostname.com/horizon_workspace_rootca.pem*.

Vous pouvez installer le certificat de l'autorité de Workspace à la page Programme de configuration du dispositif > Installer le certificat. Vous pouvez également ajouter le certificat de l'autorité de certification racine de l'équilibrage de charge sur cette page. Voir « Appliquer le certificat racine de Workspace à l'équilibrage de charge », page 45.

Appliquer l'autorité de certification publique à Workspace

Certaines entreprises utilisent des certificats générés par leur propre société ou par d'autres autorités de certification. Ces certificats ne sont pas inclus dans la liste des autorités de certification de confiance.

Vous pouvez ajouter de nouveaux certificats à Workspace.

Remarque Si FQDN de Workspace pointe vers un équilibrage de charge, le certificat SSL est appliqué à celui-ci.

Prérequis

Générez une demande de signature de certificat (CSR) pour obtenir un certificat valide et signé d'une autorité de certification. Si votre entreprise fournit des certificats SSL signés par une autorité de certification, vous pouvez les utiliser.

Procédure

1 Pour appliquer le certificat à Workspace, sur la console d'administration de Workspace, cliquez sur **Paramètres** et sélectionnez **Configuration VA**.

2 Cliquez sur **Gérer la configuration**.

3 Connectez-vous au Programme de configuration du dispositif avec le mot de passe administrateur de Workspace.

4 Sélectionnez **Installer le certificat**.

5 Dans l'onglet Mettre fin à SSL sur le dispositif Workspace, collez la chaîne de certificat et la clé privée complètes. Vérifiez que le certificat inclut le nom d'hôte FQDN de Workspace.

6 Enregistrez le certificat SSL.

Suivant

Vérifiez que les utilisateurs peuvent se connecter.

Informations sur le fichier journal

Les fichiers journaux de Workspace peuvent vous aider à effectuer un débogage ou un dépannage. Les fichiers journaux répertoriés ci-dessous constituent un point de départ courant. Vous trouverez des journaux supplémentaires dans le répertoire `/opt/vmware/horizon/workspace/logs`.

Tableau 4-3. Informations sur le fichier journal

Composant	Emplacement du fichier journal	Description
Journaux de service Workspace	`/opt/vmware/horizon/workspace/logs/horizon.log`	Informations sur l'activité de l'application Workspace, comme les droits d'accès, les utilisateurs et les groupes.
Journaux du Programme de configuration	`/opt/vmware/horizon/workspace/logs/configurator.log`	Requêtes que Configurator reçoit du client REST et de l'interface Web.
Connector Journaux	`/opt/vmware/horizon/workspace/logs/connector.log`	Enregistrement de chaque demande reçue de l'interface Web. Chaque entrée de journal inclut également l'URL, l'horodatage et les exceptions de la requête. Aucune action de synchronisation n'est enregistrée.
Mettre à jour les journaux	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Enregistrement des messages sortants associés aux demandes de mise à jour pendant la mise à niveau de Workspace . Les fichiers du répertoire `/opt/vmware/var/log/vami` sont utiles pour le dépannage. Vous trouverez ces fichiers sur toutes les machines virtuelles après une mise à niveau.
Journaux Apache Tomcat	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat enregistre les messages qui ne sont pas enregistrés dans d'autres fichiers journaux.

Collecter les informations de journalisation

Pendant un essai ou une résolution de problème, les journaux vous fournissent des commentaires sur l'activité et les performances des dispositifs virtuels, ainsi que des informations sur tous les problèmes qui se produisent.

Vous collectez les journaux auprès de chaque dispositif workspace-va se trouvant dans votre environnement.

Procédure

1 Connectez-vous à Configurateur de dispositifs

2 Ouvrez la page Emplacements des fichiers journaux et cliquez sur **Préparer le bundle de journaux**.

Les informations sont collectées dans un fichier tar.gz que vous pouvez télécharger.

3 Téléchargez le bundle préparé.

Suivant

Pour collecter tous les journaux, procédez ainsi avec chaque dispositif workspace-va.

Mettre à jour les paramètres de Workspace depuis les pages de Administrateur de Connector Services

5

Après avoir configuré Workspace, vous pouvez accéder aux pages de Administrateur de Connector Services pour gérer l'annuaire de Workspace, activer ou désactiver les adaptateurs d'authentification, modifier les attributs utilisateur d'Active Directory, gérer les groupes Active Directory, synchroniser manuellement l'annuaire et configurer les ressources utilisées dans Workspace, notamment les pools View, les ressources Citrix et les modules ThinApp.

Tableau 5-1. Paramètres gérés depuis les pages de Administrateur de Connector Services

Nom de la page	Paramètre
À propos de	La page À propos de affiche des informations générales sur Workspace, notamment le numéro de version.
Configuration	La page Configuration n'est pas applicable pour le moment pour le dispositif Workspace.
Joindre le domaine	Activez Joindre le domaine et fournissez les informations sur cette page pour utiliser les ressources View ou ThinApp dans Workspace et pour fournir une authentification SSO à l'interface Web à l'aide de l'authentification Windows Kerberos. Vous devez joindre le même Active Directory que celui utilisé par la ressource. Les informations sur Active Directory que vous fournissez sur cette page sont destinées à l'utilisateur autorisé à joindre des machines au domaine Active Directory. Consultez les chapitres connexes dans *Configuration des ressources dans le Guide de VMware Workspace Portal* pour en savoir plus sur la configuration de ces ressources.
Méthode d'authentification de répertoire	Activez l'authentification Windows pour configurer un environnement à domaines multiples, à forêt unique ou à forêts multiples approuvées avec Workspace. Voir « Configurer l'authentification Windows pour des domaines multiples ou des domaines à forêts multiples approuvés dans Active Directory », page 38.
Fournisseur d'identité	La page Fournisseur d'identité affiche l'instance du fournisseur d'identité que vous utilisez pour authentifier les utilisateurs auprès d'Active Directory au sein du réseau d'entreprise.
Adaptateurs d'authentification	La page Adaptateurs d'authentification affiche les méthodes d'authentification disponibles dans Workspace, notamment l'authentification par mot de passe, Kerberos et SecureID. Vous pouvez activer et configurer les informations d'authentification. Voir Chapitre 8, « Configuration de l'authentification utilisateur », page 49.
Répertoire	Affichez et gérez les informations de connexion d'Active Directory à partir de cette page. Voir « Établissement d'une connexion à Active Directory », page 36.
Association des attributs utilisateur	Le mappage des attributs Active Directory à ceux du répertoire Workspace est affiché sur cette page. Si vous configurez les ressources de View, l'attribut userPrincipalName doit être coché sur cette page.
Synchronisation de l'annuaire	Modifiez la planification de synchronisation. Lorsque Workspace a été installé, la planification par défaut était définie pour synchroniser les répertoires une fois par jour à 23 h 55. Vous pouvez également modifier les règles de synchronisation de l'annuaire pour sélectionner les utilisateurs et les groupes à partir d'Active Directory.

Tableau 5-1. Paramètres gérés depuis les pages de Administrateur de Connector Services (suite)

Nom de la page	Paramètre
Protection de la synchronisation	Définissez des protections de la synchronisation pour empêcher les modifications imprévues des utilisateurs et des groupes qui sont ajoutés à Workspace suite à une synchronisation d'annuaire. Par exemple, vous pouvez fixer une limite pour le pourcentage maximal d'utilisateurs pouvant être supprimés simultanément. Si l'une des conditions de déclenchement est remplie, la synchronisation d'annuaire n'a pas lieu, auquel cas vous devez intervenir manuellement. Les conditions par défaut sont activées, mais vous pouvez les modifier pour changer le niveau de protection. Vous pouvez afficher les alertes de protection sur l'onglet Dépannage.
Ressources Horizon DaaS	Activez et configurez Horizon DaaS en tant que ressource. Vous devez activer l'attribut distinguishedName sur la page Mapper les attributs utilisateur.
Pools View	Activez et configurez des pools View en tant que ressource dans Workspace. Vous devez d'abord configurer la connexion au domaine sur la page Joindre le domaine et activer l'attribut userPrincipalName sur la page Mapper les attributs utilisateur. Consultez les chapitres connexes dans *Configuration des ressources dans le Guide de VMware Workspace Portal* pour en savoir plus sur la configuration de cette ressource.
Applications publiées - Citrix	Activez et configurez les applications Citrix en tant que ressource dans Workspace. Consultez les chapitres connexes dans *Configuration des ressources dans le Guide de VMware Workspace Portal* pour en savoir plus sur la configuration de cette ressource.
Applications empaquetées - ThinApp	Activez et configurez des modules ThinApp en tant que ressource dans Workspace. Vous devez d'abord configurer le domaine dans la page de connexion Joindre le domaine. Consultez les chapitres connexes dans *Configuration des ressources dans le Guide de VMware Workspace Portal* pour en savoir plus sur la configuration de cette ressource.

Procédure

1 Accédez à https://*Workspace_FQDN*.com:8443.

2 Connectez-vous à Administrateur de Connector Services avec le mot de passe administrateur de Workspace.

3 Utilisez le volet de navigation gauche pour sélectionner la page à consulter.

Suivant

Vérifiez que les nouveaux paramètres ou les mises à jour sont disponibles.

Gestion de la connexion à Active Directory avec Workspace 6

L'environnement Active Directory peut être composé d'un seul domaine Active Directory, de plusieurs domaines dans une forêt Active Directory unique ou de plusieurs domaines dans plusieurs forêts Active Directory. Après avoir personnalisé Active Directory, vous mettez à jour vos informations de configuration dans Workspace.

Intégration de Workspace avec Active Directory

Vous pouvez intégrer Workspace avec un environnement Active Directory composé d'un seul domaine Active Directory, de plusieurs domaines dans une forêt Active Directory unique, ou de plusieurs domaines dans plusieurs forêts Active Directory.

Lorsque vous installez Workspace, connectez Workspace à un domaine Active Directory unique. Si vous disposez de plusieurs domaines, vous pouvez intégrer Workspace dans votre environnement Active Directory existant à partir des pages Administrateur de Connector Services après l'installation de Workspace.

Environnement à un seul domaine Active Directory

Un déploiement Active Directory vous permet de synchroniser les utilisateurs et les groupes d'un seul domaine Active Directory. Pour installer Workspace dans un environnement Active Directory à domaine unique, reportez-vous à « Établissement d'une connexion à Active Directory », page 36.

Environnement Active Directory à domaines multiples, forêt unique

Un déploiement à domaines multiples, forêt unique vous permet de synchroniser des utilisateurs et des groupes à partir de multiples domaines Active Directory au sein d'une forêt unique.

Vos activez l'authentification Windows comme une méthode d'authentification d'annuaire pour configurer un environnement Active Directory à domaines multiples, forêt unique pour Workspace.

Pour installer Workspace dans un environnement Active Directory à domaines multiples, forêt unique, reportez-vous à « Configurer l'authentification Windows pour des domaines multiples ou des domaines à forêts multiples approuvés dans Active Directory », page 38.

Environnement Active Directory à forêts multiples avec relations d'approbation

Un déploiement Active Directory à forêts multiples avec relations d'approbation vous permet de synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts où des relations d'approbation bidirectionnelles existent entre les domaines.

Vos activez l'authentification Windows comme une méthode d'authentification d'annuaire pour configurer un environnement Active Directory à forêts multiples pour Workspace.

Pour installer Workspace dans un environnement Active Directory à forêts multiples approuvées, reportez-vous à « Configurer l'authentification Windows pour des domaines multiples ou des domaines à forêts multiples approuvés dans Active Directory », page 38.

Environnement Active Directory à forêts multiples sans relations d'approbation

Un déploiement Active Directory à forêts multiples sans relations d'approbation vous permet de synchroniser des utilisateurs et des groupes provenant de plusieurs domaines Active Directory dans des forêts sans relation d'approbation entre les domaines. Ce déploiement nécessite l'utilisation de la technologie de magasin d'utilisateurs de Workspace.

Contactez les services professionnels VMware pour en savoir plus sur le déploiement d'Active Directory à forêts multiples sans relations d'approbation.

Établissement d'une connexion à Active Directory

Workspace utilise votre infrastructure Active Directory existante pour l'authentification et la gestion des utilisateurs. Vous configurez les informations Active Directory lors de l'installation et de la configuration de Workspace.

Informations Active Directory requises

Workspace utilise les informations Active Directory suivantes pour vérifier les informations d'identification des utilisateurs finaux lorsqu'ils se connectent. Vous configurez ces informations lorsque vous installez Workspace.

Hôte du serveur	Adresse de l'hôte Active Directory.
Utiliser SSL	Si vous utilisez SSL pour votre connexion d'annuaire, configurez ce paramètre et ajoutez le certificat au champ de certificat.
Utiliser l'emplacement du service DNS	Si vous ne connaissez pas le nom d'hôte et le numéro de port du serveur, cochez Utiliser l'emplacement du service DNS. Workspace utilise les enregistrements d'emplacement du service DNS pour localiser le domaine Active Directory.
Port du serveur	Numéro de port de l'hôte Active Directory. Le port par défaut pour LDAP est 389. Le port par défaut pour LDAP sur SSL est 636.
Attribut de recherche	Attribut du compte Active Directory contenant le nom d'utilisateur. La plupart des déploiements du service de domaine Active Directory utilisent **`sAMAccountName`**.
Nom unique de base (ND)	DN de base qui est le point de départ des recherches sur le serveur d'annuaires. Par exemple : DC=mycompany, DC=com. Connector part de ce DN pour créer des listes principales à partir desquelles vous pourrez ultérieurement filtrer des utilisateurs et des groupes.

ND Bind	Bind DN du compte d'utilisateur Active Directory qui dispose de privilèges de recherche d'utilisateurs. L'enregistrement de l'utilisateur du compte ND Bind dans Active Directory doit inclure un nom d'utilisateur, un prénom, un nom, une adresse e-mail, tout attribut étendu requis et un attribut ND défini dans Active Directory. Cet utilisateur devient l'administrateur de votre déploiement de Workspace. Vous pouvez promouvoir d'autres utilisateurs Active Directory au rôle d'administrateur dans la Console d'administration Workspace. **Remarque** Lorsqu'une instance d'Active Directory à forêts multiples est configurée et que le groupe local du domaine contient des membres de domaines situés dans différentes forêts, l'utilisateur Bind DN utilisé sur la page Workspace Directory doit être ajouté au groupe d'administrateurs du domaine dans lequel réside le groupe local du domaine. Sinon, ces membres ne seront pas présents dans le groupe local du domaine. Les exemples suivants illustrent les meilleures pratiques à suivre lors de la sélection du nom unique de base et du nom unique Bind : ■ DN de base : dc=example, dc=com. Utilisez le plus haut niveau hiérarchique du nom de base afin d'inclure tous les utilisateurs et groupes. ■ Bind DN : cn=admin user, ou=users, dc=example, dc=com. Assurez-vous que le nom unique Bind est inclus dans le nom unique de base de votre choix.
Mot de passe Bind	Mot de passe Active Directory du compte Bind DN.

Sélection des utilisateurs et des groupes Active Directory à synchroniser avec Workspace

Lorsque vous configurez la connexion Active Directory dans Workspace, vous configurez un DN de base comme le point d'origine de la recherche d'utilisateurs. Cette recherche inclut tous les utilisateurs. Pour restreindre le nombre d'utilisateurs qui se synchronisent avec Workspace, vous pouvez créer des filtres de recherche basés sur des attributs utilisateur pour exclure des types spécifiques d'utilisateurs.

Le DN de base que vous configurez est utilisé pour rechercher des utilisateurs. Pour inclure des groupes dans votre recherche, vous pouvez créer des filtres pour ajouter des types spécifiques de groupes à l'annuaire de Workspace.

Avant de créer des filtres et d'ajouter des groupes dans Workspace, avec l'aide de votre administrateur Active Directory analysez la structure de votre annuaire Active Directory pour sélectionner les utilisateurs et les groupes appropriés à synchroniser.

Utilisation de filtres pour ajouter des utilisateurs et des groupes

Vous sélectionnez les utilisateurs et les groupes que vous souhaitez synchroniser avec Workspace. La première synchronisation se produit lors de la configuration initiale de Workspace. Vous pouvez à tout moment apporter des modifications dans les pages Administrateur de Connector Services.

Procédure

1 Connectez-vous à la Administrateur de Connector Services.

2 Sélectionnez la page Synchronisation d'annuaires et cliquez sur **Modifier les règles de synchronisation de l'annuaire**.

3 Dans la page Sélectionner des utilisateurs, la zone de texte DN de base pour les utilisateurs affiche le DN de base existant. Pour ajouter un DN de base, cliquez sur **Ajouter un autre**.

4 Dans le menu déroulant **Appliquer des filtres pour exclure des utilisateurs**, pour exclure certains types d'utilisateurs, sélectionnez l'attribut d'utilisateur avec lequel vous souhaitez filtrer, sélectionnez la règle de requête, et ajoutez la valeur.

5 Cliquez sur **Ajouter un autre** pour ajouter des filtres supplémentaires.

6 Cliquez sur **Suivant** pour ajouter des groupes.

7 Pour trouver des groupes spécifiques dans la liste Groupes sélectionnés, dans la zone de texte **Filtre de nom de groupe**, entrez le nom du groupe que vous souhaitez ajouter.

8 Cliquez sur **Ajouter** en regard des noms de groupes que vous souhaitez inclure.

9 Cliquez sur **Suivant**.

La page Transmettre à Workspace affiche le nombre d'utilisateurs et de groupes que vous avez sélectionnés pour les ajouter à Workspace.

10 Cliquez sur **Enregistrer et continuer**.

Active Directory est synchronisé avec Workspace.

Établissement d'une connexion à des domaines multiples ou des domaines à forêts multiples approuvées dans Active Directory

Lorsque Workspace est installé, un domaine Active Directory unique est configuré et synchronisé avec Workspace. Vous devez activer l'authentification Windows pour configurer un environnement Active Directory à domaines multiples, à forêt unique ou à forêts multiples approuvées avec Workspace.

Remarque Lorsque vous activez l'authentification Windows, la configuration de l'annuaire est modifiée pour activer le champ Emplacement du service DNS. Si vous souhaitez remplacer la recherche SRV intégrée, consultez « Créer un fichier de recherche d'hôtes de domaine pour remplacer la recherche de l'emplacement du service DNS (SRV) », page 41.

Pour configurer Workspace afin de fournir une authentification Windows interactive, vous devez joindre Workspace au domaine Active Directory, activer l'authentification Windows dans Workspace et synchroniser les utilisateurs et les groupes avec Workspace.

Configurer l'authentification Windows pour des domaines multiples ou des domaines à forêts multiples approuvés dans Active Directory

Pour configurer Workspace pour fournir une authentification Windows interactive pour les domaines Active Directory à domaines multiples ou à forêts multiples approuvées, vous devez joindre Workspace au domaine Active Directory, activer l'authentification Windows, et synchroniser des utilisateurs et des groupes avec Workspace.

Procédure

1 Joindre Workspace à un domaine Active Directory à domaines multiples ou à forêts multiples approuvées page 39

Pour configurer un annuaire Active Directory à domaines multiples, à forêt unique ou à forêts multiples approuvées à l'aide de la méthode d'authentification Windows interactive, vous devez joindre le dispositif Workspace au domaine Active Directory.

2 Activer l'accès à l'authentification Windows pour un domaine Active Directory à forêts multiples approuvées page 39

Pour configurer Workspace afin de fournir une authentification d'utilisateur Windows interactive, une fois que vous avez joint Workspace au domaine Active Directory à forêts multiples approuvées, vous devez activer l'authentification Windows dans Workspace.

3 Sélectionner des utilisateurs et des groupes à synchroniser avec Workspace page 40

Avant de synchroniser des utilisateurs et des groupes de domaines Active Directory avec Workspace, limitez le type d'utilisateur à ajouter à Workspace et sélectionnez les groupes devant être ajoutés à partir des différents domaines.

4 Ajouter des noms de domaines multiples à la page de connexion page 41

   Après la configuration de l'authentification Windows pour plusieurs domaines Active Directory, vous activez Adaptateur de mot de passe pour ajouter les domaines à la page de connexion de l'utilisateur. Les utilisateurs peuvent sélectionner leur domaine dans la liste déroulante lors de la connexion à Workspace.

5 Créer un fichier de recherche d'hôtes de domaine pour remplacer la recherche de l'emplacement du service DNS (SRV) page 41

   Lorsque vous activez l'authentification Windows, la configuration de l'annuaire est modifiée pour activer le champ Emplacement du service DNS. Pour remplacer la recherche SRV intégrée, vous pouvez créer un fichier nommé `domain_krb.properties` et ajouter le domaine aux valeurs des hôtes qui ont priorité sur la recherche SRV.

Joindre Workspace à un domaine Active Directory à domaines multiples ou à forêts multiples approuvées

Pour configurer un annuaire Active Directory à domaines multiples, à forêt unique ou à forêts multiples approuvées à l'aide de la méthode d'authentification Windows interactive, vous devez joindre le dispositif Workspace au domaine Active Directory.

Prérequis

- Vérifiez que vous disposez du nom de domaine Active Directory, du nom d'utilisateur et du mot de passe d'un compte de ce domaine Active Directory autorisé à joindre le domaine.

Procédure

1 Connectez-vous à l'administrateur des services Connector.

2 Sélectionnez la page **Joindre le domaine**.

3 Dans la zone de texte **Domaine AD**, entrez le nom de domaine complet d'Active Directory.

4 Dans la zone de texte **Nom d'utilisateur AD**, entrez le nom d'utilisateur d'un compte Active Directory disposant d'autorisations pour joindre les systèmes à ce domaine Active Directory.

5 Dans la zone de texte **Mot de passe AD**, entrez le mot de passe associé au nom d'utilisateur AD. Ce mot de passe n'est pas stocké par Workspace.

6 Cliquez sur **Joindre le domaine**.

La page Joindre le domaine est actualisée et affiche un message confirmant que vous êtes actuellement joint au domaine.

Suivant

Activez l'authentification Windows pour accéder au domaine Active Directory à domaines multiples, à forêt unique ou à forêts multiples approuvées.

Activer l'accès à l'authentification Windows pour un domaine Active Directory à forêts multiples approuvées

Pour configurer Workspace afin de fournir une authentification d'utilisateur Windows interactive, une fois que vous avez joint Workspace au domaine Active Directory à forêts multiples approuvées, vous devez activer l'authentification Windows dans Workspace.

Prérequis

Assurez-vous que vous avez joint Workspace au domaine Active Directory.

Procédure

1 Connectez-vous à la Administrateur de Connector Services.

2 Sélectionnez la page **Méthode d'authentification d'annuaire**.

3 Cliquez sur **Activer l'authentification Windows**.

4 Cliquez sur **Enregistrer**.

La méthode d'authentification Windows est activée. Workspace met à jour la page Annuaire et la page Adapteurs d'authentification, PasswordIdpAdapter pour ajouter une coche au champ Utiliser l'emplacement du service DNS et pour modifier le format du compte Bind DN en sAMAccountName.

Dès qu'Active Directory a synchronisé les domaines avec Workspace, une liste de domaines est ajoutée à la page Méthode d'authentification d'annuaire. Lorsque Authentification d'adaptateur par mot de passe est activé dans la page Adaptateurs d'authentification, PasswordldpAdapter, les noms de domaines sont ajoutés à la page de connexion utilisateur.

Suivant

Si une instance d'Active Directory à forêts multiples est configurée et que le groupe local du domaine contient des membres de domaines situés dans différentes forêts, l'utilisateur Bind DN utilisé sur la page Workspace Directory doit être ajouté au groupe d'administrateurs du domaine dans lequel réside le groupe local du domaine. Sinon, ces membres ne seront pas présents dans le groupe local du domaine.

Sélectionnez des utilisateurs et des groupes à partir des domaines Active Directory et synchronisez Active Directory avec Workspace.

Sélectionner des utilisateurs et des groupes à synchroniser avec Workspace

Avant de synchroniser des utilisateurs et des groupes de domaines Active Directory avec Workspace, limitez le type d'utilisateur à ajouter à Workspace et sélectionnez les groupes devant être ajoutés à partir des différents domaines.

Prérequis

Créez la liste des attributs utilisateur Active Directory à utiliser comme filtres et la liste des groupes à ajouter à Workspace.

Procédure

1 Connectez-vous à la Administrateur de Connector Services.

2 Sélectionnez la page Synchronisation d'annuaires. cliquez sur **Modifier les règles de synchronisation de l'annuaire**.

3 Dans la page Sélectionner des utilisateurs, les zone de texte DN de base pour les utilisateurs affiche la configuration DN de base existante. Pour ajouter un DN de base, cliquez sur **Ajouter un autre**.

4 Dans le menu déroulant **Appliquer des filtres pour exclure des utilisateurs**, pour exclure certains types d'utilisateurs, sélectionnez l'attribut d'utilisateur avec lequel vous souhaitez filtrer, sélectionnez la règle de requête et ajoutez la valeur.

5 Cliquez sur **Ajouter un autre** pour ajouter des filtres supplémentaires.

6 Cliquez sur **Suivant** pour ajouter des groupes.

7 Les groupes qui sont créés dans votre annuaire Active Directory sont répertoriés dans la page Groupes sélectionnés. Pour trouver des groupes spécifiques, dans le champ de texte **Filtre de nom de groupe**, entrez le nom de groupe à ajouter.

8 Cliquez sur **Ajouter** en regard des noms de groupes que vous souhaitez inclure.

9 Cliquez sur **Suivant**.

La page Transmettre à Workspace affiche le nombre d'utilisateurs et de groupes que vous avez sélectionnés pour les ajouter à Workspace.

10 Cliquez sur **Enregistrer et continuer**.

Les utilisateurs et les groupes des domaines Active Directory sont synchronisés avec Workspace. Les noms de domaines sont ajoutés à la page Méthode d'authentification d'annuaire à mesure que les domaines sont synchronisés avec Workspace.

Suivant

Activez la fonctionnalité d'adaptateur de mot de passe afin que les noms de domaines Active Directory soient ajoutés à la page de connexion utilisateur. Les utilisateurs sélectionnent leur domaine lorsqu'ils se connectent.

Ajouter des noms de domaines multiples à la page de connexion

Après la configuration de l'authentification Windows pour plusieurs domaines Active Directory, vous activez Adaptateur de mot de passe pour ajouter les domaines à la page de connexion de l'utilisateur. Les utilisateurs peuvent sélectionner leur domaine dans la liste déroulante lors de la connexion à Workspace.

Prérequis

La méthode d'authentification Windows doit être activée dans Workspace pour établir la connexion à des domaines à domaines multiples ou à forêts multiples approuvées.

Les domaines Active Directory sont synchronisés avec Workspace.

Procédure

1 Connectez-vous à la Administrateur de Connector Services.

2 Ouvrez la page Adaptateurs d'authentification et sur la ligne PasswordldpAdapter, cliquez sur **Modifier**.

3 Sélectionnez **Activer l'adaptateur de mot de passe**.

4 Cliquez sur **Enregistrer**.

Les noms de domaines

Créer un fichier de recherche d'hôtes de domaine pour remplacer la recherche de l'emplacement du service DNS (SRV)

Lorsque vous activez l'authentification Windows, la configuration de l'annuaire est modifiée pour activer le champ Emplacement du service DNS. Pour remplacer la recherche SRV intégrée, vous pouvez créer un fichier nommé `domain_krb.properties` et ajouter le domaine aux valeurs des hôtes qui ont priorité sur la recherche SRV.

Procédure

1 À partir de la ligne de commande workspace-va, connectez-vous en tant qu'utilisateur disposant de privilèges racine.

2 Remplacez les répertoires par `/usr/local/horizon/conf` et créez un fichier nommé `domain_krb.properties`.

3 Modifiez le fichier domain_krb.properties pour ajouter la liste du domaine aux valeurs des hôtes. Ajoutez les informations sous la forme `<AD Domain>=<host:port>, <host2:port2>, <host2:port2>`.

   Par exemple, entrez la liste sous la forme `example.com=examplehost.com:636, examplehost2.example.com:389`

4 Remplacez le propriétaire du fichier domain_krb.properties par horizon et le groupe par www. Entrez**`chown horizon:www /usr/local/horizon/conf/domain_krb.properties`**.

5 Redémarrez Workspace. Entrez **`service horizon-workspace restart`**.

Configuration avancée du dispositif VMware Workspace Portal 7

Après avoir effectué l'installation de base de Workspace, vous pouvez avoir besoin d'effectuer d'autres tâches de configuration, comme l'activation de l'accès externe à Workspace ou le clonage de machines virtuelles.

Le diagramme de l'architecture de Workspace indique ce que vous pouvez mettre en place dans l'environnement Workspace. Voir Chapitre 2, « Préparation de l'installation de VMware Workspace Portal », page 7 pour un déploiement standard.

- Utilisation d'un équilibrage de charge pour activer l'accès externe à Workspace page 43

  Pendant le déploiement, Workspace est configuré à l'intérieur du réseau interne. Si vous voulez fournir l'accès à Workspace aux utilisateurs se connectant depuis des réseaux externes, vous devez installer un équilibreur de charge, tel qu'Apache, nginx, F5, etc., dans la zone DMZ.

- Configuration de la redondance/du basculement pour le dispositif virtuel Workspace page 45

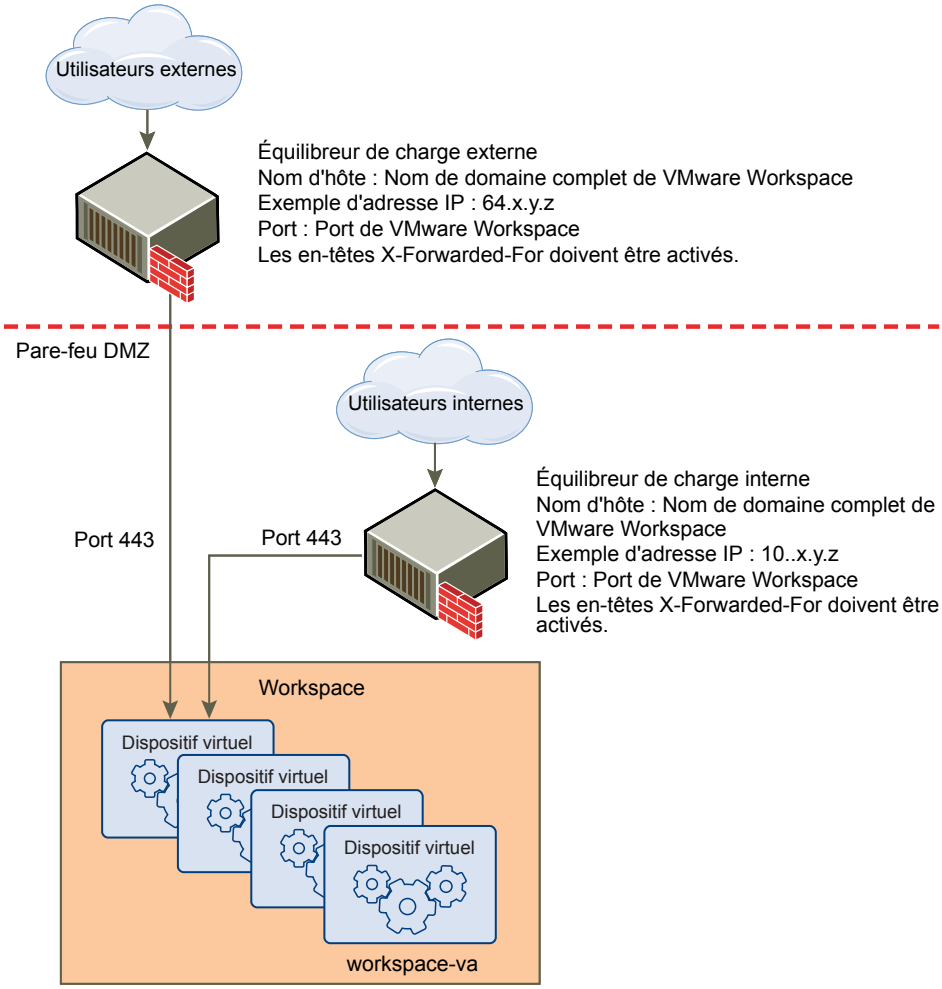
  Workspace permet aux entreprises d'assurer le basculement et la redondance en ajoutant plusieurs dispositifs virtuels workspace-va au cluster Workspace. Si l'un des dispositifs virtuels workspace-va s'arrête sans raison, Workspace est toujours disponible.

Utilisation d'un équilibrage de charge pour activer l'accès externe à Workspace

Pendant le déploiement, Workspace est configuré à l'intérieur du réseau interne. Si vous voulez fournir l'accès à Workspace aux utilisateurs se connectant depuis des réseaux externes, vous devez installer un équilibreur de charge, tel qu'Apache, nginx, F5, etc., dans la zone DMZ.

Si vous n'utilisez pas d'équilibreur de charge, vous ne pourrez pas étendre le nombre de machines virtuelles Workspace dans l'avenir. Vous devrez peut-être ajouter des machines virtuelles Workspace supplémentaires pour implémenter la redondance et l'équilibrage de charge. Le diagramme suivant montre l'architecture de déploiement de base que vous pouvez utiliser pour activer l'accès externe.

Figure 7-1. Proxy d'équilibrage de charge externe avec une machine virtuelle



Spécifiez le nom de domaine complet d' Workspace pendant le déploiement.

Pendant le déploiement de la machine virtuelle Workspace, vous devez entrer le FQDN d'Workspace et le numéro du port d'Workspace. Ces valeurs doivent pointer vers le nom d'hôte auquel vous voulez que les utilisateurs finaux accèdent.

La machine virtuelle Workspace s'exécute toujours sur le port 443. Vous pouvez utiliser un autre numéro de port pour l'équilibreur de charge. Si vous utilisez un numéro de port différent, vous devez le spécifier au moment du déploiement.

Paramètres sur l'équilibrage de charge à configurer pour Workspace

Les paramètres d'équilibrage de charge à configurer pour Workspace incluent l'activation des en-têtes X-Forwarded-For, la définition correcte du délai d'expiration de l'équilibrage de charge et l'activation de Sticky sessions. En outre, la relation d'approbation SSL doit être configurée entre Workspace et l'équilibrage de charge.

- En-têtes X-Forwarded-For. Vous devez activer les en-têtes X-Forwarded-For sur votre équilibrage de charge. Cela détermine la méthode d'authentification. Consultez la documentation du fournisseur de votre équilibreur de charge pour plus d'informations.

- Délai d'expiration de l'équilibrage de charge. Pour un bon fonctionnement de Workspace, vous pouvez avoir besoin d'augmenter la valeur par défaut du délai d'expiration des demandes d'équilibrage de charge. Cette valeur est définie en minutes. Si le paramétrage du délai d'expiration est trop bas, cette erreur peut se produire : « Erreur 502 : Le service est actuellement indisponible. »
- Activation de la fonction Sticky Session sur l'équilibrage de charge de Workspace. Assurez-vous d'activer Sticky Session sur l'équilibrage de charge des serveurs workspace-va si votre déploiement utilise plusieurs serveurs workspace. L'utilisation de Sticky session améliore les performances de l'interface Web. Si Sticky session n'est pas activé, certaines fonctionnalités peuvent échouer.

Appliquer le certificat racine de Workspace à l'équilibrage de charge

Quand Workspace est configuré avec un équilibrage de charge, vous devez établir la relation d'approbation SSL entre l'équilibrage de charge et Workspace. Le certificat racine de Workspace doit être copié dans l'équilibrage de charge. Le certificat peut être téléchargé sur la page Programme de configuration du dispositif, Installer le certificat.

Si le nom de domaine complet d'Workspace pointe vers un équilibreur de charge, le certificat SSL peut uniquement être appliqué à cet équilibreur de charge. Dans la mesure où l'équilibrage de charge communique avec la machine virtuelle Workspace, vous devez copier le certificat CA racine de Workspace dans l'équilibrage de charge en tant que certificat de confiance racine.

Procédure

1 Dans Console d'administration Workspace, cliquez sur **Paramètres** et sélectionnez **Configuration VA**.

2 Cliquez sur **Gérer la configuration**.

3 Connectez-vous à Configurateur de dispositifs avec le mot de passe administrateur de Workspace.

4 Sélectionnez **Installer le certificat**.

5 Sélectionnez l'onglet Mettre fin à SSL sur un équilibrage de charge et dans le champ Certificat de l'autorité de certification racine du dispositif, cliquez sur le lien `https://workspacehostname/horizon_workspace_rootca.pem`.

   Le certificat racine de Workspace s'affiche.

6 Copiez-collez le certificat racine à l'emplacement requis dans chaque équilibrage de charge. Reportez-vous à la documentation fournie par votre fournisseur d'équilibrage de charge.

Suivant

Copiez-collez le certificat racine de l'équilibrage de charge sur la page Workspace Configurateur de dispositifs Installer le certificat, Mettre fin à SSL sur un équilibrage de charge.

Configuration de la redondance/du basculement pour le dispositif virtuel Workspace

Workspace permet aux entreprises d'assurer le basculement et la redondance en ajoutant plusieurs dispositifs virtuels workspace-va au cluster Workspace. Si l'un des dispositifs virtuels workspace-va s'arrête sans raison, Workspace est toujours disponible.

Pour configurer le basculement de Workspace, clonez le dispositif virtuel workspace-va. Le clonage du dispositif virtuel crée un double du dispositif virtuel avec la même configuration que le dispositif d'origine. Vous pouvez personnaliser le dispositif virtuel cloné pour changer le nom du dispositif virtuel, ses paramètres réseau et ses autres propriétés au besoin.

L'adresse IP du dispositif virtuel cloné doit respecter les mêmes recommandations que l'adresse IP du dispositif virtuel d'origine. L'adresse IP doit renvoyer vers un nom d'hôte valide à l'aide de la résolution DNS normale et inverse.

Tous les nœuds du cluster sont identiques et des copies pratiquement sans état les uns des autres. La synchronisation avec Active Directory et les ressources configurées dans Workspace, notamment View ou ThinApp, est désactivée sur le dispositif virtuel cloné.

Créer plusieurs dispositifs virtuels Workspace

Pour le basculement, votre entreprise peut cloner le dispositif virtuel workspace-va pour créer plusieurs dispositifs virtuels du même type afin de distribuer le trafic et d'éliminer tout risque d'indisponibilité.

L'utilisation de plusieurs dispositifs virtuels workspace-va améliore la disponibilité, équilibre la charge des demandes à Workspace et diminue les temps de réponse à l'utilisateur final.

Prérequis

- Le dispositif virtuel doit être configuré derrière un équilibrage de charge. Assurez-vous que le port de l'équilibrage de charge est le port 443. N'utilisez pas 8443, car ce numéro de port est le port administratif de Workspace et est propre à chaque dispositif virtuel.
- Pour ajouter des dispositifs workspace-va supplémentaires, vous devez configurer une base de données externe, comme décrit dans « Connexion à une base de données externe », page 24, ou interne, comme décrit dans l'article KB 2094258 de la base de connaissances VMware, Utilisation d'une base de données vPostgres intégrée pour VMware Workspace Portal VA 2.1.
- VMware vSphere Client ou vSphere Web Client est requis pour cloner le dispositif virtuel et pour accéder au dispositif virtuel cloné afin de configurer la mise en réseau.
- Ajouter une adresse IP aux propriétés d'un dispositif virtuel cloné page 47

  Vous devez attribuer une nouvelle adresse IP avant de mettre sous tension un dispositif virtuel cloné. Cette adresse IP doit être résolvable dans le DNS. Si l'adresse IP ne se trouve pas dans le DNS inversé, vous devez également attribuer le nom d'hôte.
- Activation de l'authentification SecurID page 47

  Dans bien des cas, les entreprises activent l'authentification RSA SecurID pour leurs utilisateurs finaux qui se connectent depuis des réseaux externes. Une fois le dispositif virtuel workspace-va cloné, si vous utilisez l'authentification RSA SecureID, vous devez ajouter le nom d'hôte et l'adresse IP du dispositif Workspace cloné au serveur RSA, puis créer un agent sur le dispositif virtuel cloné.
- Activation de l'authentification Kerberos page 48

  Les entreprises peuvent activer l'authentification Kerberos pour leurs utilisateurs finaux qui se connectent depuis des machines Windows internes. Lorsque vous utilisez l'authentification Kerberos, les utilisateurs finaux peuvent se connecter à Workspace sans taper de nom d'utilisateur et de mot de passe. Une fois que vous avez cloné le dispositif virtuel Workspace, si vous utilisez l'authentification Kerberos, vous devez permettre de nouveau de joindre le domaine et l'authentification Kerberos sur la machine virtuelle clonée.

Procédure

1. Mettez hors tension le dispositif virtuel workspace-va en cours de clonage.
2. Cliquez avec le bouton droit sur le dispositif virtuel qui est cloné, puis cliquez sur **Suivant**.
3. Entrez le nom que vous souhaitez utiliser pour identifier le dispositif virtuel cloné. Il doit être unique dans le dossier de dispositifs virtuels.
4. Sélectionnez l'hôte ou le cluster sur lequel exécuter le dispositif virtuel cloné.
5. Sélectionnez le pool de ressources dans lequel exécuter le dispositif virtuel, puis cliquez sur **Suivant**.
6. Sélectionnez l'emplacement de la banque de données dans laquelle vous souhaitez stocker les fichiers du dispositif virtuel.

7 Sélectionnez le format des disques du dispositif virtuel. Ce format doit être le même que celui de la source. Cliquez sur **Suivant**.

8 Sélectionnez **Ne pas personnaliser** comme option du système d'exploitation invité.

9 Vérifiez les options que vous avez sélectionnées. Si les informations sont correctes, cliquez sur **Terminer**.

Le dispositif virtuel cloné est déployé. Vous ne pouvez pas utiliser ni modifier le dispositif virtuel tant que le clonage n'est pas terminé.

Suivant

Attribuez une adresse IP au dispositif virtuel cloné workspace-va avant de mettre sous tension la machine et d'ajouter le nouveau dispositif virtuel à l'équilibrage de charge.

Ajouter une adresse IP aux propriétés d'un dispositif virtuel cloné

Vous devez attribuer une nouvelle adresse IP avant de mettre sous tension un dispositif virtuel cloné. Cette adresse IP doit être résolvable dans le DNS. Si l'adresse IP ne se trouve pas dans le DNS inversé, vous devez également attribuer le nom d'hôte.

Procédure

1 Depuis vSphere Client ou vSphere Web Client, sélectionnez le dispositif virtuel ayant été cloné.

2 Sélectionnez **Résumé > Commandes**, cliquez sur **Modifier**.

3 Sélectionnez **Options** et dans la liste **Paramètres des options**, sélectionnez **Propriétés**.

4 Modifiez l'adresse IP du champ **Adresse IP**.

5 Si l'adresse IP ne se trouve pas dans le DNS inversé, ajoutez le nom d'hôte dans la zone de texte **Nom d'hôte**.

6 Cliquez sur **OK.**

7 Mettez sous tension la machine clonée.

Suivant

Activez les méthodes d'authentification configurées pour Workspace sur chacun des dispositifs virtuels clonés.

Activation de l'authentification SecurID

Dans bien des cas, les entreprises activent l'authentification RSA SecurID pour leurs utilisateurs finaux qui se connectent depuis des réseaux externes. Une fois le dispositif virtuel workspace-va cloné, si vous utilisez l'authentification RSA SecureID, vous devez ajouter le nom d'hôte et l'adresse IP du dispositif Workspace cloné au serveur RSA, puis créer un agent sur le dispositif virtuel cloné.

Prérequis

Créez un agent d'authentification de serveur RSA à l'aide du nom d'hôte et de l'adresse IP du dispositif Workspace cloné. Voir « Préparation du serveur RSA SecurID pour Administrateur de Connector Services », page 50.

Procédure

1 Connectez-vous à la Administrateur de Connector Services.

2 Cliquez sur **Adaptateurs d'authentification**.

3 Sur la ligne Secure ID, cliquez sur **Modifier**.

4 Reconfigurez la page Adaptateur d'authentification SecureID en ajoutant l'adresse IP du nouveau dispositif Workspace. Voir « Configurer l'authentification RSA SecurID dans Workspace », page 50.

Activation de l'authentification Kerberos

Les entreprises peuvent activer l'authentification Kerberos pour leurs utilisateurs finaux qui se connectent depuis des machines Windows internes. Lorsque vous utilisez l'authentification Kerberos, les utilisateurs finaux peuvent se connecter à Workspace sans taper de nom d'utilisateur et de mot de passe. Une fois que vous avez cloné le dispositif virtuel Workspace, si vous utilisez l'authentification Kerberos, vous devez permettre de nouveau de joindre le domaine et l'authentification Kerberos sur la machine virtuelle clonée.

Procédure

- Connectez-vous à la Administrateur de Connector Services.
  a Sélectionnez la page **Joindre le domaine**.
  b Dans la zone de texte Mot de passe AD, entrez le mot de passe de l'utilisateur dans Active Directory qui a les droits requis pour joindre le domaine.
  c Cliquez sur **Joindre le domaine**.
  d Cliquez sur **Adaptateurs d'authentification**.
  e Sélectionnez KerberosldAdapter et dans la page qui s'ouvre, sélectionnez **Activer l'authentification Windows**.
  f Cliquez sur **Enregistrer.**

Si vous avez intégré View dans un déploiement Workspace à plusieurs connecteurs, assurez-vous d'activer et de configurer Pools View sur chaque connecteur prenant en charge des postes de travail View. Vous ne pouvez pas vous connecter à votre poste de travail à partir d'un connecteur sur lequel Pools View n'est pas activé. Lorsque vous planifiez une opération **Synchroniser Pool View** à partir de l'un des connecteurs, cette opération synchronise les connecteurs avec la configuration de View.

Configuration de l'authentification utilisateur 8

Workspace prend en charge les méthodes d'authentification suivantes : mot de passe Active Directory, Kerberos et RSA SecureID.

Types d'authentification d'Workspace pris en charge par défaut	Description
Mot de passe	Sans configuration, Workspace prend en charge l'authentification par mot de passe Active Directory. Cette méthode authentifie les utilisateurs avec Active Directory.
Kerberos	L'authentification Kerberos fournit aux utilisateurs du domaine un accès à authentification unique à Workspace, ce qui leur permet d'éviter de se connecter à Workspace après s'être connectés au réseau de l'entreprise. L'instance de fournisseur d'identité valide les informations d'identification de poste de travail de l'utilisateur à l'aide de tickets Kerberos remis par le centre de distribution de clés (KDC).
RSA SecurID	L'authentification RSA SecurID nécessite l'utilisation d'un système d'authentification à jeton par les utilisateurs. RSA SecurID est la méthode d'authentification recommandée pour les utilisateurs qui accèdent à Workspace depuis l'extérieur du réseau de l'entreprise.

Pour plus d'informations sur la configuration de l'authentification d'utilisateur de Workspace, reportez-vous au *Guide de l'administrateur de Workspace*.

Ce chapitre aborde les rubriques suivantes :

Configuration de SecurID pour Workspace

Lorsque vous configurez le serveur RSA SecurID, vous devez ajouter les informations sur le dispositif Workspace en tant qu'agent d'authentification sur le serveur RSA SecurID et configurer les informations du serveur RSA SecureID sur Workspace.

Après avoir déployé Workspace, vous pouvez configurer SecurID pour qu'il fournisse une sécurité supplémentaire. Assurez-vous que votre réseau est correctement configuré pour votre déploiement d'Workspace. Pour SecurID en particulier, assurez-vous que le port adéquat est ouvert afin de permettre à SecurID d'authentifier les utilisateurs hors du réseau de l'entreprise.

Après avoir exécuté l'assistant de configuration d'Workspace, vous disposez des informations nécessaires pour préparer le serveur RSA SecurID. Après avoir préparé le serveur RSA SecurID pour le dispositif Workspace, accédez à la page Adaptateurs d'authentification Workspace Administrateur de Connector Services pour activer SecurID.

Préparation du serveur RSA SecurID pour Administrateur de Connector Services

Le serveur RSA SecurID doit être configuré avec des informations sur le dispositif Workspace en tant qu'agent d'authentification. Les informations requises correspondent au nom d'hôte et aux adresses IP des interfaces réseau.

Prérequis

Workspace

- Vérifiez que l'une des versions suivantes de RSA Authentication Manager est installée et fonctionne sur le réseau d'entreprise pour permettre de communiquer avec Administrateur de Connector Services : RSA AM 6.1.2, 7.1 SP2 et versions ultérieures ainsi que 8.0 et versions ultérieures. Workspace utilise AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), qui prend en charge uniquement les versions précédentes de RSA Authentication Manager (serveur RSA SecurID). Pour obtenir des informations sur l'installation et la configuration de RSA Authentication Manager (serveur RSA SecurID), consultez la documentation de RSA.

Procédure

1 Sur une version prise en charge du serveur RSA SecurID, ajoutez le dispositif Workspace en tant qu'agent d'authentification. Entrez les informations suivantes.

Option	Description
Adresse Internet	Nom d'hôte du dispositif Workspace.
adresse IP	Adresse IP du dispositif Workspace.
Adresse IP alternative	Si le trafic sortant du dispositif Workspace passe par un périphérique NAT (network address translation) pour atteindre le serveur RSA SecurID, entrez l'adresse IP privée du dispositif Workspace.

2 Téléchargez le fichier de configuration compressé et extrayez le fichier `sdconf.rec`.

Préparez-vous à charger ce fichier ultérieurement lorsque vous configurez RSA SecurID dans Workspace.

Suivant

Accédez à l'onglet Avancé de Administrateur de Connector Services et, sur la page Adaptateurs d'authentification, configurez SecurID.

Configurer l'authentification RSA SecurID dans Workspace

Une fois le dispositif Workspace configuré en tant qu'agent d'authentification sur le serveur RSA SecurID, vous devez ajouter les informations de configuration RSA SecureID à Workspace.

Prérequis

- Vérifiez que RSA Authentication Manager (serveur RSA SecurID) est installé et correctement configuré.

- Téléchargez le fichier compressé depuis le serveur RSA SecurID et extrayez le fichier de configuration du serveur.

Procédure

1 Accédez à la page Adaptateurs d'authentification de Administrateur de Connector Services et sur la ligne SecurIDldpAdapter, cliquez sur **Modifier**.

2 Cochez la case **Activer SecurID**.

3 Configurez la page Adaptateur d'authentification SecurID.

Les informations utilisées et les fichiers générés sur le serveur RSA SecurID sont nécessaires lors de la configuration de la page SecurID.

Option	Action
Nom	Un nom est requis. Le nom par défaut est SecurIDldpAdapter. Vous pouvez modifier cela à tout moment.
Activer SecurID	Cochez cette case pour activer l'authentification securID.
Nombre de tentatives d'authentification autorisées	Nombre maximal d'échecs de tentatives de connexion à l'aide du jeton RSA SecurID. La valeur par défaut est de cinq tentatives.
Adresse du connecteur	Entrez le nom d'hôte local ou l'adresse IP de Workspace. La valeur que vous entrez doit correspondre à la valeur que vous avez utilisée lorsque vous avez ajouté le dispositif Workspace en tant qu'agent d'authentification du serveur RSA SecurID. Si votre serveur RSA SecurID a une valeur attribuée à l'invite de l'adresse IP alternative, entrez cette valeur en tant qu'adresse IP de Workspace. Si aucune adresse IP alternative n'est attribuée, entrez la valeur attribuée à l'invite de l'adresse IP.
Adresse IP de l'agent	Entrez la valeur assignée à l'invite **Adresse IP** sur le serveur RSA SecurID.
Configuration du serveur	Chargez le fichier de configuration du serveur RSA SecureID. Vous devez d'abord télécharger le fichier compressé auprès du serveur RSA SecurID, puis extraire le fichier de configuration du serveur qui est appelé par défaut `sdconf.rec`.
Nœud secret	Laisser vide le champ nœud secret permet à celui-ci de se générer lui-même. Nous vous recommandons d'effacer le fichier du secret du nœud du serveur RSA SecurID et de ne pas charger volontairement le fichier du secret du nœud. Assurez-vous que le fichier du secret du nœud sur le serveur RSA SecurID et sur le dispositif Workspace correspondent toujours l'un à l'autre. Si vous modifiez le nœud secret à un emplacement, modifiez-le respectivement à l'autre emplacement. Par exemple, si vous effacez ou générez le secret du nœud sur le serveur RSA SecurID, effacez ou chargez également le fichier du secret du nœud sur le dispositif Workspace.

4 Enregistrez vos paramètres SecurID.

Configuration de Kerberos pour Workspace

L'authentification Kerberos fournit aux utilisateurs d'un domaine un accès Single Sign-On à Workspace. Vous activez l'authentification Windows pour permettre au protocole Kerberos de sécuriser les interactions entre les navigateurs des utilisateurs et Workspace. Il n'est pas nécessaire de configurer directement Active Directory pour faire fonctionner Kerberos avec votre déploiement d'Workspace.

Vous accédez aux pages Administrateur de Connector Services pour activer l'authentification Kerberos. Vous devez joindre le domaine dans la page Joindre le domaine de Administrateur de Connector Services et activer Kerberos dans la page Adaptateurs d'authentification.

Prise en charge de l'authentification Kerberos par le système d'exploitation

Actuellement, les interactions entre le navigateur d'un utilisateur et Workspace sont authentifiées par Kerberos sur les systèmes d'exploitation Windows uniquement. L'accès à Workspace depuis d'autres systèmes d'exploitation ne profite pas de l'authentification Kerberos.

Configuration de votre navigateur

Les navigateurs Web suivants peuvent être configurés pour envoyer vos informations d'identification Kerberos à Workspace sur les ordinateurs fonctionnant sous Windows : Firefox, Internet Explorer et Chrome. Tous les navigateurs nécessitent une configuration supplémentaire.

Lorsque Kerberos est activé, vous devez configurer les navigateurs Web pour qu'ils envoient vos informations d'identification Kerberos à Workspace quand les utilisateurs se connectent.

- Configurer Kerberos sur Workspace page 52

  Pour configurer Workspace pour qu'il fournisse l'authentification Kerberos, vous devez joindre le domaine et autoriser l'authentification Kerberos sur Workspace.

- Configuration d'Internet Explorer pour accéder à l'interface Web page 53

  Vous devez configurer le navigateur Internet Explorer si Kerberos est configuré pour votre déploiement d'Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web à l'aide d'Internet Explorer.

- Configuration de Firefox pour accéder à l'interface Web page 54

  Vous devez configurer le navigateur Firefox si Kerberos est configuré pour votre déploiement Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Firefox.

- Configuration du navigateur Chrome pour accéder à l'interface Web page 55

  Vous devez configurer le navigateur Chrome si Kerberos est configuré pour votre déploiement Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Chrome.

Configurer Kerberos sur Workspace

Pour configurer Workspace pour qu'il fournisse l'authentification Kerberos, vous devez joindre le domaine et autoriser l'authentification Kerberos sur Workspace.

Procédure

1 Accédez à Administrateur de Connector Services et sélectionnez **Joindre le domaine**.

2 Sur la page Joindre le domaine, entrez les informations pour le domaine Active Directory.

   a Dans la zone de texte **Domaine AD**, entrez le nom de domaine complet d'Active Directory. Le nom de domaine que vous entrez doit être le même domaine Windows que celui dans lequel se trouve le dispositif Workspace.

   b Dans la zone de texte **Nom d'utilisateur AD**, entrez le nom d'utilisateur d'un compte Active Directory disposant d'autorisations pour joindre les systèmes à ce domaine Active Directory.

   c Dans la zone de texte **Mot de passe AD**, entrez le mot de passe associé au nom d'utilisateur AD. Ce mot de passe n'est pas stocké par Workspace.

   d Cliquez sur **Joindre le domaine**.

   La page Joindre le domaine est actualisée et affiche un message confirmant que vous êtes actuellement joint au domaine.

3 Dans la page Administrateur de Connector Services, sélectionnez **Adaptateurs d'authentification** et cliquez sur **Modifier** sur la ligne KerberosldpAdapter.

   a Le champ Nom affiche KerberosldpAdapter en tant que nom. Vous pouvez modifier ce paramètre.

   b Dans la zone de texte **Attribut UID de l'annuaire**, entrez l'attribut du compte contenant le nom d'utilisateur.

   c Cochez **Activer l'authentification Windows** pour étendre les interactions d'authentification entre les navigateurs des utilisateurs et Workspace.

   d Cochez **Activer le NTLM** pour activer l'authentification basée sur le protocole NTLM (NT LAN Manager).

   e Cochez **Activer la redirection** si le DNS tourniquet et les équilibrages de charge ne disposent pas de la prise en charge de Kerberos. Les demandes d'authentification sont redirigées vers Rediriger le nom d'hôte. Si cette option est cochée, entrez le nom d'hôte de redirection dans la zone de texte **Rediriger le nom d'hôte**.

   f Cliquez sur **Enregistrer**.

Configuration d'Internet Explorer pour accéder à l'interface Web

Vous devez configurer le navigateur Internet Explorer si Kerberos est configuré pour votre déploiement d'Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web à l'aide d'Internet Explorer.

L'authentification Kerberos fonctionnement conjointement avec Workspace sur les systèmes d'exploitation Windows.

Remarque N'effectuez pas ces étapes relatives à Kerberos sur d'autres systèmes d'exploitation.

Prérequis

Configurez le navigateur Internet Explorer pour chaque utilisateur ou fournissez les instructions aux utilisateurs après avoir configuré Kerberos.

Procédure

1 Vérifiez que vous êtes connecté à Windows en tant qu'utilisateur du domaine.

2 Dans Internet Explorer, activez la connexion automatique.

   a Sélectionnez **Outils > Options Internet > Sécurité**.

   b Cliquez sur **Personnaliser le niveau**.

   c Sélectionnez **Connexion automatique uniquement dans la zone intranet**.

   d Cliquez sur **OK.**

3 Vérifiez que cette instance du dispositif Workspace fait partie de la zone intranet locale.

   a Utilisez Internet Explorer pour accéder à l'URL de connexion de Workspace à l'adresse *https://workspaceHostname.DomainName/authenticate/*.

   b Localisez la zone dans le coin inférieur droit de la barre d'état de la fenêtre du navigateur.

   Si la zone est Intranet local, la configuration d'Internet Explorer est terminée.

4 Si la zone n'est pas un intranet local, ajoutez Workspace à la zone intranet.

   a Sélectionnez **Outils > Options Internet > Sécurité > Intranet local > Sites.**

   b Sélectionnez **Détecter automatiquement le réseau Intranet**.

   Si cette option n'a pas été sélectionnée, il peut suffire de la sélectionner pour ajouter Workspace à la zone intranet.

   c (Facultatif) Si vous avez sélectionné **Détecter automatiquement le réseau Intranet**, cliquez sur **OK** jusqu'à ce que toutes les boîtes de dialogue soient fermées.

   d Dans la boîte de dialogue Intranet local, cliquez sur **Avancé**.

   Une deuxième boîte de dialogue nommée Intranet local s'affiche.

   e Tapez l'URL de Workspace dans la zone de texte **Ajouter ce site Web à la zone**.

   https://workspaceHostname.DomainName/authenticate/

   f Cliquez sur **Ajouter > Fermer > OK**.

5 Vérifiez qu'Internet Explorer est autorisé à passer l'authentification Windows pour accéder au site de confiance.

   a Dans la boîte de dialogue Options Internet, cliquez sur l'onglet **Avancé**.

   b Sélectionnez **Activer l'authentification Windows intégrée**.

   Cette option prend effet seulement après le redémarrage d'Internet Explorer.

   c Cliquez sur **OK**.

6 Connectez-vous à l'interface Web de Workspace à l'adresse *https://workspaceHostname.DomainName/authenticate/* pour vérifier l'accès.

   Si l'authentification Kerberos est réussie, l'URL de test vous redirige vers l'interface Web.

Le protocole Kerberos sécurise toutes les interactions entre cette instance Internet Explorer et Workspace. Maintenant, les utilisateurs peuvent accéder à Workspace à l'aide d'une connexion unique.

Configuration de Firefox pour accéder à l'interface Web

Vous devez configurer le navigateur Firefox si Kerberos est configuré pour votre déploiement Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Firefox.

L'authentification Kerberos fonctionnement conjointement avec Workspace sur les systèmes d'exploitation Windows.

Remarque N'effectuez pas ces étapes relatives à Kerberos sur d'autres systèmes d'exploitation.

Prérequis

Configurez le navigateur Firefox pour chaque utilisateur, ou communiquez des instructions aux utilisateurs après la configuration de Kerberos.

Procédure

1 Dans l'URL du navigateur Firefox, tapez `about:config` pour accéder aux paramètres avancés.

2 Cliquez sur **Je ferai attention, promis !**.

3 Double-cliquez sur **network.negotiate-auth.trusted-uris** dans la colonne Nom de l'option.

4 Tapez l'URL de Workspace dans la zone de texte.

   https://workspaceHostname

5 Cliquez sur **OK.**

6 Double-cliquez sur **network.negotiate-auth.delegation-uris** dans la colonne Nom de l'option.

7 Tapez l'URL de Workspace dans la zone de texte.

https://workspaceHostname

8 Cliquez sur **OK.**

9 Testez la fonctionnalité de Kerberos à l'aide du navigateur Firefox pour vous connecter à Workspace à l'adresse *https://workspaceHostname*.

Si l'authentification Kerberos réussit, l'URL de test vous redirige vers l'interface Web.

Le protocole Kerberos sécurise toutes les interactions entre cette instance Firefox et Workspace. Maintenant, les utilisateurs peuvent accéder à Workspace à l'aide d'une connexion unique.

Configuration du navigateur Chrome pour accéder à l'interface Web

Vous devez configurer le navigateur Chrome si Kerberos est configuré pour votre déploiement Workspace et si vous voulez accorder aux utilisateurs l'accès à l'interface Web via Chrome.

L'authentification Kerberos fonctionnement conjointement avec Workspace sur les systèmes d'exploitation Windows.

Remarque N'effectuez pas ces étapes relatives à Kerberos sur d'autres systèmes d'exploitation.

Prérequis

- Configurez Kerberos.
- Dans la mesure où Chrome utilise la configuration d'Internet Explorer pour activer l'authentification Kerberos, vous devez configurer Internet Explorer afin de permettre à Chrome d'utiliser la configuration d'Internet Explorer. Pour en savoir plus sur la procédure de configuration de Chrome pour l'authentification Kerberos, reportez-vous à la documentation de Google.

Procédure

1 Testez les fonctionnalités de Kerberos à l'aide du navigateur Chrome.

2 Connectez-vous à Workspace à l'adresse *https://Workspace FQDN*.

Si l'authentification Kerberos réussit, l'URL de test vous redirige vers l'interface Web.

Si toutes les configuration relatives à Kerberos sont correctes, le protocole correspondant (Kerberos) sécurise toutes les interactions entre cette instance Chrome et Workspace. Les utilisateurs peuvent accéder à Workspace à l'aide de Single Sign-On.

Personnalisation du magasin d'utilisateurs de démonstration

9

Le service OpenLDAP embarqué est généralement utilisé pour des configurations de démonstration ou d'essai. Lorsque vous utilisez le service OpenLDAP embarqué, il se peut que vous souhaitiez effectuer certaines opérations LDAP de base, telles que l'ajout d'utilisateurs, la suppression d'utilisateurs existants ou la modification de mots de passe d'utilisateur.

Ces informations sont destinées aux administrateurs système expérimentés qui sont familiers avec les opérations et commandes LDAP standard.

Le serveur OpenLDAP embarqué s'exécute sur le port TCP 389. Le serveur OpenLDAP est accessible localement uniquement à partir de la console Linux sur le dispositif virtuel workspace-va. Vous pouvez utiliser les commandes LDAP standard pour effectuer des opérations sur le serveur OpenLDAP embarqué. Les fichiers binaires requis (`ldapadd`, `ldapsearch`, `ldapdelete` et `ldapmodify`) sont installés sur le dispositif virtuel.

Vous devez utiliser certains paramètres lorsque vous configurez OpenLDAP dans les pages Configurateur de dispositifs et Administrateur de Connector Services.

Tableau 9-1. Informations de configuration d'OpenLDAP

Attribut	Valeur
Adresse Internet	*ConnectorFullyQualifiedDomainName* ou *localhost*
Attribut de recherche	`sAMAccountName`
Port du serveur	389
ND de base	ou=users, dc=test, dc=example, dc=com
ND Bind	cn=test user1, ou=users, dc=test, dc=example, dc=com
Mot de passe Bind	mot de passe

Le magasin d'utilisateurs de démonstration inclut dix exemples d'utilisateurs et un groupe à des fins de démonstration.

Des exemples de données spécifiques sont inclus dans le magasin d'utilisateurs de démonstration. Lors du déploiement, ces données sont chargées dans l'exemple de bases de données.

Pour ajouter des utilisateurs ou des groupes, créez des fichiers et nommez-les `ldapusers.ldif` et `ldapgroups.ldif`. Utilisez les fichiers originaux, `users.ldif` et `groups.ldif`, comme modèles. Voir « Ajout d'un utilisateur au magasin d'utilisateurs de démonstration », page 58 et « Ajout de groupes et attribution d'utilisateurs à des groupes dans le magasin d'utilisateurs de démonstration », page 60.

Tableau 9-2. Exemple d'informations inclus dans le magasin d'utilisateurs de démonstration

Nom de l'exemple	Valeur
Fichiers de l'exemple	`users.ldif` `groups.ldif`
Chemin du répertoire	`/etc/openldap`
Exemples de noms d'utilisateurs	testuser1 – testuser10
Mot de passe pour tous les utilisateurs	mot de passe
Exemple de groupe L'exemple de groupe, testgroup1, contient dix exemples d'utilisateurs.	testgroup1

- Ajout d'un utilisateur au magasin d'utilisateurs de démonstration page 58

  Lorsque vous configurez votre magasin d'utilisateurs de démonstration, vous déterminez le nombre d'utilisateurs que vous voulez ajouter en fonction de votre environnement de production. Vous devez ajouter suffisamment d'utilisateurs pour permettre à vos essais de fournir des résultats pertinents pour votre environnement de production.

- Ajout de groupes et attribution d'utilisateurs à des groupes dans le magasin d'utilisateurs de démonstration page 60

  Lorsque vous configurez votre magasin d'utilisateurs de démonstration, déterminez le nombre de groupes et d'utilisateurs à ajouter, en fonction de la taille de votre environnement de production. Ajoutez suffisamment de groupes et d'utilisateurs pour créer un environnement qui ressemble étroitement à votre environnement de production.

Ajout d'un utilisateur au magasin d'utilisateurs de démonstration

Lorsque vous configurez votre magasin d'utilisateurs de démonstration, vous déterminez le nombre d'utilisateurs que vous voulez ajouter en fonction de votre environnement de production. Vous devez ajouter suffisamment d'utilisateurs pour permettre à vos essais de fournir des résultats pertinents pour votre environnement de production.

Vous pouvez ajouter un utilisateur au magasin d'utilisateurs de démonstration en modifiant le fichier `ldapusers.ldif` et en exécutant la commande `ldapadd` sur la machine virtuelle workspace-va.

Prérequis

Vous devez utiliser `sAMAccountName` comme attribut de recherche dans le magasin d'utilisateurs de démonstration. Workspace ne prend pas en charge `userPrincipalName` lorsque vous utilisez le magasin d'utilisateurs de démonstration.

Procédure

1 Remplacez la balise *value* dans le fichier `ldapusers.ldif` avec vos informations. Voir l'exemple de tableau `ldapusers.ldif`.

2 Copiez le fichier `ldif` sur la machine virtuelle workspace-va.

3 Exécutez la commande `ldapadd` pour ajouter un nouvel utilisateur au magasin d'utilisateurs de démonstration.

`/usr/bin/ldapadd –h 127.0.0.1 –D` *cn=Manager,dc=test,dc=example,dc=com* `–w H0rizon! –x –f` *ldif file path*

Vous pouvez ajouter plusieurs utilisateurs en utilisant différentes valeurs dans un fichier `ldif` unique.

4 Redémarrez le service LDAP.

```
/sbin/service ldap restart
```

Tableau 9-3. Fichier d'exemple `ldapusers.ldif`

Exemple `ldapusers.ldif`
Utilisez une valeur *value* unique pour chaque paramètre. dn: cn=*value*,ou=users,dc=test,dc=example,dc=com objectClass: user objectCategory: person cn: *value* sn: *value* sAMAccountName: *value* canonicalName: *value* mail: *value* givenName: *value* distinguishedName: cn=*value*,ou=users,dc=test,dc=example,dc=com objectGUID: *value* (par exemple, cd0ff02b-f9d6-4fac-a5bc-6380d1867999.) userPassword: *value* (par exemple, {SSHA}WbipwJh13Jdy2tItppdkFMzzNVSfkqsZ.)

Suivant

Générez un mot de passe chiffré qui sera employé par les utilisateurs de votre magasin d'utilisateurs de démonstration. Voir « Génération d'un mot de passe chiffré par SSHA », page 59.

Génération d'un mot de passe chiffré par SSHA

L'alogrithme SSHA (salted secure hash algorithm) est une version améliorée de l'algorithme SHA qui mélange le hachage et diminue la probabilité qu'il soit déchiffré.

Vous devez générer un mot de passe chiffré par SSHA. Vous pouvez utiliser le même mot de passe pour tous les comptes utilisateurs de démonstration. Si vous avez besoin d'un mot de passe différent pour chaque utilisateur, chiffrez chaque mot de passe un par un.

Prérequis

« Ajout d'un utilisateur au magasin d'utilisateurs de démonstration », page 58.

Procédure

1 Ouvrez le dispositif virtuel workspace-va.

2 Exécutez la commande `slappasswd`.

3 Tapez un nouveau mot de passe et vérifiez-le.

La valeur chiffrée par SSHA est affichée.

4 Ajoutez cette valeur au fichier `ldif` pour définir le mot de passe utilisateur.

Suivant

Ajoutez des groupes et assignez les utilisateurs au magasin d'utilisateurs de démonstration.

Ajout de groupes et attribution d'utilisateurs à des groupes dans le magasin d'utilisateurs de démonstration

Lorsque vous configurez votre magasin d'utilisateurs de démonstration, déterminez le nombre de groupes et d'utilisateurs à ajouter, en fonction de la taille de votre environnement de production. Ajoutez suffisamment de groupes et d'utilisateurs pour créer un environnement qui ressemble étroitement à votre environnement de production.

Vous ajoutez un groupe au magasin de l'utilisateur de démonstration en modifiant le fichier `ldapgroups.ldif` et en exécutant la commande `ldapadd` sur la machine virtuelle workspace-va.

Procédure

1 Remplacez les balises *value* et *user DN* dans le fichier `ldapgroups.ldif`.

User DN doit être le nom distinctif d'un utilisateur existant dans LDAP. Le remplacement de la balise *value* crée un groupe, et le remplacement de la balise *User DN* assigne un utilisateur au nouveau groupe que vous créez.

2 Copiez le fichier `ldif` sur la machine virtuelle workspace-va.

3 Exécutez la commande `ldapadd` pour ajouter un groupe au magasin d'utilisateurs de démonstration.

```
/usr/bin/ldapadd –h 127.0.0.1 –D cn=Manager,dc=test,dc=example,dc=com –w H0rizon! –x –fldif file path
```

Vous pouvez ajouter plusieurs groupes en utilisant différentes valeurs dans un fichier `ldif` unique.

4 Redémarrez le service LDAP.

```
/sbin/service ldap restart
```

Tableau 9-4. Exemple de fichier `ldapgroups.ldif`

Exemple de paramètres
Utilisez une valeur *value* unique pour chaque paramètre. dn: cn=*value*,ou=users,dc=test,dc=example,dc=com objectClass: group objectCategory: group sAMAccountName: *value* canonicalName: *value* mail: *value* distinguishedName: cn=*value*,ou=users,dc=test,dc=example,dc=com objectGUID: *value* (par exemple, cd0ff02b-f9d6-4fac-a5bc-6380d1867899) member: *User DN1* (par exemple, cn=user1,ou=users,dc=test,dc=example,dc=com) member: *User DN2* member: *User DN3* member: *User DN4*

Suivant

Utilisez le magasin d'utilisateurs de démonstration à des fins de test jusqu'à ce que vous soyez prêt à mettre Workspace en production.

Index