Guide de l'administrateur 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-001537-00

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 du guide de l'administrateur d' VMware Workspace Portal

1

Le *VMware Workspace PortalGuide de l'administrateur* de fournit des informations et des instructions concernant l'utilisation et la maintenance de VMware Workspace™ Portal. Avec Workspace, vous pouvez personnaliser un catalogue de ressources pour les applications de votre organisation et fournir un accès utilisateur géré, sécurisé et multipériphériques à ces ressources. Ces ressources comprennent des applications Web, des applications Windows capturées sous forme de modules ThinApp, des applications Citrix et des pools de postes de travail et d'applications View™. Workspace fournit aux utilisateurs une expérience homogène et offre à votre département informatique des systèmes de sécurité et de gestion unifiés pour l'ensemble des services et des applications sur de multiples périphériques.

Public concerné

Le *Guide de l'administrateur d'VMware Workspace Portal* est destiné aux administrateurs d'entreprise. Ces informations sont écrites à l'intention des administrateurs Windows ou Linux expérimentés et familiers avec la technologie des machines virtuelles, de la gestion d'identité, de Kerberos et des services de dossiers. La connaissance d'autres technologies, telles que VMware ThinApp®, View, la virtualisation d'applications Citrix et RSA SecurID est utile si vous prévoyez de mettre en œuvre ces fonctionnalités.

Aperçu du Guide de l'administrateur d' Workspace

Utilisez le Guide de l'administrateur de *VMware Workspace Portal* après l'installation de Workspace.

Pour administrer Workspace, vous utilisez Console d'administration Workspace.

La principale tâche que vous effectuez à partir de Console d'administration Workspace consiste à octroyer des ressources aux utilisateurs. D'autres tâches soutiennent cette tâche principale en vous fournissant un contrôle plus précis sur les utilisateurs ou groupes qui sont attribués à certaines ressources sous certaines conditions.

Les tâches que vous effectuerez en tant qu'administrateur varient en fonction des types de ressources que vous prévoyez de gérer. Vous pouvez gérer les pools de postes de travail et d'applications View, les applications Windows (modules ThinApp), les postes de travail DaaS, les applications Citrix et les applications Web. Les types de ressources réels que vous gérerez varient en fonction des besoins de votre organisation. Pour octroyer un type de ressource, vous effectuez d'abord les tâches de préconfiguration respectives décrites dans Configuration des ressources du Guide de VMware Workspace Portal.

Présentation d' Workspace pour les administrateurs 2

Workspace offre une console de gestion centralisée permettant de personnaliser le catalogue de votre organisation et de gérer les droits d'accès aux ressources de ce catalogue. Votre catalogue contient les applications et les ressources de votre entreprise.

Workspace détecte les attributs des utilisateurs et applique des stratégies aux applications. L'espace de travail d'un utilisateur consiste en l'ensemble des ressources qui lui sont attribuées. Pour chaque utilisateur, vous pouvez personnaliser la mise à disposition des applications Windows, Web et SaaS (Software-as-a-Service) en permettant leur accès à partir d'un portail unique, tout en offrant aux utilisateurs un accès en libre-service aux applications.

Services administratifs de Workspace

Vous gérez les groupes d'utilisateurs Workspace et l'administration des ressources, l'authentification, la configuration de la synchronisation et la connexion à la base de données à partir de différents services administratifs de 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 pouvez afficher le tableau de bord Engagement de l'utilisateur et le tableau de bord Diagnostics du système pour surveiller les utilisateurs, l'utilisation des ressources et la santé du dispositif Workspace. 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.
- Dans les pages Administrateur de Connector Services, vous configurez l'annuaire, définissez les brokers d'authentification et administrez d'autres intégrations d'entreprise, par exemple 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. Un lien vers les pages Administrateur de Connector Services est accessible à l'adresse https://*Workspace_FQDN* .com:8443.
- Dans les pages Configurateur de dispositifs, vous pouvez gérer la base de données de Workspace, mettre à jour des certificats, activer Syslog, modifier les mots de passe de Workspace et du 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 Appliance Configurator à partir de la console d'administration Workspace, page Paramètres > Configuration VA.

Workspace Composants de l'utilisateur final

Les utilisateurs peuvent accéder aux ressources qui leur sont octroyées en utilisant le portail des applications Workspace (client sans agent) et ils peuvent accéder aux applications Windows virtualisées capturées sous forme de modules ThinApp à partir de Workspace pour Windows.

Tableau 2-1. Composants client utilisateur d' Workspace

Composant utilisateur de Workspace	Description	Points de terminaison disponibles
Portail des applications Workspace	Le portail d'applications Workspace est une application Web sans agent. Il s'agit de l'interface par défaut utilisée lorsque les utilisateurs accèdent avec un navigateur aux ressources d'espace de travail qui leur ont été octroyées. Ce portail permet aux utilisateurs d'accéder à leurs postes de travail View et à leurs applications Web Workspace. Si un utilisateur dispose d'applications ThinApp autorisées et emploie un système Windows sur lequel le programme Workspace pour Windows est installé et actif, il peut voir et lancer à l'aide de ce portail d'applications les modules ThinApp qui lui ont été octroyés. Sur les périphériques iOS, les utilisateurs peuvent ouvrir ce portail dans une application de navigateur telle que Safari, puis utiliser leurs postes de travail View, leurs applications Web Workspace et les applications Citrix.	Le portail des applications Web est disponible sur tous les points de terminaison système pris en charge, tels que les systèmes Windows, les systèmes Mac, les périphériques iOS et les périphériques Android.
Workspace pour Windows	Lorsque ce programme est installé sur les systèmes Windows des utilisateurs, ces derniers peuvent travailler avec leurs applications Windows virtualisées capturées sous forme de modules ThinApp.	Systèmes Windows

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

Les utilisateurs finaux peuvent accéder à leur portail d'applications Workspace à partir des navigateurs suivants.

- Mozilla Firefox (dernière version)
- Google Chrome (dernière version)
- Safari (dernière version)
- Internet Explorer 8 ou version ultérieure
- Navigateur natif et Google Chrome sur les périphériques Android
- Safari sur les périphériques iOS

La visualisation des pages Workspace avec Internet Explorer 8 risque de ne pas afficher correctement tous les éléments sur la page. Pour optimiser la visualisation, les utilisateurs doivent procéder à une mise à niveau vers une version plus récente.

Utilisation des tableaux de bord de la console d'administration de Workspace pour surveiller les utilisateurs, les ressources et la santé du dispositif

3

La console d'administration de Workspace inclut un tableau de bord Engagement de l'utilisateur et un tableau de bord Diagnostics du système qui vous aident à surveiller les utilisateurs, l'utilisation des ressources et la santé du dispositif Workspace.

Ce chapitre aborde les rubriques suivantes :

Suivi des utilisateurs et des ressources utilisés dans Workspace

Le tableau de bord Engagement de l'utilisateur affiche des informations relatives aux utilisateurs et aux ressources. Vous pouvez voir les personnes connectées, les ressources utilisées et la fréquence d'accès aux applications. Vous pouvez créer des rapports pour assurer le suivi des utilisateurs, des activités de groupe et de l'utilisation des ressources.

L'heure affichée sur le tableau de bord Engagement de l'utilisateur est fondée sur le fuseau horaire défini pour le navigateur. Le tableau de bord est mis à jour toutes les minutes.

Procédure

- L'en-tête affiche le nombre d'utilisateurs uniques connectés ce jour-là ainsi qu'un calendrier indiquant le nombre d'événements de connexion quotidiens sur une période de sept jours. Le nombre affiché dans le tableau de bord Utilisateurs connectés aujourd'hui est entouré d'un cercle qui indique le pourcentage d'utilisateurs connectés. Le graphique mobile Connexions affiche les événements de connexion survenus pendant la semaine. Pointez sur l'un des points du graphique pour afficher le nombre de connexions ce jour-là.
- La section Utilisateurs et groupes affiche le nombre de comptes utilisateurs et de groupes configurés dans Workspace. Les utilisateurs s'étant connecté récemment sont affichés. Vous pouvez cliquer sur **Voir les rapports complets** pour créer un rapport sur les événements d'audit qui affiche les utilisateurs qui se sont connectés durant une plage de jours.
- La section Popularité des applications affiche un graphique à barres du nombre de lancements des applications, groupées par type, sur une période de sept jours. Pointez sur un jour spécifique pour afficher une infobulle indiquant le type des applications utilisées et le nombre d'applications lancées ce jour-là. La liste en dessous du graphique indique le nombre de lancements des applications spécifiques. Cliquez sur la flèche du menu déroulant de droite pour sélectionner l'affichage de ces informations sur un jour, une semaine, un mois ou 12 semaines. Vous pouvez cliquez sur **Voir les rapports complets** pour créer un rapport d'utilisation des ressources indiquant l'application, le type de ressource et l'activité du nombre d'utilisateurs sur une plage de temps.

- La section Adoption des applications affiche un graphique à barres indiquant le pourcentage de personnes ayant ouvert les applications auxquelles elles ont ont droit. Pointez sur l'application pour afficher une infobulle indiquant le nombre réel d'adoptions et de droits.
- Le graphique à secteurs Applications lancées affiche les ressources lancées sous forme de pourcentage du total. Pointez sur une section spécifique du graphique à secteurs pour voir le nombre réel par type de ressource. Cliquez sur la flèche du menu déroulant de droite pour sélectionner l'affichage de ces informations sur un jour, une semaine, un mois ou 12 semaines.
- La section Clients Workspace affiche le nombre de clients Windows pour Workspace en cours d'utilisation.

Suivant

Cliquez sur le menu déroulant Tableau de bord pour voir le tableau de bord Diagnostics du système.

Surveiller les informations système et la santé de Workspace

Le tableau de bord Diagnostics du système Workspace affiche une présentation détaillée des dispositifs Workspace dans votre environnement et des informations sur les services Workspace. Vous pouvez visualiser la santé globale sur le serveur de base de données Workspace, les machines virtuelles workspace-va et les services disponibles sur chacune d'entre elles.

Dans le tableau de bord Diagnostics du système, vous pouvez sélectionner la machine virtuelle workspace-va à surveiller et voir l'état des services sur cette dernière, y compris la version de Workspace qui est installée. En cas de problème lié à la base de données ou à une machine virtuelle, la barre d'en-tête affiche l'état de la machine en rouge. Pour voir les problèmes, vous pouvez sélectionner la machine virtuelle affichée en rouge.

Procédure

- Expiration du mot de passe utilisateur Les dates d'expiration du mot de passe racine du dispositif Workspace et du mot de passe de connexion à distance sont affichées. Si un mot de passe expire, accédez à la page Paramètres et sélectionnez **Configurations VA**. Ouvrez la page **Sécurité du système** pour modifier le mot de passe.
- Certificats. L'émetteur du certificat, la date de début et la date de fin sont affichés. Pour gérer le certificat, accédez à la page Paramètres et sélectionnez **Configurations VA**. Ouvrez la page **Installer le certificat**.
- Configurator - État de déploiement de l'application. Les informations relatives aux services Appliance Configurator sont affichées. L'état du serveur Web indique si le serveur Tomcat est en cours d'exécution. L'état de l'application Web indique si la page Appliance Configurator est accessible. La version du dispositif indique la version du dispositif Workspace installé.
- Application Manager - État de déploiement de l'application. L'état de connexion du dispositif Workspace est affiché.
- Connector - État de déploiement de l'application. L'état de la connexion Administrateur de Connector Services est affiché. Lorsque Connexion réussie s'affiche, vous pouvez accéder aux pages Administrateur de Connector Services.
- Nom de domaine complet Workspace Affiche le nom de domaine complet que les utilisateurs entrent pour accéder à leur portail d'applications Workspace. Le nom de domaine complet Workspace pointe vers l'équilibreur de charge lorsqu'un équilibreur de charge est utilisé.
- Application Manager - Composants intégrés. Les informations relatives à la connexion de base de données Workspace, aux services d'audit et à la connexion d'analyse sont affichées.
- Connector - Composants intégrés. Les informations relatives aux services gérés à partir des pages d'administration des services Connector sont affichées. Les informations relatives aux ressources d'applications ThinApp, View et Citrix publiées sont affichées.

- Modules. Affiche les ressources activées dans Workspace. Cliquez sur **Activé** pour accéder à la page d'administration des ressources des services Connector pour la ressource concernée.

Configuration de l'authentification des utilisateurs d' Workspace 4

L'authentification de l'utilisateur de Workspace nécessite l'utilisation d'une ou de plusieurs instances de fournisseur d'identité. Il peut s'agir de l'instance de Workspace, par défaut, d'instances de fournisseur d'identités tiers, ou d'une combinaison des deux. Les instances de fournisseur d'identité authentifient les utilisateurs avec Active Directory au sein du réseau de l'entreprise.

Pour configurer et ajouter des instances de fournisseur d'identité à votre déploiement Workspace, vous devez effectuer plusieurs vérifications préalables pour vous assurer qu'Workspace peut accéder correctement à votre déploiement Active Directory.

Ce chapitre aborde les rubriques suivantes :

Présentation de l'authentification des utilisateurs d' Workspace

Workspace tente d'authentifier les utilisateurs en fonction des méthodes d'authentification, de l'ensemble des stratégies d'accès par défaut, des plages réseau et des instances de fournisseur d'identité que vous configurez.

Les instances de fournisseur d'identité que vous utilisez avec Workspace créent une autorité fédératrice intégrée au réseau qui communique avec Workspace à l'aide d'assertions SAML 2.0. Les instances de fournisseur d'identité authentifient l'utilisateur avec Active Directory au sein du réseau de l'entreprise.

Workspace prend en charge les méthodes d'authentification d'utilisateur par mot de passe Active Directory, Kerberos et RSA SecurID. Cependant, votre fournisseur d'identité tiers peut prendre charge des méthodes d'authentification supplémentaires, telles que l'authentification par carte à puce, que vous pouvez utiliser avec votre déploiement d'Workspace.

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 mettre en œuvre l'authentification Kerberos ou l'authentification RSA SecurID, vous pouvez utiliser une instance de fournisseur d'identité existante ou déployer une ou plusieurs instances de fournisseurs d'identité supplémentaires, selon votre déploiement.

Lorsqu'un utilisateur tente de se connecter, Workspace doit déterminer l'instance de fournisseur d'identité servant à authentifier l'utilisateur.

Pour faire ce choix, Workspace évalue l'ensemble de stratégies d'accès par défaut pour sélectionner la stratégie à appliquer. La stratégie appliquée détermine le score d'authentification minimal requis pour cet événement de connexion. Workspace filtre et trie ensuite les méthodes d'authentification disponibles en fonction du score d'authentification minimal requis et de l'ordre des méthodes, que vous pouvez définir de manière à répondre aux exigences de votre organisation. Workspace sélectionne la première instance de fournisseur d'identité qui répond aux exigences de méthode d'authentification et de plages réseau de la stratégie, puis transfère la demande d'authentification utilisateur à cette instance pour authentification. Si l'authentification échoue, le processus de sélection de fournisseur d'identité essaie l'entrée suivante dans la liste.

Important Lorsque vous supprimez ou réinitialisez une instance de fournisseur d'identité, vous devez supprimer le nom du fournisseur d'identité correspondant de la liste Fournisseurs d'identité.

Vous pouvez déployer Workspace pour utiliser le processus de sélection de fournisseur d'identité de plusieurs façons, dont l'une est présentée brièvement dans l'exemple suivant.

Exemple d'authentification RSA SecurID externe et par mot de passe interne ou supérieure

Cela constitue une façon de configurer Workspace de manière à utiliser le mot de passe Active Directory ou la méthode d'authentification Kerberos pour les utilisateurs internes et la méthode d'authentification RSA SecurID pour les utilisateurs externes dans le même déploiement Workspace.

- Stratégie interne - Utilisez Workspace console d'administration pour créer une stratégie dans l'ensemble de stratégies d'accès par défaut avec un score d'authentification minimal qui accepte le mot de passe Active Directory comme méthode d'authentification. Pour s'assurer que Workspace tente d'abord d'authentifier les utilisateurs avec l'authentification Kerberos, attribuez à l'authentification de la méthode Kerberos un score plus élevé que celui de la méthode par mot de passe et placez Kerberos en haut de la liste sur la page Méthodes d'authentification. Vous pouvez également attribuer une plage réseau aux utilisateurs internes.

- Stratégie externe - Utilisez Workspace console d'administration pour créer une stratégie dans l'ensemble de stratégies d'accès par défaut avec un score d'identification minimal qui garantit que la méthode d'authentification RSA SecurID est utilisée pour authentifier les utilisateurs. Vous attribuez également une plage réseau qui inclut tous les utilisateurs possibles, à savoir entre 0.0.0.0 et 255.255.255.255.

Avec cette configuration, les utilisateurs qui tentent d'accéder à Workspace à l'intérieur du réseau d'entreprise sont redirigés vers une instance de fournisseur d'identité qui fournit l'authentification Kerberos ou l'authentification par mot de passe, tandis que les utilisateurs à l'extérieur du réseau d'entreprise sont redirigés vers une instance de fournisseur d'identité qui fournit l'authentification RSA SecurID. Les utilisateurs internes et externes peuvent être redirigés vers la même instance de fournisseur d'identité ou vers des instances différentes selon la configuration des méthodes d'authentification.

Ajout ou modification d'une plage réseau

Vous pouvez ajouter une plage réseau d'adresses IP que vous souhaitez diriger vers une instance de fournisseur d'identité spécifique.

La plage réseau par défaut, appelée TOUTES LES PLAGES, comprend chaque adresse IP disponible sur Internet, de 0.0.0.0 à 255.255.255.255. Même si votre déploiement d'Workspace a une seule instance de fournisseur d'identité, vous devrez peut-être configurer la plage par défaut et ajouter d'autres plages afin d'exclure ou d'inclure des adresses IP spécifiques. Vous devez définir plusieurs plages réseau si votre déploiement dispose de plusieurs instances de fournisseurs d'identité appliquant différentes méthodes d'authentification. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.

Remarque La plage réseau par défaut (TOUTES LES PLAGES) et sa description (« un réseau pour toutes les plages ») sont modifiables. Vous pouvez modifier le nom et la description, notamment traduire le texte dans une autre langue, à l'aide de la fonctionnalité **Modifier** de la page Plages réseau.

Prérequis

Effectuez la planification de plages réseau nécessaire.

- Déterminez le meilleur moyen d'intégrer Workspace à Active Directory pour répondre aux besoins de votre organisation. Cette planification a une incidence sur le nombre d'instances de fournisseurs d'identité de votre déploiement, ce qui détermine le nombre de plages réseau requises.
- En fonction de votre topologie réseau, définissez les plages réseau de votre déploiement d'Workspace.
- Pour ajouter une plage réseau lorsque le module View est activé, notez l'URL d'accès à Horizon Client et le numéro de port de la plage réseau. Pour plus d'informations, consultez la documentation de View.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Paramètres > Plages réseau**.

3 Modifiez une plage réseau existante ou ajoutez une plage.

Option	Description
Modifier une plage réseau existante	Cliquez sur **Modifier** pour la plage à modifier.
Ajouter une plage	Cliquez sur **+ Plage réseau** pour ajouter une plage.

4 Renseignez le formulaire.

Élément de formulaire	Description
Nom	Entrez un nom pour la plage réseau.
Description	Entrez une description pour la plage réseau.
Espaces View	L'option Espaces View s'affiche uniquement lorsque le module View est activé. Hôte de l'URL d'accès au client. Entrez l'URL d'accès à Horizon Client correspondant à la plage réseau. Port d'accès à Client. Entrez le numéro de port d'accès à Horizon Client correspondant à la plage réseau. Reportez-vous au chapitre *Configuration des ressources dans le Guide de VMware Workspace Portal* , Fourniture d'un accès aux pools de postes de travail et d'applications View.
Plages d'adresses IP	Modifiez ou ajoutez des plages d'adresses IP jusqu'à ce que toutes les adresses IP souhaitées soient incluses et toutes les adresses IP non souhaitées soient exclues.

Suivant

- Associez chaque plage réseau à une instance de fournisseur d'identité. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.
- Associez les plages réseau aux ensembles de stratégies d'accès appropriés. Voir Chapitre 5, « Gestion des ensembles de stratégies d'accès », page 25.

Ajouter ou modifier une méthode d'authentification d'utilisateur

Vous pouvez modifier des méthodes d'authentification d'utilisateur existantes. Lorsque vous ajoutez un fournisseur d'identité tiers, vous pouvez configurer les méthodes d'authentification d'utilisateur qu'Workspace ne prend pas en charge par défaut. Vous pouvez également créer des stratégies pour associer des méthodes d'authentification à des applications Web spécifiques.

Workspace prend en charge les méthodes d'authentification d'utilisateur par mot de passe Active Directory, Kerberos et RSA SecurID. En ajoutant un fournisseur d'identité tiers qui prend en charge une autre méthode d'authentification, telle que l'authentification par carte à puce, vous pouvez permettre à Workspace d'appliquer cette méthode. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20. Reportez-vous à « Aperçu de la configuration d'Workspace de manière à utiliser une instance de fournisseur d'identité tiers », page 22 pour consulter la liste complète des tâches liées à la configuration d'Workspace permettant d'utiliser un fournisseur d'identité tiers.

Le score d'authentification minimal d'une méthode et l'ordre de la méthode sur la page Méthodes d'authentification sont significatifs dans le processus qu'exécute Workspace pour sélectionner une instance de fournisseur d'identité lors de l'authentification d'un utilisateur. Pour imposer aux utilisateurs l'emploi d'une méthode d'authentification bénéficiant d'un score d'authentification minimal spécifié, reportez-vous à « Gestion des ensembles de stratégies d'accès spécifiques à une application Web », page 27.

Le nombre de tentatives qu'Workspace effectue à l'aide d'une méthode d'authentification donnée est variable. Workspace n'effectue qu'une seule tentative d'authentification Kerberos. Si Kerberos ne parvient pas à connecter l'utilisateur, la méthode d'authentification suivante sur la liste est tentée. Le nombre maximal d'échecs de tentative de connexion pour l'authentification par mot de passe Active Directory ou RSA SecurID est de cinq. Après cinq échecs de connexion, Workspace tente de connecter l'utilisateur avec la méthode d'authentification suivante sur la liste. Lorsque toutes les méthodes d'authentification ont été utilisées sans succès, Workspace émet un message d'erreur.

Prérequis

- Déployez les systèmes d'authentification que vous prévoyez intégrer à Workspace. Par exemple, si vous prévoyez d'intégrer RSA SecurID à votre déploiement d'Workspace, vérifiez que RSA SecurID est installé et configuré sur votre réseau.
- Utilisez vos propres critères pour déterminer les niveaux de sécurité, sur une échelle allant de 1, la sécurité la plus faible, à 5, la sécurité la plus élevée, des méthodes d'authentification que vous prévoyez d'utiliser dans votre déploiement d'Workspace.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Paramètres > Méthodes d'authentification**.

3 Modifiez une méthode d'authentification existante ou ajoutez-en une.

Option	Description
Modifier une méthode d'authentification existante	Cliquez sur **Modifier** pour la méthode d'authentification existante à configurer.
Ajouter une nouvelle méthode d'authentification	Cliquez sur **+ Ajouter une méthode d'authentification** pour ajouter une nouvelle méthode. Par exemple, lors de l'ajout d'une nouvelle instance de fournisseur d'identité tiers à votre déploiement.

4 Modifiez les paramètres de la méthode d'authentification.

Élément de formulaire	Description
Nom	Tapez un nom pour cette instance de fournisseur d'identité.
Contexte SAML	Sélectionnez le contexte SAML approprié dans le menu déroulant. La liste inclut les contextes d'authentification SAML actuellement pris en charge conformément aux spécifications SAML 2.0.
Score d'authentification	Lorsque vous créez des stratégies d'accès pour l'ensemble de stratégies d'accès par défaut ou pour des ensembles de stratégies spécifiques à une application Web, vous devez configurer un score d'authentification minimal. Les stratégies obligent les utilisateurs à s'authentifier à l'aide d'une méthode d'authentification dotée du score d'authentification spécifié ou plus élevé pour accéder à Workspace (dans le cas d'une stratégie d'accès par défaut) ou à une application Web (dans le cas d'une stratégie spécifique à une application Web). Appliquez un score d'authentification basé sur vos niveaux de sécurité prédéterminés pour les méthodes d'authentification.
Méthode par défaut	Pour désigner la méthode d'authentification comme méthode par défaut, sélectionnez **Méthode par défaut**. L'option **Méthode par défaut** est associée à l'option Contexte SAML. La situation suivante illustre l'utilisation par Workspace de la méthode d'authentification que vous avez désignée comme méthode par défaut. Lors de l'ajout d'une méthode d'authentification, vous sélectionnez un contexte SAML. Plus tard, le contexte SAML que l'instance de fournisseur d'identité tiers envoie ne correspond pas au contexte SAML que vous avez sélectionné pour cette instance de fournisseur d'identité et Workspace ne reconnaît pas le contexte SAML envoyé. Workspace ne termine pas la tentative d'authentification mais tente plutôt d'authentifier l'utilisateur à l'aide de la méthode d'authentification que vous avez sélectionnée comme méthode par défaut.

5 Cliquez sur **Enregistrer**.

Suivant

- Associez chaque méthode d'authentification à l'instance de fournisseur d'identité appropriée. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.

- Associez les stratégies d'accès à des méthodes d'authentification en définissant le score d'authentification minimal approprié pour chaque stratégie d'accès.

Ajouter et configurer une instance de fournisseur d'identité

En ajoutant et en configurant des instances de fournisseur d'identité à votre déploiement d'Workspace, vous assurez une haute disponibilité, introduisez des méthodes d'authentification d'utilisateurs supplémentaires et améliorez la souplesse de gestion du processus d'authentification des utilisateurs en fonction des plages d'adresses IP de ces derniers.

Ajoutez des instances de fournisseur d'identité supplémentaires à votre déploiement d'Workspace à des fins de haute disponibilité.

Prérequis

- Effectuez la planification nécessaire.
  - Déterminez le meilleur moyen d'intégrer Workspace à Active Directory pour répondre aux besoins de votre organisation. Vous pouvez configurer un seul domaine ou une forêt à domaines multiples.
  - Déterminez les types d'authentification requis pour répondre aux besoins de votre organisation. Par exemple, vous pouvez configurer l'authentification Kerberos pour les utilisateurs internes à votre organisation et l'authentification RSA SecurID pour les utilisateurs externes. Vous pouvez définir ce type de configuration en utilisant une seule et unique instance de fournisseur d'identité pour les deux méthodes d'authentification ou une instance de fournisseur d'identité distincte pour chaque méthode d'authentification.
- Déployez Workspace avec un seul domaine Active Directory pendant la validation technique de votre déploiement.
- Préparez des instances de fournisseurs d'identité supplémentaires pour votre déploiement d'Workspace.
  - Pour ajouter une instance de fournisseur d'identité tiers, procédez comme suit. Reportez-vous à « Aperçu de la configuration d'Workspace de manière à utiliser une instance de fournisseur d'identité tiers », page 22 pour consulter la liste complète des tâches liées à la configuration d'Workspace permettant d'utiliser un fournisseur d'identité tiers.
    - Vérifiez que les instances tierces sont conformes à la norme SAML 2.0 et que Workspace peut y accéder.
    - Déterminez la manière dont Workspace obtient les métadonnées de l'instance tierce, puis copiez et enregistrez les informations de métadonnées appropriées de l'instance tierce (vous pouvez coller ces informations dans Console d'administration Workspace lors de la configuration). Les informations de métadonnées que vous obtenez de l'instance tierce correspondent à l'URL d'accès aux métadonnées ou aux métadonnées proprement dites.
    - Pour permettre à Workspace d'utiliser des méthodes d'authentification supplémentaires, configurez-les à l'aide de console d'administration. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18.
- Utilisez console d'administration pour configurer des plages réseau. Voir « Ajout ou modification d'une plage réseau », page 17

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Paramètres > Fournisseurs d'identité**.

3 Cliquez sur **Ajouter un fournisseur d'identité**. Cette option vous invite à entrer les informations qui permettent à Workspace d'enregistrer une instance de fournisseur d'identité tiers.

4 Modifiez les paramètres de l'instance de fournisseur d'identité.

Élément de formulaire	Description
Type	Sélectionnez **Manuel** pour les instances de fournisseurs d'identité tiers. **Remarque** Ne sélectionnez Automatique que si l'assistance technique VMware vous y invite.
Nom du fournisseur	Tapez un nom pour cette instance de fournisseur d'identité.
Description	Tapez une description pour cette instance de fournisseur d'identité.
Magasin d'utilisateurs	La zone de texte Magasin d'utilisateurs répertorie les magasins d'utilisateurs disponibles dans votre déploiement d'Workspace. Sélectionnez tous les magasins d'utilisateurs que vous souhaitez associer à cette instance de fournisseur d'identité.
Méthodes d'authentification	La zone de texte Méthodes d'authentification répertorie les méthodes d'authentification d'utilisateur disponibles dans votre déploiement d'Workspace. La liste inclut les méthodes d'authentification par défaut et les méthodes d'authentification supplémentaires que vous avez précédemment ajoutées pour prendre en charge des fournisseurs d'identité tiers. L'ajout de méthodes d'authentification supplémentaires est décrit comme une condition préalable à cette tâche. Si la méthode d'authentification que vous prévoyez de sélectionner ne figure pas dans la liste, ajoutez-la de la manière décrite dans la condition préalable. Sélectionnez les méthodes d'authentification d'Workspace à appliquer lorsque les utilisateurs associés à cette instance de fournisseur d'identité se connectent. **Remarque** Vérifiez que les méthodes d'authentification sélectionnées sont activées et correctement configurées. Reportez-vous à *Installation et configuration d' Workspace*.
Configurer via	L'option Configurer via est disponible uniquement lorsque vous ajoutez une instance de fournisseur d'identité tiers et sélectionnez Manuel comme type de fournisseur d'identité. Sélectionnez une méthode d'identificateur d'URL. ■ Sélectionnez URL de découverte automatique pour permettre à Workspace de recevoir les métadonnées de l'instance de fournisseur d'identité tiers à des fins d'enregistrement, tapez l'URL donnant accès aux métadonnées dans la zone de texte **Découverte automatique**. ■ Sélectionnez XML de métadonnées et copiez les métadonnées XML de l'instance de fournisseur d'identité et collez-les dans la zone de texte **XML de métadonnées**.
Plages réseau	La zone de texte Plages réseau répertorie les plages réseau existantes dans votre déploiement d'Workspace. Sélectionnez les plages réseau des utilisateurs, en fonction de leurs adresses IP, que vous souhaitez diriger vers cette instance de fournisseur d'identité à des fins d'authentification.

5 Cliquez sur **Enregistrer**.

6 Si nécessaire, changez l'ordre des instances de fournisseurs d'identité.

Workspace recherche une adresse IP dans la liste des instances de fournisseurs d'identité, de haut en bas. Si une adresse IP est attribuée à plusieurs instances de fournisseurs d'identité, Workspace reconnaît la première instance, celle se trouvant le plus haut dans la liste.

a Cliquez sur **Modifier l'ordre des fournisseurs d'identité**.

b Utilisez les flèches haut et bas pour placer une instance de fournisseur d'identité à la position appropriée.

c Cliquez sur **Enregistrer**.

Suivant

■ Si vous configurez Workspace pour un environnement à forêts multiples, indiquez à vos utilisateurs d'Workspace leurs domaines respectifs et précisez que, lors de la connexion, ils doivent sélectionner un domaine dans le menu déroulant. Indiquez-leur qu'ils peuvent cocher la case **Mémoriser ce paramètre** pour empêcher l'affichage de cette invite à chaque connexion.

- Si vous avez ajouté une instance de fournisseur d'identité tiers, copiez et enregistrez les informations d'Workspace requises pour configurer cette instance. Voir « Obtenir les informations SAML d'Workspace requises pour configurer une instance de fournisseur d'identité tiers », page 23.

Aperçu de la configuration d' Workspace de manière à utiliser une instance de fournisseur d'identité tiers

Pour configurer Workspace de manière à utiliser une instance de fournisseur d'identité tiers, vous devez effectuer des étapes spécifiques.

Pré-configuration

Exécutez les tâches suivantes avant d'utiliser Workspace console d'administration pour ajouter l'instance de fournisseur d'identité tiers.

1. Vérifiez que les instances tierces sont conformes à la norme SAML 2.0 et que Workspace peut y accéder.
2. Déterminez la manière dont Workspace obtient les métadonnées de l'instance tierce, puis copiez et enregistrez les informations de métadonnées appropriées de l'instance tierce (vous pouvez coller ces informations dans Workspace console d'administration lors de la configuration). Les informations de métadonnées que vous obtenez de l'instance tierce correspondent à l'URL d'accès aux métadonnées ou aux métadonnées proprement dites.
3. Pour permettre à Workspace d'utiliser les méthodes d'authentification prises en charge par le fournisseur d'identité tiers, utilisez console d'administration pour configurer les méthodes d'authentification supplémentaires. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18
4. Pour modifier des méthodes d'authentification, cochez la case **Méthode par défaut**. Vous permettez ainsi à Workspace d'utiliser cette méthode d'authentification en cas de problème avec la méthode d'authentification tierce. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18.

Configuration

Pour ajouter une instance de fournisseur d'identité, effectuez les étapes suivantes spécifiques aux fournisseurs d'identité tiers. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.

1. Dans la page console d'administration, Paramètres > Fournisseurs d'identité, cliquez sur le bouton **+ Ajouter un fournisseur d'identité** et sélectionnez **Manuel** dans le menu déroulant **Type**.
2. Sélectionnez les méthodes d'authentification prises en charge par l'instance de fournisseur d'identité tiers que vous prévoyez d'utiliser avec Workspace.
3. Utilisez l'option **Configurer via** pour sélectionner le mode de transfert des métadonnées de l'instance de fournisseurs d'identité tiers à Workspace, soit par l'utilisation d'une URL pointant vers les métadonnées soit par copier-coller de ces dernières.

Post-configuration

Collectez les informations SAML d'Workspace et appliquez-les à l'instance de fournisseur d'identité tiers. Voir « Obtenir les informations SAML d'Workspace requises pour configurer une instance de fournisseur d'identité tiers », page 23.

1. Utilisez Workspace console d'administration pour collecter les informations SAML nécessaires pour configurer l'instance de fournisseur d'identité tiers.
2. Configurez l'instance de fournisseur d'identité tiers en appliquant les informations SAML que vous avez collectées d'Workspace.

Obtenir les informations SAML d' Workspace requises pour configurer une instance de fournisseur d'identité tiers

Lors de l'intégration d'Workspace avec une instance de fournisseur d'identité tiers, après l'exécution de la configuration côté Workspace, vous devez copier et préparer les informations de certificat SAML requises pour effectuer la configuration côté fournisseur d'identité tiers.

Procédure

1 Connectez-vous à console d'administration.

2 Sélectionnez **Paramètres > Certificat SAML**

3 Copiez et enregistrez le certificat de signature SAML qui s'affiche dans Workspace.

   a Copiez les informations du certificat qui se trouve dans la section Certificat de signature.

   b Enregistrez les informations du certificat dans un fichier texte en vue d'une utilisation ultérieure, lors de la configuration de l'instance de fournisseur d'identité tiers.

4 Rendez les métadonnées SAML du fournisseur de services (SP) disponibles à l'instance de fournisseur d'identité tiers.

   a Dans la page Télécharger un certificat SAML, cliquez sur **Métadonnées du fournisseur de services (SP)**.

   b Copiez et enregistrez les informations affichées en utilisant la méthode convenant le mieux à votre organisation.

   Utilisez ces informations copiées ultérieurement, lors de la configuration du fournisseur d'identité tiers.

Méthode	Description
Copier l'URL de la page	Copiez et enregistrez l'URL de la page des métadonnées du fournisseur de services (SP).
Copier le contenu XML de la page	Copiez et enregistrez le contenu de la page dans un fichier texte.

5 Déterminez le mappage utilisateur de l'instance de fournisseur d'identité tiers à Workspace.

   Lorsque vous configurez le fournisseur d'identité tiers, modifiez l'assertion SAML dans le fournisseur d'identité tiers pour mapper des utilisateurs Workspace.

Format NameID	Mappage d'utilisateurs
urn:oasis:names:tc:SAML: 2.0:nameid-format:emailAddress	La valeur NameID dans l'assertion SAML est mappée à l'attribut d'adresse e-mail dans Workspace.
urn:oasis:names:tc:SAML: 2.0nameid-format:unspecified	La valeur NameID dans l'assertion SAML est mappée à l'attribut username dans Workspace.

Suivant

Appliquez si nécessaire les informations que vous avez copiées pour cette tâche pour configurer l'instance de fournisseur d'identité tiers.

Modification de l'ensemble de stratégies d'accès par défaut

Workspace inclut un ensemble de stratégies d'accès par défaut qui contrôle l'accès de l'utilisateur au portail des applications d'Workspace. Vous pouvez modifier l'ensemble de stratégies pour modifier les stratégies si nécessaire.

Chaque stratégie de l'ensemble de stratégies d'accès par défaut nécessite qu'un ensemble de critères soient remplis afin qu'Workspace autorise l'accès au portail des applications. Voir Chapitre 5, « Gestion des ensembles de stratégies d'accès », page 25.

L'ensemble de stratégies d'accès suivant sert d'exemple de configuration de l'ensemble de stratégies d'accès par défaut afin de contrôler l'accès au portail des applications d'Workspace. Pour obtenir des instructions, reportez-vous à la section « Modifier un ensemble de stratégies d'accès », page 28.

Exemple d'ensemble de stratégies d'accès par défaut

Cet exemple illustre la façon dont vous pouvez modifier l'ensemble de stratégies par défaut.

Nom de stratégie	Réseau	Score d'authentification minimal	TTL (heures)
Interne	Plage interne	1	8
Externe	Toutes les plages	3	4

Les stratégies sont évaluées dans l'ordre précédent. Vous pouvez faire glisser une stratégie vers le haut ou vers le bas dans un ensemble de stratégies afin de modifier la priorité en termes d'évaluation.

L'exemple précédent d'ensemble de stratégies s'applique au cas d'utilisation suivant.

Stratégies d'accès par défaut, cas d'utilisation de navigateur

1
- Interne. Pour accéder à Workspace à partir d'un réseau interne (plage interne), Workspace présente aux utilisateurs la méthode d'authentification par mot de passe Active Directory. Pour s'assurer que Workspace tente d'abord d'authentifier les utilisateurs avec l'authentification Kerberos, attribuez à l'authentification de la méthode Kerberos un score plus élevé que celui de la méthode par mot de passe et placez Kerberos en haut de la liste sur la page Méthodes d'authentification. Vous pouvez également attribuer une plage réseau aux utilisateurs internes. L'utilisateur se connecte à l'aide d'un navigateur et a désormais accès au portail de l'utilisateur pour une session de huit heures.
- Externe. Pour accéder à Workspace à partir d'un réseau externe (Toutes les plages), l'utilisateur doit se connecter avec SecurID qui, selon l'exemple, a un score d'authentification de 3. L'utilisateur se connecte à l'aide d'un navigateur et a désormais accès au portail des applications pour une session de quatre heures.

2 Lorsqu'un utilisateur tente d'accéder à une ressource (sauf s'il s'agit d'une application Web couverte par un ensemble de stratégies spécifiques à une application Web), l'ensemble de stratégies d'accès au portail par défaut s'applique.

   Par exemple, la durée de vie (TTL) de ce type de ressources correspond à la valeur TTL de l'ensemble de stratégies d'accès au portail par défaut. Si la valeur TTL d'un utilisateur qui se connecte au portail des applications est de 8 heures conformément à l'ensemble de stratégies d'accès au portail par défaut, lorsque l'utilisateur tente de lancer une ressource durant la session TTL, l'application démarre sans demander à l'utilisateur de s'authentifier à nouveau.

Gestion des ensembles de stratégies d'accès

5

Vous pouvez configurer l'ensemble de stratégies d'accès par défaut de manière à spécifier les critères à satisfaire pour permettre aux utilisateurs d'accéder à leur Portail des applications Workspace. Vous pouvez également créer des ensembles de stratégies d'accès spécifiques à une application Web afin de préciser les critères à satisfaire pour permettre aux utilisateurs de lancer les applications Web spécifiées.

Pour appliquer une stratégie d'accès, créez la stratégie dans le cadre d'un ensemble de stratégies d'accès. Chaque stratégie dans un ensemble de stratégies d'accès peut spécifier les éléments suivants.

- L'emplacement à partir duquel les utilisateurs sont autorisés à se connecter, par exemple à l'intérieur ou à l'extérieur du réseau de l'entreprise.
- Le score d'authentication minimal, qui définit les méthodes d'authentication autorisées pour cette stratégie.
- Le nombre d'heures d'accès dont disposent les utilisateurs.

Remarque Les stratégies d'accès d'Workspace ne contrôlent pas la durée d'une session d'application Web. Elles contrôlent plutôt la durée de la période pendant laquelle les utilisateurs peuvent lancer une application Web.

Workspace dispose d'un ensemble de stratégies d'accès par défaut que vous pouvez modifier. Cet ensemble de stratégies d'accès contrôle globalement l'accès à Workspace. Voir « Modification de l'ensemble de stratégies d'accès par défaut », page 24. Pour contrôler l'accès à des applications Web spécifiques, vous pouvez créer des ensembles de stratégies d'accès supplémentaires. Si vous n'appliquez pas un ensemble de stratégies d'accès à une application Web, l'ensemble de stratégies d'accès par défaut s'applique.

Ce chapitre aborde les rubriques suivantes :

Aperçu des paramètres de stratégie d'accès

Un ensemble de stratégies d'accès contient une ou plusieurs stratégies d'accès. Chaque stratégie d'accès est composée de paramètres que vous pouvez configurer pour gérer l'accès de l'utilisateur à Portail des applications Workspace de façon globale ou à des applications Web spécifiques.

Chaque stratégie d'accès lie une plage réseau à un score d'authentification minimal. Un utilisateur se connectant à partir d'une adresse IP comprise dans la plage réseau spécifiée de la stratégie se voit proposer une méthode d'authentification d'un score égal ou supérieur au score d'authentification minimal de la stratégie. Chaque instance de fournisseur d'identité de votre déploiement d'Workspace lie également des plages réseau à des méthodes d'authentification. Lorsque vous configurez une stratégie d'accès, assurez-vous que la plage réseau que vous associez au score d'authentification est couverte par une instance de fournisseur d'identité existante.

Lorsque vous créez une stratégie d'accès, vous configurez les paramètres suivants.

Réseau

Pour chaque stratégie d'accès, vous déterminez la base d'utilisateurs en spécifiant une plage réseau. Une plage réseau est composée d'une ou de plusieurs plages d'adresses IP. Vous créez des plages réseau sur la page Plages réseau de console d'administration avant de configurer des ensembles de stratégies d'accès.

Score d'authentification minimal

Vous attribuez un score d'authentification à chaque méthode d'authentification lorsque vous configurez la page Méthodes d'authentification dans console d'administration avant de configurer des ensembles de stratégies d'accès.

Par défaut, Workspace prend en charge les méthodes d'authentification d'utilisateur par mot de passe Active Directory, Kerberos et RSA SecurID. Lorsque vous intégrez des instances de fournisseur d'identité tiers à votre déploiement d'Workspace, Workspace étend la prise en charge aux méthodes d'authentification supplémentaires prises en charge par les fournisseurs d'identité tiers.

Lorsqu'un utilisateur se connecte à Workspace, Workspace enregistre l'heure de l'authentification et la méthode utilisée pour procéder à celle-ci.

Lorsque l'utilisateur tente ensuite d'accéder à une application Web disposant d'un ensemble de stratégies d'accès attribué, Workspace compare le score d'authentification actuel de l'utilisateur au score d'authentification requis pour accéder à l'application Web. Si le score d'authentification actuel de l'utilisateur est inférieur au score d'authentification minimal requis pour l'application demandée, Workspace redirige l'utilisateur vers une instance de fournisseur d'identité qui fournit le niveau d'authentification supérieur. Si le score d'authentification actuel de l'utilisateur est égal ou supérieur au score d'authentification minimal requis pour l'application demandée, Workspace lance l'application après vérification de la valeur de durée de vie. Voir la description de la durée de vie ci-dessous. Workspace refuse la demande d'accès au portail des applications ou la demande de lancement d'une application Web dans les conditions suivantes.

- Aucune stratégie n'est définie pour la demande.
- Aucune instance de fournisseur d'identité n'est définie pour le score d'authentification minimal.
- L'utilisateur n'a pas pu s'authentifier avec toutes les méthodes d'authentification.

Durée de vie

Pour chaque stratégie d'accès, vous attribuez une valeur de durée de vie (TTL). La valeur TTL détermine la période maximale dont disposent les utilisateurs depuis leur dernier événement d'authentification pour accéder à Workspace ou pour lancer une application Web spécifique. Par exemple, une valeur TTL de 4 dans une stratégie d'application Web donne aux utilisateurs quatre heures pour lancer l'application Web sans devoir initier un autre événement d'authentification et étendre la valeur TTL.

Gestion des ensembles de stratégies d'accès spécifiques à une application Web

Vous pouvez créer des stratégies d'accès spécifiques à une application. Par exemple, vous pouvez créer un ensemble de stratégies d'accès pour une application Web qui spécifie les adresses IP ayant accès à l'application, les méthodes d'authentification à utiliser et l'intervalle au terme duquel une réauthentification est requise.

ATTENTION Une bonne pratique consiste à configurer le score d'authentification minimal des stratégies spécifiques à une application Web de manière qu'il soit égal ou supérieur au score d'authentification minimal des stratégies de l'ensemble de stratégies d'accès par défaut disposant des plages réseau correspondantes.

L'ensemble de stratégies d'accès spécifiques à une application Web suivant fournit un exemple d'ensemble de stratégies que vous pouvez créer pour contrôler l'accès aux applications Web spécifiées. Voir Chapitre 5, « Gestion des ensembles de stratégies d'accès », page 25.

Exemple 1 : ensemble de stratégies spécifiques à une application Web

Cet exemple illustre un ensemble de stratégies que vous pouvez créer et appliquer à une application sensible.

Nom de stratégie	Réseau	Score d'authentification minimal	TTL (heures)
Interne	Plage interne	1	8
Externe	Toutes les plages	3	4

Les stratégies sont évaluées dans l'ordre précédent. Vous pouvez faire glisser une stratégie vers le haut ou vers le bas dans un ensemble de stratégies afin de modifier la priorité en termes d'évaluation.

L'exemple d'ensemble de stratégies précédent s'applique aux cas d'utilisation suivants.

Ensemble de stratégies d'accès spécifiques à une application Web, cas d'utilisation du navigateur

1. Pour accéder à Workspace à l'extérieur du réseau de l'entreprise, l'utilisateur doit se connecter avec RSA SecurID qui, selon l'exemple, a un score d'authentification minimal de 3. Reportez-vous à l'exemple de stratégie Externe dans « Modification de l'ensemble de stratégies d'accès par défaut », page 24. L'utilisateur se connecte à l'aide d'un navigateur et a désormais accès au portail des applications pour une session de quatre heures, comme défini par l'ensemble de stratégies d'accès par défaut.
2. Au bout de 4 heures, l'utilisateur tente de lancer une application Web à laquelle l'exemple 1 d'ensemble de stratégies propres aux applications Web est appliqué.
3. Workspace vérifie les stratégies de l'exemple 1 d'ensemble de stratégies et applique la stratégie Externe avec la plage réseau Toutes les plages, car la demande de l'utilisateur provient d'un navigateur Web et de la plage réseau Toutes les plages.

L'utilisateur se connecte avec un score d'authentification minimal de 3, score convenant au lancement de l'application sensible, mais le TTL de la stratégie vient d'expirer. Par conséquent, l'utilisateur est redirigé pour une réauthentification. La réauthentification fournit à l'utilisateur une autre session de 4 heures et la possibilité de lancer l'application. Pendant les 4 heures suivantes, l'utilisateur peut continuer à lancer l'application sans devoir se réauthentifier.

Exemple 2 : ensemble de stratégies spécifiques à une application Web

Cet exemple illustre un ensemble de stratégies que vous pouvez créer et appliquer à une application particulièrement sensible.

Nom de stratégie	Réseau	Score d'authentification minimal	TTL (heures)
ExtraSensitive	Toutes les plages	Niveau 3	1

L'exemple précédent d'ensemble de stratégies s'applique au cas d'utilisation suivant.

Ensemble supplémentaire de stratégies d'accès spécifiques à une application Web strict, cas d'utilisation

1. L'utilisateur se connecte depuis l'intérieur du réseau de l'entreprise en utilisant la méthode d'authentification par mot de passe, ce qui correspond au niveau 1 selon l'exemple. Reportez-vous à l'exemple de stratégie Interne dans « Modification de l'ensemble de stratégies d'accès par défaut », page 24.

   L'utilisateur a dorénavant accès au portail des applications pour une durée de huit heures.
2. L'utilisateur tente immédiatement de lancer une application Web à laquelle l'exemple 2 d'ensemble de stratégies est appliqué et qui nécessite une authentification de niveau 3 ou supérieur.
3. L'utilisateur est redirigé vers un fournisseur d'identité qui fournit un niveau d'authentification 3 ou supérieur nécessitant une authentification RSA SecurID.
4. Une fois que l'utilisateur s'est connecté, Workspace lance l'application et enregistre l'événement d'authentification.

   L'utilisateur peut continuer à lancer cette application pendant une période maximale d'une heure, mais il doit se réauthentifier au bout d'une heure, sauf s'il initie un événement d'authentification de niveau 3 ou supérieur à moins d'une heure du lancement, comme le spécifie la stratégie.

Modifier un ensemble de stratégies d'accès

Vous pouvez modifier l'ensemble de stratégies d'accès par défaut, lequel est un ensemble de stratégies préexistant qui contrôle globalement l'accès de l'utilisateur à Workspace, ou vous pouvez modifier les ensembles de stratégies spécifiques à une application Web que vous avez précédemment créés manuellement.

Vous pouvez à tout moment supprimer un ensemble de stratégies d'accès spécifiques à une application Web. L'ensemble de stratégies d'accès par défaut est permanent. Vous pouvez le modifier, mais pas le supprimer.

Vous pouvez modifier un ensemble de stratégies d'accès existant (soit l'ensemble de stratégies d'accès par défaut, soit un ensemble de stratégies d'accès spécifiques à une application Web) en supprimant des stratégies existantes de l'ensemble, en les modifiant ou en y ajoutant de nouvelles. Pour une présentation des ensembles de stratégies d'accès, reportez-vous à Chapitre 5, « Gestion des ensembles de stratégies d'accès », page 25.

Pour plus d'informations et des exemples d'ensembles de stratégies, consultez la rubrique appropriée.

- « Modification de l'ensemble de stratégies d'accès par défaut », page 24.

- « Gestion des ensembles de stratégies d'accès spécifiques à une application Web », page 27.

Prérequis

- Configurez les fournisseurs d'identité adaptés à votre déploiement. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.
- Configurez les plages réseau adaptées à votre déploiement d'Workspace. Voir « Ajout ou modification d'une plage réseau », page 17.
- Configurez les méthodes d'authentification adaptées à votre déploiement. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Stratégies > Ensembles de stratégies d'accès**.

3 (Facultatif) Pour supprimer de façon permanente un ensemble de stratégies d'accès spécifiques à une application Web, cliquez sur **Supprimer** pour l'ensemble de stratégies.

L'option **Supprimer** n'est pas disponible pour l'ensemble de stratégies d'accès par défaut. L'ensemble de stratégies d'accès par défaut ne peut pas être supprimé.

4 Cliquez sur **Modifier** pour l'ensemble de stratégies existant à configurer.

5 (Facultatif) Si nécessaire, modifiez le nom et la description de l'ensemble de stratégies dans les zones de texte respectives.

Remarque Workspace affiche le texte des zones de texte Nom de l'ensemble de stratégies et Description en anglais. Vous pouvez modifier ce texte, notamment le traduire dans une autre langue.

6 (Facultatif) Si nécessaire, modifiez ou supprimez une stratégie existante, ou bien ajoutez une nouvelle stratégie.

Une bonne pratique consiste à configurer le score d'authentification minimal des stratégies spécifiques à une application Web de manière qu'il soit égal ou supérieur au score d'authentification minimal des stratégies de l'ensemble de stratégies d'accès par défaut disposant des plages réseau correspondantes.

Option	Description
Modifier une stratégie existante	a Cliquez sur le nom de la stratégie à configurer. b Modifiez les paramètres de la stratégie selon vos besoins. c Cliquez sur **Appliquer**.
Supprimer une stratégie existante	a Cliquez sur le nom de la stratégie à supprimer. b Cliquez sur **Supprimer**.
Ajouter une nouvelle stratégie	a Cliquez sur **+ Stratégie d'accès** pour ajouter une nouvelle stratégie. b Configurez les paramètres de la stratégie de façon appropriée. c Cliquez sur **Ajouter**.

7 Cliquez sur **Enregistrer**.

L'ensemble de stratégies d'accès modifié prend immédiatement effet.

Suivant

Si l'ensemble de stratégies est un ensemble de stratégies d'accès spécifique d'une application Web qui n'est pas encore appliqué, appliquez l'ensemble de stratégies à une ou plusieurs applications Web.

Ajouter un ensemble de stratégies d'accès spécifiques à une application Web

Vous pouvez créer un ensemble de stratégies d'accès spécifiques à une application Web pour gérer l'accès des utilisateurs à des applications Web spécifiques.

Pour une présentation des ensembles de stratégies d'accès, reportez-vous à Chapitre 5, « Gestion des ensembles de stratégies d'accès », page 25. Pour plus d'informations et pour voir des exemples d'ensembles de stratégies d'accès spécifiques à une application Web, reportez-vous à « Gestion des ensembles de stratégies d'accès spécifiques à une application Web », page 27.

Prérequis

- Configurez les fournisseurs d'identité adaptés à votre déploiement. Voir « Ajouter et configurer une instance de fournisseur d'identité », page 20.
- Configurez les plages réseau adaptées à votre déploiement d'Workspace. Voir « Ajout ou modification d'une plage réseau », page 17.
- Configurez les méthodes d'authentification adaptées à votre déploiement. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18.
- Plus particulièrement lors de l'initialisation de la configuration d'Workspace, si vous prévoyez de modifier l'ensemble de stratégies d'accès au portail par défaut (pour contrôler globalement l'accès des utilisateurs à Workspace), apportez ces modifications avant de créer des ensembles de stratégies spécifiques à une application Web.

Procédure

1. Connectez-vous à Console d'administration Workspace.
2. Sélectionnez **Stratégies > Ensembles de stratégies d'accès**.
3. Cliquez sur **+ Ensemble de stratégies d'accès** pour ajouter un nouvel ensemble de stratégies.
4. Ajoutez le nom et la description d'un ensemble de stratégies dans les zones de texte respectives.
5. Cliquez sur **+ Stratégie d'accès** pour ajouter la première stratégie.
6. Configurez les paramètres de la stratégie de façon appropriée.

Attention Une bonne pratique consiste à configurer le score d'authentification minimal des stratégies spécifiques à une application Web de manière qu'il soit égal ou supérieur au score d'authentification minimal des stratégies de l'ensemble de stratégies d'accès par défaut disposant des plages réseau correspondantes.

7. Cliquez sur **Ajouter**.
8. (Facultatif) Ajoutez d'autres stratégies en répétant la procédure, jusqu'à ce que l'ensemble de stratégies convienne aux besoins de votre organisation.
9. Cliquez sur **Enregistrer** pour enregistrer l'ensemble de stratégies.

Suivant

Appliquez l'ensemble de stratégies à une ou plusieurs applications Web.

Appliquer un ensemble de stratégies d'accès spécifiques à une application Web

Une fois que vous avez créé un ensemble de stratégies d'accès spécifiques à une application Web, vous pouvez appliquer cet ensemble à des applications Web spécifiques afin d'en contrôler l'accès.

Workspace applique l'ensemble de stratégie d'accès par défaut à toutes les nouvelles applications Web. Vous devez appliquer un ensemble de stratégies spécifique à une application Web pour remplacer l'ensemble de stratégies d'accès par défaut.

Prérequis

Si ce n'est pas déjà fait, créez un ensemble de stratégies spécifiques à une application Web pour contrôler l'accès de l'utilisateur à une application Web spécifique. Voir « Ajouter un ensemble de stratégies d'accès spécifiques à une application Web », page 30

Procédure

1 Cliquez sur l'onglet **Catalogue**.

2 Cliquez sur **Tous les types d'applications > Applications Web**.

3 Cliquez sur l'application Web à laquelle vous souhaitez appliquer un ensemble de stratégies d'accès spécifiques à une application Web.

La page d'informations de l'application Web s'affiche avec l'onglet **Droits** sélectionné par défaut.

4 Cliquez sur **Stratégies d'accès**.

5 Dans le menu déroulant Ensemble de stratégies d'accès, sélectionnez l'ensemble de stratégies d'accès spécifiques à une application Web que vous souhaitez appliquer à l'application.

6 Cliquez sur **Enregistrer**.

L'ensemble de stratégies d'accès contrôle désormais l'accès des utilisateurs à l'application.

Gestion des utilisateurs et des groupes

6

Vous pouvez gérer et surveiller des utilisateurs et des groupes, ce qui inclut les utilisateurs et les groupes importés d'Active Directory, les utilisateurs invités et les groupes Workspace.

Dans Workspace console d'administration, la page Utilisateurs et groupes fournit un affichage axé sur les utilisateurs et les groupes d'Workspace. Par exemple, depuis la page Droits d'un utilisateur, vous pouvez octroyer une ressource à cet utilisateur, et depuis la page Droits d'un groupe, vous pouvez octroyer une ressource à ce groupe. Vous pouvez aussi choisir une vue axée sur les ressources d'Workspace en utilisant la page du Catalogue. Par exemple, depuis la page Droits d'une ressource, vous pouvez octroyer cette ressource à un utilisateur ou à un groupe.

Ce chapitre aborde les rubriques suivantes :

Types d'utilisateurs et de groupes d' Workspace

Workspace console d'administration vous permet de gérer les utilisateurs, les utilisateurs invités et les groupes.

Utilisateurs

Les utilisateurs de Workspace sont les utilisateurs importés à partir d'Active Directory. La base d'utilisateurs Workspace est mise à jour en fonction de la planification de synchronisation de votre serveur de dossiers.

Groupes

Les types de groupes qui peuvent apparaître dans Console d'administration Workspace sont des groupes importés depuis votre serveur de dossiers et des groupes Workspace, qui sont des groupes que vous créez vous-même à l'aide d'Workspace.

Type de groupe	Description
Groupes du serveur de dossiers	Vous utilisez la page Synchronisation d'annuaires de Administrateur de Connector Services, Sélectionner des groupes pour importer des groupes à partir d'Active Directory vers Workspace. Dans console d'administration, une icône de cadenas en regard du nom d'un groupe indique que ce groupe est un groupe du serveur de dossiers. Vous ne pouvez pas utiliser Workspace pour modifier ou supprimer des groupes du serveur de dossiers. Les groupes importés depuis le serveur d'annuaire sont mis à jour dans Workspace en fonction de la planification de synchronisation de votre serveur d'annuaire.
Groupes Workspace	Vous pouvez utiliser Console d'administration Workspace pour créer des groupes Workspace, qui sont des groupes que vous personnalisez afin de correspondre au mieux à l'utilisation d'Workspace au sein de votre entreprise. Vous pouvez créer des groupes Workspace en ajoutant une combinaison d'utilisateurs et de groupes. Les groupes que vous ajoutez peuvent être des groupes Workspace préexistants, ou des groupes importés depuis votre serveur de dossiers. Dans console d'administration, une case à cocher en regard du nom d'un groupe indique que ce groupe est un groupe Workspace. Vous pouvez utiliser Workspace pour supprimer un groupe Workspace ou pour modifier les utilisateurs du groupe.

Vous pouvez spécifier quelles ressources les membres du groupe peuvent accéder et utiliser. Plutôt que de définir des droits pour chaque utilisateur individuel, vous pouvez accorder des droits à un ensemble d'utilisateurs en accordant des droits au groupe. Un utilisateur peut appartenir à plusieurs groupes. Par exemple, si vous créez un groupe Ventes et un groupe Gestion, un représentant commercial peut appartenir aux deux groupes. Vous pouvez spécifier quels paramètres de stratégies mobiles s'appliquent aux membres du groupe.

Gérer les groupes d' Workspace

La création de groupes, la modification de l'appartenance aux groupes et la suppression de groupes sont des tâches que vous pouvez effectuer dans Workspace et qui s'appliquent uniquement aux groupes Workspace. L'attribution de groupes aux ressources est une tâche que vous pouvez effectuer pour les groupes Workspace et les groupes Active Directory.

Procédure

- Pour créer un groupe Workspace, sélectionnez **Utilisateurs & Groupes > Groupes**, cliquez sur **Créer un groupe** et entrez le nom et la description du groupe.
- Pour supprimer un ou plusieurs groupes Workspace, sélectionnez **Utilisateurs & Groupes > Groupes**, cochez les cases qui correspondent aux groupes Workspace que vous voulez supprimer et cliquez sur **Supprimer des groupes**.

  Vous pouvez supprimer uniquement des groupes Workspace. Une icône de verrouillage s'affiche en regard des noms de groupes Active Directory. Elle indique que le groupe est un groupe Active Directory et que vous ne pouvez pas utiliser Workspace pour le modifier ou le supprimer.

Modifier l'appartenance à un groupe Workspace

Vous pouvez modifier l'appartenance à un groupe Workspace.

Utilisez les groupes pour attribuer simultanément plusieurs utilisateurs aux mêmes ressources, plutôt que d'attribuer chaque utilisateur individuellement.

Vous pouvez utiliser les règles de groupe pour définir les utilisateurs qui sont membres d'un groupe Workspace particulier. Un utilisateur peut appartenir à plusieurs groupes. Par exemple, si vous créez un groupe Ventes et un groupe Gestion, un gestionnaire des ventes peut être membre des deux groupes.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Utilisateurs et groupes > Groupes**.

- Une case à cocher en regard du nom d'un groupe indique qu'il s'agit d'un groupe Workspace.
- Un cadenas en regard du nom d'un groupe indique que le groupe est un groupe du serveur de dossiers. Vous devez gérer les groupes du serveur de dossiers directement sur ce serveur. Vous ne pouvez pas utiliser Workspace pour définir l'appartenance aux groupes du serveur de dossiers.

3 Cliquez sur le nom du groupe Workspace dont vous souhaitez modifier les règles d'appartenance.

4 Cliquez sur l'onglet **Utilisateurs dans ce groupe**.

Le système affiche la liste des utilisateurs qui sont actuellement membres de ce groupe.

5 Cliquez sur **Modifier les utilisateurs dans ce groupe**.

6 Sélectionnez une option dans le menu déroulant.

Option	Action
L'un des éléments suivants	Accorde l'appartenance au groupe lorsque l'une des conditions d'appartenance au groupe est satisfaite. Cette option fonctionne comme une condition OU. Par exemple, si vous sélectionnez **L'un des éléments suivants** pour les règles Groupe Est Ventes et Groupe Est Marketing, le personnel des Ventes et du Marketing devient membre de ce groupe.
Tous les éléments suivants	Accorde l'appartenance au groupe lorsque toutes les conditions d'appartenance au groupe sont satisfaites. Cette option fonctionne comme une condition ET. Par exemple, si vous sélectionnez **Tous les éléments suivants** pour les règles Groupe Est Ventes et Email Commence par 'région_ouest', seul le personnel des Ventes dans la région Ouest devient membre de ce groupe. Le personnel des Ventes des autres régions ne devient pas membre.

7 Configurez une ou plusieurs règles pour votre groupe Workspace.

Vous pouvez imbriquer des règles.

Option	Action
Groupe	■ Sélectionnez **Est** pour choisir un groupe à associer à ce groupe Workspace. Taper un nom de groupe dans le champ texte. Pendant que vous tapez, une liste de noms de groupe apparaît. ■ Sélectionnez **N'est pas** pour choisir un groupe à exclure de ce groupe Workspace. Taper un nom de groupe dans le champ texte. Pendant que vous tapez, une liste de noms de groupe apparaît.
Règles d'attributs	Les règles suivantes sont disponibles pour tous les attributs, y compris les attributs par défaut et tout attribut personnalisé supplémentaire que votre entreprise a configuré. Des exemples d'attributs sont l'adresse e-mail et le numéro de téléphone. **Remarque** Les règles ne respectent pas la casse. ■ Sélectionnez **Correspond à** pour accorder l'appartenance au groupe aux entrées du serveur de dossiers qui correspondent exactement au critère que vous avez saisi. Par exemple, votre organisation pourrait avoir un département de voyages d'affaires qui partage le même numéro de central téléphonique. Si vous voulez accorder l'accès à une application de réservation de voyages à tous les employés qui partagent le même numéro de téléphone, vous pouvez créer une règle telle que Téléphone Correspond à (555) 555-1000. ■ Sélectionnez **Ne correspond pas à** pour accorder l'appartenance au groupe à toutes les entrées du serveur de dossiers, à l'exception de celles qui correspondent au critère que vous avez entré. Par exemple, si l'un de vos départements partage un numéro de central téléphonique, vous pouvez exclure ce département de l'accès à une application de réseau social en créant une règle telle que Téléphone Ne correspond pas à (555) 555-2000. Les entrées du serveur de dossiers avec d'autres numéros de téléphone ont accès à l'application. ■ Sélectionnez **Commence par** pour accorder l'appartenance au groupe aux entrées du serveur qui commencent par le critère que vous avez entré. Par exemple, l'adresse e-mail de votre organisation peut commencer par le nom du département, comme ventes_nomutilisateur@exemple.com. Si vous voulez accorder l'accès à une application à tous les membres de l'équipe des Ventes, vous pouvez créer une règle telle que E-mail Commence par ventes_. ■ Sélectionnez **Ne commence pas par** pour accorder l'appartenance au groupe à toutes les entrées du serveur de dossiers, à l'exception de celles qui commencent par le critère que vous avez entré. Par exemple, si les adresses e-mail de votre département des ressources humaines sont au format rh_nomutilisateur@exemple.com, vous pouvez refuser l'accès à une application en créant une règle telle que E-mail Ne commence pas par rh_. Les entrées du serveur de dossiers comportant d'autres adresses e-mail ont accès à l'application.

Option	Action
L'un des éléments suivants	L'appartenance au groupe est accordée lorsque l'une des conditions d'appartenance au groupe est satisfaite pour cette règle. Il est possible d'imbriquer les règles. Par exemple, vous pouvez créer une règle qui stipule Tous les éléments suivants : Groupe Est Ventes ; Groupe Est Californie. Pour Groupe Est Californie, Tous les éléments suivants : Téléphone Commence par 415 ; Téléphone Commence par 510. Le membre du groupe doit appartenir à votre équipe des Ventes en Californie et disposer d'un numéro de téléphone qui commence par 415 ou 510.
Tous les éléments suivants	Toutes les conditions à satisfaire pour cette règle. Il est possible d'imbriquer les règles. Par exemple, vous pouvez créer une règle qui stipule L'un des éléments suivants : Groupe Est Gestionnaires ; Groupe Est Service Client. Pour Groupe Est Service Client, Tous les éléments suivants : E-mail Commence par sc_ ; Téléphone Commence par 555. Les membres du groupe peuvent être gestionnaires ou représentants du service client, mais les représentants du service client doivent disposer d'une adresse e-mail qui commence par sc_ et d'un numéro de téléphone qui commence par 555.

8 (Facultatif) Spécifiez des utilisateurs individuels à ajouter à, ou à exclure de, ce groupe Workspace en cochant la case appropriée et en tapant les noms des utilisateurs.

9 Cliquez sur **Suivant**, puis cliquez sur **Enregistrer**.

Informations relatives aux groupes Workspace

Vous pouvez voir des informations détaillées sur un groupe, telles que ses ressources attribuées, son appartenance et ses ensembles de stratégies mobiles appliquées, à l'aide de Workspace console d'administration.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur **Utilisateurs et groupes > Groupes**.

La page affiche la liste de tous les groupes de votre déploiement Workspace ainsi que des informations générales sur chaque groupe.

- Une case à cocher en regard du nom d'un groupe indique qu'il s'agit d'un groupe Workspace. Vous pouvez définir et gérer des groupes Workspace au sein d'Workspace.
- Un cadenas en regard du nom d'un groupe indique que le groupe est un groupe du serveur de dossiers. Vous pouvez gérer les groupes du serveur de dossiers sur le serveur de dossier de votre organisation.
- La page affiche les informations suivantes sur chaque groupe.

Type d'informations	Description
Nombre d'utilisateurs	Le nombre de membres du groupe.
Nombre d'applications	Le nombre de ressources globalement octroyées au groupe.
Magasin d'utilisateurs	Le magasin d'utilisateurs auquel un groupe Active Directory est associé. Sauf si Workspace est déployé dans un environnement Active Directory à forêts multiples, le déploiement dispose d'un magasin d'utilisateurs unique nommé default.

3 Cliquez sur le nom d'un groupe.

La page de détails du groupe est affichée, le nom du groupe figurant en haut de la page.

4 Cliquez sur l'onglet qui correspond aux informations que vous voulez voir.

Option	Description
Droits	La page Droits de groupe s'affiche. Dans cette page, vous pouvez : ■ Voir la liste des ressources attribuées aux utilisateurs du groupe. ■ Cliquez sur **Ajouter un droit** pour attribuer aux utilisateurs du groupe les ressources qui sont disponibles dans votre catalogue. ■ Cliquez sur le nom d'une ressource attribuée listée pour afficher la page Modifier de cette ressource. ■ Pour les types de ressources disposant d'un bouton **Modifier**, vous pouvez cliquer sur ce bouton pour attribuer les ressources de ce type aux utilisateurs du groupe, pour annuler cette attribution ou pour personnaliser les options de chaque ressource attribuée. Dans la page Droits, vous pouvez apporter les modifications suivantes : ■ Pour les applications Web, cliquez sur **Modifier** pour changer les droits du groupe sur les applications Web ou le type de déploiement pour chacune des applications Web attribuées au groupe. Sélectionnez **Automatique** pour que l'application Web s'affiche par défaut dans le portail de l'utilisateur. Sélectionnez **Activé par l'utilisateur** pour permettre aux utilisateurs d'ajouter l'application Web à leur zone Mes applications à partir de la collection d'applications du Centre des applications auquel ils ont accès. ■ Pour les pools de postes de travail et d'applications View, vous pouvez afficher les droits d'accès existants du groupe aux pools View intégrés à votre système Workspace. Les droits d'accès aux pools de postes de travail et d'applications View sont configurés dans les instances de Serveur de connexion View intégrées à votre système Workspace. Vous ne pouvez pas modifier les droits d'accès aux pools View à l'aide de la page Droits d'accès du groupe. ■ Pour les modules ThinApp, cliquez sur **Modifier** pour modifier les droits du groupe sur les modules ThinApp ou le type de déploiement des modules ThinApp octroyés au groupe. Sélectionnez **Automatique** pour que le module ThinApp s'affiche par défaut dans la zone Mes applications du portail de l'utilisateur. Sélectionnez **Activé par l'utilisateur** pour permettre aux utilisateurs d'ajouter manuellement le module ThinApp du catalogue des applications dans leur zone Mes applications. ■ Pour les applications publiées Citrix, vous pouvez afficher les droits existants du groupe sur les applications Citrix qui sont intégrées dans votre système Workspace. Les droits sur les applications Citrix sont configurés dans les déploiements Citrix qui sont intégrés dans votre système Workspace. Vous ne pouvez pas modifier les droits sur les applications Citrix à l'aide de la page Droits du groupe. ■ Certains types de ressources disposent d'un bouton **Retirer les droits** ; vous pouvez cliquer dessus pour retirer au groupe l'accès à cette ressource. **Remarque** La colonne État de provisionnement n'est pas utilisée. Par défaut, sur cette page, les colonnes État de provisionnement des lignes de la table contenant des entrées pré-renseignées indiquent Non activé, et vous ne pouvez pas modifier cette valeur.
Utilisateurs dans ce groupe	La page d'appartenance du groupe s'affiche. Dans cette page, vous pouvez : ■ Voir la liste des utilisateurs qui appartiennent au groupe. ■ Cliquer sur le nom d'un utilisateur pour afficher la page de détails de cet utilisateur.

Option	Description
	■ Cliquez sur **Modifier les utilisateurs dans ce groupe** pour afficher et configurer les règles qui définissent l'appartenance au groupe Workspace. L'option **Modifier les utilisateurs dans ce groupe** est disponible pour les groupes Workspace, mais pas pour les groupes du serveur de dossiers.

Gérer les utilisateurs d' Workspace

Vous pouvez gérer les utilisateurs importés à partir d'Active Directory, à l'aide de Console d'administration Workspace.

La gestion des utilisateurs dans Workspace comprend des tâches telles que l'attribution d'utilisateurs aux ressources, l'ajout d'utilisateurs aux groupes Workspace et la gestion de l'état des espaces de travail provisionnés aux utilisateurs.

Informations relatives aux utilisateurs de Workspace

Vous pouvez afficher des informations détaillées sur un utilisateur, telles que les ressources octroyées à un utilisateur, ses affiliations à des groupes et ses systèmes de postes de travail et périphériques mobiles provisionnés, à l'aide de Console d'administration Workspace.

Les attributs utilisateurs font partie des informations sur l'utilisateur que vous pouvez consulter, telles que l'attribut nom d'hôte du nœud de données ainsi que des attributs supplémentaires que la configuration d'Workspace permet de retrouver depuis votre serveur de dossiers pendant les synchronisations. L'utilité de la consultation des attributs supplémentaires du serveur de dossiers pour un utilisateur individuel dépend de votre façon d'utiliser ces attributs dans votre déploiement. Vous pouvez utiliser ces attributs supplémentaires des façons suivantes :

- Pour modifier l'appartenance à un groupe Workspace. Par exemple, si vous utilisez l'attribut de gestion dans Active Directory, vous pouvez mapper cet attribut dans Workspace. Vous pouvez créer un groupe dans lequel les règles du groupe restreignent l'appartenance aux utilisateurs disposant de l'attribut de gestion dans leur enregistrement utilisateur Workspace.
- Permettre aux utilisateurs d'accéder aux applications Web exigeant des attributs spécifiques. Par exemple, une application financière peut restreindre son accès aux utilisateurs disposant de l'attribut d'identifiant d'employé dans leur enregistrement d'utilisateur Workspace.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Utilisateurs et groupes > Utilisateurs**.

La page affiche une liste de tous vos utilisateurs Workspace.

3 Cliquez sur le nom d'un utilisateur.

La page des détails de l'utilisateur s'affiche. Le nom de l'utilisateur, son adresse e-mail et son rôle sont indiqués en haut de la page.

4 (Facultatif) Cliquez sur le nom du rôle affiché, **Utilisateur** ou **Administrateur**, pour changer le rôle de l'utilisateur.

Vous pouvez promouvoir des utilisateurs au rôle d'administrateur, leur permettant ainsi d'accéder à Workspace console d'administration. Les personnes auxquelles a été assigné le rôle d'administrateur peuvent encore accéder à leur portail d'applications à partir du Web en tant qu'utilisateur. L'URL d'accès à console d'administration est différente de celle servant à accéder au portail des applications.

Pour les URL suivantes, remplacez l'espace réservé *WorkspaceFQDN* par la valeur réelle.

Interface Web	Rôle requis	Exemple d'URL
Console d'administration Workspace	administrateur	https://*WorkspaceFQDN*/admin
Portail des applications Workspace	Utilisateur	https://*WorkspaceFQDN*/web

5 (Facultatif) Cliquez sur **Afficher les attributs supplémentaires** pour voir les attributs supplémentaires assignés à l'utilisateur, tels que les attributs du serveur de dossiers.

6 Cliquez sur l'onglet qui correspond aux informations que vous voulez voir.

Option	Description
Droits	La page Droits de l'utilisateur est affichée. Dans cette page, vous pouvez : ■ Voir la liste des ressources attribuées à l'utilisateur. ■ Cliquez sur **Ajouter un droit** pour attribuer à l'utilisateur les ressources disponibles dans votre catalogue. ■ Cliquez sur le nom d'une ressource attribuée listée pour afficher la page Modifier de cette ressource. ■ Pour les types de ressources disposant d'un bouton **Modifier**, vous pouvez cliquer sur ce bouton pour attribuer les ressources de ce type aux utilisateurs du groupe, pour annuler cette attribution ou pour personnaliser les options de chaque ressource attribuée. Dans la page Droits, vous pouvez apporter les modifications suivantes : ■ Pour les applications Web, cliquez sur **Modifier** pour changer les droits de l'utilisateur sur les applications Web ou le type de déploiement pour chacune des applications Web attribuées. Sélectionnez **Automatique** pour que l'application Web s'affiche par défaut dans le portail de l'utilisateur. Sélectionnez **Activé par l'utilisateur** pour permettre à l'utilisateur d'ajouter l'application Web à sa zone Mes applications à partir de la collection d'applications du Centre des applications à laquelle il a accès. ■ Pour les pools de postes de travail et d'applications View, vous pouvez afficher les droits d'accès existants de l'utilisateur aux pools View intégrés à votre système Workspace. Les droits d'accès aux pools de postes de travail et d'applications View sont configurés dans les instances de Serveur de connexion View intégrées à votre système Workspace. Vous ne pouvez pas modifier les droits l'accès aux pools View à l'aide de la page Droits d'accès de l'utilisateur. ■ Pour les modules ThinApp, cliquez sur **Modifier** pour modifier les droits de l'utilisateur sur les modules ThinApp ou le type de déploiement des modules ThinApp octroyés à l'utilisateur. Sélectionnez **Automatique** pour que le module ThinApp s'affiche par défaut dans la zone Mes applications du portail de l'utilisateur. Sélectionnez **Activé par l'utilisateur** pour permettre à l'utilisateur d'ajouter manuellement le module ThinApp du catalogue des applications dans la zone Mes applications. ■ Pour les applications publiées Citrix, vous pouvez afficher les droits existants de l'utilisateur sur les applications Citrix qui sont intégrées dans votre système Workspace. Les droits sur les applications Citrix sont configurés dans les déploiements Citrix qui sont intégrés dans votre système Workspace. Vous ne pouvez pas modifier les droits sur les applications Citrix à l'aide de la page Droits de l'utilisateur. ■ Certains types de ressources disposent d'un bouton **Retirer les droits** ; vous pouvez cliquer dessus pour retirer à l'utilisateur l'accès à cette ressource. **Remarque** La colonne État de provisionnement n'est pas utilisée. Par défaut, sur cette page, les colonnes État de provisionnement des lignes de la table contenant des entrées pré-renseignées indiquent Non activé, et vous ne pouvez pas modifier cette valeur.
Affiliations du groupe	Une liste des groupes auxquels l'utilisateur appartient s'affiche. Chaque nom de groupe représente un groupe dont l'utilisateur est membre. Vous pouvez cliquer sur le nom d'un groupe pour afficher la page des détails de ce groupe.
Espaces de travail	La page Espaces de travail de l'utilisateur s'affiche. Sur cette page, vous pouvez voir l'espace de travail de poste de travail qui a été provisionné sur les systèmes de postes de travail des utilisateurs, et notamment son état actuel.

Option	Description
	■ Pour un système de poste de travail, cliquez sur **Supprimer** pour supprimer le système correspondant d'Workspace. Vous pouvez ainsi supprimer un système d'Workspace s'il est perdu, volé ou n'est plus utilisé.

Modification de l'utilisateur et des groupes qui se synchronisent à partir d'Active Directory

Pendant la configuration de Workspace, vous avez entré les informations de connexion au serveur Active Directory, sélectionné les attributs et les filtres d'utilisateur Active Directory pour spécifier les utilisateurs qui se synchronisent dans le répertoire Workspace, et sélectionné les groupes Active Directory à ajouter. Vous pouvez modifier ces paramètres à partir de Administrateur de Connector Services, pages Synchronisation de l'annuaire.

Les modifications qui sont apportées et enregistrées dans ces pages sont automatiquement actualisées dans Workspace après la synchronisation d'annuaire suivante. Voir « Modifier les paramètres qui sélectionnent les utilisateurs pour Workspace », page 42

Modification de la page Mapper les attributs utilisateur

La page Mapper les attributs utilisateur affiche le mappage entre les attributs dans Active Directory et les attributs dans Workspace. Si vous souhaitez inclure des informations supplémentaires à partir d'Active Directory sur les utilisateurs, vous pouvez ajouter des attributs utilisateur dans la page Mapper les attributs utilisateur.

L'un des attributs d'utilisateur par défaut mappés dans la page Mapper les attributs utilisateur est l'attribut de désactivation d'un compte. L'attribut UserAccountControl est mappé à l'attribut Workspace désactivé. Les utilisateurs sont désactivés dans le répertoire Workspace lorsque l'attribut UserAccountControl d'Active Directory est signalé d'un indicateur UF_Account_Disable.

Lorsqu'un compte est désactivé, les utilisateurs ne peuvent pas se connecter pour accéder à leurs applications et à leurs ressources. Comme les ressources qui ont été attribuées aux utilisateurs ne sont pas supprimées du compte, lorsque l'indicateur est supprimé du compte, les utilisateurs peuvent se connecter et accéder aux ressources qui leur sont octroyées

Modifier les paramètres qui sélectionnent les utilisateurs pour Workspace

Pendant la configuration d'Workspace, vous spécifiez Active Directory, les attributs utilisateur et des filtres pour sélectionner les utilisateurs Active Directory que vous souhaitez employer avec Workspace. Vous pouvez mettre à jour ces paramètres dans les pages Administrateur de Connector Services.

Prérequis

Vérifiez que vous disposez des informations relatives aux modifications que vous souhaitez apporter, par exemple la nouvelle ND de base, les attributs utilisateur à inclure, les groupes à inclure.

Procédure

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

2 Prenez les mesures qui s'imposent.

Option	Action
Changez les informations du serveur Active Directory, par exemple l'hôte du serveur, le port, la ND de base, la ND Bind, le mot de passe Bind, etc.	a Cliquez sur **Annuaire**. b Apportez vos modifications. c Cliquez sur **Enregistrer**.
Changez le mappage des attributs utilisateur d'Workspace aux attributs utilisateur d'Active Directory.	a Cliquez sur **Mapper les attributs utilisateur**. b Apportez vos modifications. c Cliquez sur **Enregistrer**.
Créez des filtres pour exclure un utilisateur Active Directory spécifique se synchronisant à Workspace et mettez à jour les groupes Active Directory qui sont synchronisés avecWorkspace.	a Cliquez sur **Synchronisation de l'annuaire**. b Cliquez sur **Modifier les règles de synchronisation de l'annuaire**. c Apportez les modifications nécessaires dans la page Sélection des utilisateurs, puis cliquez sur **Enregistrer**. d Apportez les modifications nécessaires dans la page Sélection des groupes, puis cliquez sur **Enregistrer**. e Cliquez sur **Transfert vers Workspace**. f Cliquez sur **Enregistrer et continuer**.

Gestion du catalogue Workspace 7

Votre catalogue Workspace est le référentiel de toutes les ressources que vous pouvez attribuer aux utilisateurs. La disponibilité des types de ressources particuliers dans votre catalogue est déterminée en fonction des modules qui sont activés dans Workspace.

Pour afficher votre catalogue, cliquez sur l'onglet **Catalogue** dans le Workspace console d'administration. Sur la page Catalogue, vous pouvez effectuer les tâches suivantes :

- Ajouter de nouvelles ressources à votre catalogue.
- Visualiser les ressources auxquelles vous pouvez actuellement attribuer des utilisateurs.
- Accéder aux informations sur chaque ressource de votre catalogue.

En fonction de leur type, certaines ressources peuvent être ajoutées directement à votre catalogue à l'aide de la page Catalogue. D'autres types de ressources nécessitent une action de votre part en dehors de console d'administration. Pour plus d'informations sur la configuration des ressources, reportez-vous à *Configuration des ressources dans le Guide de VMware Workspace Portal* .

Ressource	Comment voir la ressource dans votre catalogue
Application Web	Activez le module Applications Web. Utilisez le console d'administration pour sélectionner le type d'application **Applications Web** sur la page Catalogue.
Application Windows virtualisée capturée en tant que module ThinApp	Synchronisez les packages ThinApp avec votre catalogue à partir de Administrateur de Connector Services, page Applications packagées - ThinApp. Utilisez le console d'administration, pour sélectionner le type d'application **Modules ThinApp** sur la page Catalogue.
Pool de postes de travail View	Synchronisez les pools View avec votre catalogue à partir de Administrateur de Connector Services, page Pools View. Utilisez le console d'administration pour sélectionner le type d'application **Pools de postes de travail View** sur la page Catalogue.
Applications hébergées View	Synchronisez les applications View hébergées avec votre catalogue à partir de Administrateur de Connector Services, page Pools View. Utilisez le console d'administration pour sélectionner le type d'application **Application hébergée View** comme type d'application sur la page Catalogue.
Application Citrix	Synchronisez les applications Citrix avec votre catalogue à partir de Administrateur de Connector Services, page Applications packagées - Citrix. Utilisez le console d'administration pour sélectionner le type d'application **Applications publiées Citrix** sur la page Catalogue.

Ce chapitre aborde les rubriques suivantes :

Aperçu des types de ressources d' Workspace

Les types de ressources que vous pouvez définir dans votre catalogue pour l'octroi et la distribution à des utilisateurs sont des applications Web, des applications Windows capturées sous forme de modules VMware ThinApp, des applications Citrix, des pools de postes de travail VMware View et des applications hébergées View.

Avant de pouvoir attribuer une ressource particulière à vos utilisateurs, vous devez doter votre catalogue de cette ressource. La méthode utilisée pour doter votre catalogue d'une ressource dépend du type de cette ressource.

Pour obtenir plus d'informations et connaître les exigences, l'installation et la configuration de ces ressources, reportez-vous à *Configuration des ressources dans le Guide de VMware Workspace Portal* .

Applications web

Vous pouvez doter votre catalogue d'applications Web directement sur la page Catalogue d'Workspace console d'administration. Lorsque vous cliquez sur une application Web affichée sur la page Catalogue, les informations sur cette application s'affichent. Depuis la page qui s'affiche, vous pouvez configurer l'application Web, par exemple fournir les attributs SAML appropriés pour configurer une connexion Single Sign-On entre Workspace et l'application Web ciblée. Lorsque l'application Web est configurée, vous pouvez alors lui attribuer des utilisateurs et des groupes. Voir « Ajouter des ressources à votre catalogue », page 50.

Modules ThinApp

Pour doter le catalogue d'applications Windows capturées sous forme de modules ThinApp, procédez comme suit.

1 Si les modules ThinApp auxquels vous souhaitez donner accès aux utilisateurs n'existent pas déjà, créez des modules ThinApp compatibles avec Workspace. Voir la documentation de VMware ThinApp.

2 Créez un partage réseau et insérez-y les modules ThinApp compatibles.

3 Configurez Workspace afin de l'intégrer aux modules sur le partage réseau.

Une fois ces tâches effectuées, les applications Windows virtualisées, les modules ThinApp que vous avez ajoutés au partage réseau, sont maintenant disponibles en tant que ressources dans votre catalogue. Vous pouvez alors attribuer des utilisateurs à ces ressources.

Pour lancer et exécuter les modules ThinApp distribués et gérés par Workspace, Workspace pour Windows doit être installé sur le système Windows des utilisateurs.

Applications publiées Citrix

Pour insérer des applications Citrix à votre catalogue, procédez comme suit.

1 Si ce n'est pas déjà fait, déployez des serveurs Citrix, ce qui implique l'octroi d'applications Citrix aux utilisateurs. Reportez-vous à la documentation Citrix appropriée.

2 Intégrez votre déploiement d'Workspace aux serveurs Citrix.

Une fois ces tâches effectuées, les applications Citrix que vous octroyez à des utilisateurs avec des serveurs Citrix sont maintenant disponibles en tant que ressources dans votre catalogue.

Pools de postes de travail View

Pour doter votre catalogue de pools de postes de travail View et des postes de travail View correspondants, procédez comme suit.

1 Si ce n'est pas déjà fait, déployez des pools de postes de travail View dans VMware View, ce qui inclut l'octroi de postes de travail à des utilisateurs. Voir la documentation de VMware View.

2 Intégrez votre déploiement d'Workspace dans VMware View.

Une fois ces tâches effectuées, les postes de travail View que vous avez octroyés à des utilisateurs avec VMware View sont maintenant disponibles en tant que ressources dans votre catalogue.

Application hébergées View

Pour insérer des pools d'applications View dans votre catalogue, procédez comme suit.

1 Vérifiez que les pools d'applications sont déployés dans View en tant que service Bureau à distance. Voir la documentation de View.

2 Intégrez votre déploiement d'Workspace à View.

Une fois ces tâches effectuées, les pools d'applications hébergées que vous avez octroyés à des utilisateurs avec View sont maintenant disponibles en tant que ressources dans votre catalogue.

Aperçu de l'utilisation des catégories de ressources

Par défaut, la recherche de ressources de catalogue s'effectue par type de ressource. Vous pouvez également effectuer une recherche par catégorie.

Pour permettre une recherche de ressources de catalogue Workspace par catégorie, créez des catégories et appliquez-les aux ressources

Créer une catégorie de ressources

Vous pouvez créer une catégorie de ressources Workspace sans l'appliquer immédiatement, ou vous pouvez la créer et l'appliquer simultanément.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur l'onglet **Catalogue**.

3 Cliquez sur la case à cocher d'une ou de plusieurs ressources.

Dès qu'une ressource est cochée, le bouton **Appliquer les catégories** s'active, condition préalable à la création d'une catégorie. Pour simultanément créer et appliquer des catégories, cliquez sur les cases à cocher de toutes les ressources auxquelles vous souhaitez appliquer la nouvelle catégorie. Si vous souhaitez créer une catégorie sans l'appliquer immédiatement, la ressource sélectionnée n'est pas significative. Dans ce cas, vous pouvez cliquer sur la case à cocher de n'importe quelle ressource du catalogue.

4 Cliquez sur **Appliquer les catégories**.

5 Tapez le nom d'une nouvelle catégorie dans la zone de texte **Rechercher des catégories**.

6 Cliquez sur **Ajouter une catégorie...**.

Workspace crée la nouvelle catégorie, mais ne l'applique pas.

7 (Facultatif) Pour appliquer la catégorie aux ressources sélectionnées, cliquez sur la case à cocher du nom de la nouvelle catégorie.

Workspace applique la catégorie aux ressources sélectionnées.

Suivant

Le cas échéant, appliquez la catégorie à des ressources. Voir « Appliquer une catégorie à des ressources », page 48.

Appliquer une catégorie à des ressources

Une fois que vous avez créé une catégorie, vous pouvez l'appliquer à toute ressource du catalogue

Prérequis

Créez une catégorie de ressources.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur l'onglet **Catalogue**.

3 Cliquez sur les cases à cocher de toutes les ressources auxquelles vous souhaitez appliquer la catégorie.

4 Cliquez sur **Appliquer les catégories** et sélectionnez le nom de la catégorie à appliquer.

La catégorie est appliquée aux ressources sélectionnées.

Retirer ou supprimer une catégorie

Vous pouvez dissocier une catégorie d'une ressource et retirer de façon permanente une catégorie du catalogue.

Vous pouvez retirer l'étiquette de la catégorie pour dissocier cette dernière de la ressource. Vous pouvez également supprimer la catégorie du catalogue de façon permanente. Lorsque vous supprimez une catégorie de façon permanente, celle-ci ne figure plus au catalogue. Elle ne figure plus dans le menu déroulant **Toute catégorie** ou sous la forme d'une étiquette dans toute ressource à laquelle vous l'aviez précédemment appliquée.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur l'onglet **Catalogue**.

3 Cliquez sur la case à cocher d'une ou de plusieurs ressources.

Dès qu'une ressource est cochée, le bouton **Appliquer les catégories** s'active, condition préalable au retrait et à la suppression d'une catégorie. Pour retirer une étiquette de catégorie d'une ou de plusieurs ressources, cliquez sur les cases à cocher de toutes les ressources desquelles vous souhaitez retirer l'étiquette de catégorie. Si vous souhaitez supprimer de façon permanente une catégorie, la ressource sélectionnée n'est pas significative. Dans ce cas, vous pouvez cliquer sur la case à cocher de n'importe quelle ressource du catalogue.

4 Cliquez sur **Appliquer les catégories**.

Option	Description
Retirer une catégorie des ressources	La case à cocher de l'étiquette est sélectionnée. Cliquez sur cette case à cocher pour retirer l'étiquette de la catégorie de la ressource sélectionnée.
Supprimer une catégorie de façon permanente	Placez le pointeur au-dessus de la catégorie. Un x s'affiche. Cliquez sur le x pour supprimer de façon permanente la catégorie du catalogue.

Accéder aux ressources de Workspace

Accédez à votre catalogue pour afficher les informations sur les ressources que vous pouvez octroyer aux utilisateurs, telles que les applications Web Workspace, les modules ThinApp, les applications Citrix et les pools de postes de travail View. Vous pouvez afficher les ressources par type ou par catégorie d'applications.

Prérequis

- Activez les modules de ressources qui correspondent aux types de ressources auxquelles vous voulez attribuer des utilisateurs. Les modules Applications Web, Gestion mobile, View, Modules ThinApp et Applications publiées Citrix sont disponibles.
- Ajoutez des ressources au catalogue pour répondre aux besoins de votre entreprise. Voir Chapitre 7, « Gestion du catalogue Workspace », page 45.
- Pour afficher les ressources par catégorie, créez et appliquez des catégories. Voir « Aperçu de l'utilisation des catégories de ressources », page 47.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur l'onglet **Catalogue**.

Workspace répertorie toutes les ressources dans le catalogue.

3 (Facultatif) Pour changer la méthode de tri, cliquez sur **Application** ou **Type d'applications**.

4 (Facultatif) Pour afficher les ressources d'un type spécifique, sélectionnez un type de ressources dans le menu déroulant **Tous les types d'applications**.

Les types d'applications que vous n'avez pas ajoutés à Workspace ne figurent pas dans le menu déroulant.

Option	Description
Tous les types d'applications	Affiche toutes les ressources dans votre catalogue.
Applications web	Affiche uniquement les applications Web dans votre catalogue. Les applications Web comprennent les applications SaaS et les applications Web gérées de façon interne par votre entreprise.
Modules ThinApp	Affiche uniquement les applications Windows capturées en tant que modules ThinApp. Des modules ThinApp apparaissent dans votre catalogue si vous les ajoutez à votre déploiement pendant la configuration d'Workspace avant d'accéder à console d'administration.
Pools de postes de travail View	Répertorie uniquement les pools de postes de travail View. Les pools de postes de travail View apparaissent dans votre catalogue si vous intégrez Workspace dans VMware View avant d'accéder à Console d'administration Workspace.
Applications hébergées View	Répertorie uniquement les applications hébergées. Les applications hébergées View s'affichent dans votre catalogue si vous intégrez Workspace à View avant d'accéder à console d'administration.
Applications publiées Citrix	Répertorie uniquement les applications Citrix. Les applications Citrix figurent dans votre catalogue si vous intégrez Workspace dans votre déploiement Citrix avant d'accéder à console d'administration.

5 (Facultatif) Pour afficher les ressources d'une catégorie spécifique, sélectionnez un ou plusieurs noms de catégorie dans le menu déroulant **Toute catégorie**.

Workspace répertorie toutes les ressources répondant aux critères sélectionnés.

- Si vous sélectionnez une catégorie, Workspace répertorie toutes les ressources comportant cette étiquette de catégorie.
- Si vous sélectionnez plusieurs catégories, Workspace répertorie uniquement les ressources comportant ces étiquettes de catégorie.

6 Cliquez sur l'icône d'une ressource spécifique pour en afficher les détails.

Ajouter des ressources à votre catalogue

Vous pouvez directement ajouter des applications Web dans votre catalogue à l'aide de la page Catalogue de Workspace console d'administration.

Reportez-vous à la section Configuration des ressources dans le Guide de VMware Workspace Portal, chapitre Fourniture d'un accès aux applications Web, pour obtenir des instructions détaillées sur l'ajout d'une application Web à votre catalogue.

Les instructions suivantes fournissent un aperçu des étapes impliquées dans l'ajout de ces types de ressources à votre catalogue.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Cliquez sur l'onglet **Catalogue**.

3 Cliquez sur **+ Ajouter une application**.

4 Cliquez sur une option en fonction du type de ressource et de l'emplacement de l'application. Lorsque vous importez l'image d'un espace de travail Android, vous n'avez à cliquer sur aucune option à cette étape.

Nom du lien	Type de ressource	Description
Applications Web ...du catalogue d'applications Cloud	Application Web	Workspace inclut l'accès à plusieurs applications Web par défaut, disponibles dans le catalogue d'applications Cloud et que vous pouvez ajouter à votre catalogue en tant que ressources.
Application Web ... créer un nouvel enregistrement	Application Web	En renseignant le formulaire approprié, vous pouvez créer un enregistrement d'application pour les applications Web que vous voulez ajouter à votre catalogue en tant que ressources.
Application Web ... importer un fichier ZIP ou JAR	Application Web	Vous pouvez importer une application Web précédemment configurée dans Workspace. Vous pouvez utiliser cette méthode pour effectuer un déploiement d'Workspace depuis l'environnement de test jusqu'à la production. Dans une telle situation, vous pouvez exporter une application Web depuis le déploiement de l'environnement de test sous forme de fichier ZIP. Vous pouvez ensuite importer le fichier ZIP dans le déploiement de production.

5 Suivez les invites à l'écran pour finir l'ajout des ressources au catalogue.

Rechercher des utilisateurs, des groupes ou des ressources de catalogue

8

Utilisez la zone de texte de recherche de Console d'administration Workspace pour rechercher des utilisateurs, des groupes ou des ressources d'Workspace dans votre catalogue.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Entrez une chaîne dans la zone de texte de recherche.

Par exemple, pour rechercher tous les utilisateurs ayant une adresse e-mail monentreprise.com, entrez `monentreprise.com`.

La page Résultats de recherche affiche les résultats renvoyés dans trois onglets, conformément aux règles suivantes.

Onglet Utilisateurs	La chaîne saisie correspond aux premiers caractères de tout mot inclus dans le prénom, le nom ou le nom d'utilisateur principal de l'utilisateur d'Workspace.
Onglet Groupes	La chaîne saisie correspond aux premiers caractères de tout mot inclus dans le nom ou la description du groupe.
Onglet Catalogue	La chaîne saisie correspond aux premiers caractères de tout mot inclus dans le nom ou la description de la ressource du catalogue.

Remarque Jusqu'à 100 résultats sont renvoyés pour chaque type d'enregistrement. Par exemple, si la chaîne apparaît dans les enregistrements de plus de 100 utilisateurs, un maximum de 100 résultats sont répertoriés dans l'onglet **Utilisateurs**. Vous ne pouvez pas modifier cette valeur maximale.

Visualisation des rapports d' Workspace 9

Workspace génère plusieurs rapports, par exemple à propos des utilisateurs, des ressources et des événements d'audit. Vous pouvez visualiser les rapports dans l'onglet **Rapports** de Console d'administration Workspace.

Vous pouvez utiliser Workspace pour générer plusieurs rapports.

Tableau 9-1. Types de rapports Workspace

Rapport Workspace	Description
Activité récente	Ce rapport répertorie les types d'action que l'utilisateur a exécutés dans Workspace le jour précédent, le mois précédent ou les 12 semaines précédentes. Vous pouvez cliquer sur **Afficher les événements** pour voir la date, l'heure et les détails de l'utilisateur correspondant à l'activité.
Utilisation des ressources	Ce rapport affiche toutes vos ressources avec des détails respectifs pour chaque ressource, tels que le nombre d'utilisateurs et de licences.
Droits des ressources	Ce rapport répertorie les droits des utilisateurs sur une ressource que vous spécifiez.
Appartenance à un groupe	Ce rapport affiche les membres d'un groupe que vous spécifiez.
Utilisateurs	Ce rapport affiche tous vos utilisateurs Workspace et fournit des détails sur chacun d'eux, tels que l'adresse e-mail, le rôle ou les affiliations de groupe de l'utilisateur.
Utilisateurs simultanés	Ce rapport indique le nombre de sessions utilisateur simultanément ouvertes.
Événements d'audit	Ce rapport affiche les événements d'audit relatifs à une recherche que vous spécifiez, telle que les connexions utilisateur pendant les 30 derniers jours. Cette fonctionnalité est utile dans le cadre de la résolution de problèmes. Voir « Générer un rapport d'événement audité », page 53.

Générer un rapport d'événement audité

Vous pouvez générer un rapport des événements audités que vous spécifiez.

Les rapports d'événements audités peuvent être utiles en tant que méthode de résolution de problèmes.

Prérequis

Activer l'audit. Voir « Aperçu des paramètres d'administration d'Workspace », page 55.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Rapports > Événements audités**

3 Sélectionnez les critères d'événement audité.

Critères d'événement audité	Description
Utilisateur	Ce champ texte vous permet de réduire la recherche des événements audités à ceux générés par un utilisateur spécifique.
Type	Cette liste déroulante vous permet de réduire la recherche des événements audités à un type d'événement audité spécifique. La liste déroulante n'affiche pas tous les types d'événements audités potentiels. La liste n'affiche que les types d'événements qui se sont produits dans votre déploiement d'Workspace. Les types d'événements audités qui sont affichés en majuscules sont des événements d'accès, tels que CONNEXION et LANCEMENT, qui ne génèrent pas de modification dans la base de données. Les autres types d'événements audités génèrent des modifications dans la base de données.
Action	Cette liste déroulante vous permet de réduire votre recherche à des actions spécifiques. La liste affiche des événements qui produisent des modifications spécifiques dans la base de données. Si vous sélectionnez un événement d'accès dans la liste déroulante Type, ce qui signifie un événement de non-action, ne spécifiez pas d'action dans la liste déroulante Action.
Objet	Ce champ texte vous permet de réduire la recherche à un objet spécifique. Des exemples d'objets sont les groupes, les utilisateurs et les périphériques. Les objets sont identifiés par un nom ou un numéro d'identification.
Plage de dates	Ces champs texte vous permettent de réduire votre recherche à une plage de dates au format « De ___ à ___ jours auparavant ». La plage de date maximale est de 30 jours. Par exemple, la plage « De 90 à 60 jours auparavant » est valide tandis que la plage « De 90 à 45 jours auparavant » ne l'est pas, car elle dépasse la période maximale de 30 jours.

4 Cliquez sur **Afficher**.

Un rapport d'événement audité apparaît conformément aux critères que vous avez spécifiés.

Remarque Occasionnellement, lors du redémarrage du sous-système d'audit, la page Auditer les événements risque d'afficher un message d'erreur et de ne pas afficher le rapport. Si vous voyez un tel message d'erreur concernant le non-affichage du rapport, attendez quelques minutes, puis recommencez.

5 Pour plus d'informations sur un événement audité, cliquez sur **Afficher les détails** pour cet événement.

Configuration des paramètres d' Workspace pour les administrateurs 10

Après avoir installé Workspace et effectué la configuration initiale, vous pouvez configurer plusieurs paramètres d'administration.

Ce chapitre aborde les rubriques suivantes :

Aperçu des paramètres d'administration d' Workspace

Vous pouvez configurer plusieurs paramètres d'administration d'Workspace.

Vous accédez aux paramètres d'administration à l'aide de Console d'administration Workspace.

Paramètre	Description
Configuration VA	Sélectionnez **Paramètres > Configuration VA** pour accéder aux pages Appliance Configurator Ces pages vous permettent de mettre à jour et de modifier la base de données Workspace, les certificats SSL et le serveur syslog externe, de modifier les mots de passe Workspace et système, et d'afficher les fichiers journaux.
Licence	Sélectionnez **Paramètres > Licence** pour entrer votre clé de licence Workspace.
SMTP	Sélectionnez **Paramètres > SMTP** pour entrer les paramètres SMTP.
Récupération du mot de passe	Sélectionnez **Paramètres > Récupération du mot de passe** pour configurer le comportement du lien Mot de passe oublié qui s'affiche sur la page de connexion de l'utilisateur lorsque l'utilisateur clique sur Mot de passe oublié.
Magasins d'utilisateurs	Sélectionnez **Paramètres > Magasins d'utilisateurs** pour configurer les magasins d'utilisateurs pour des déploiements Active Directory à forêts multiples sans relations d'approbation. Reportez-vous au guide *Installation et configuration d' Workspace*, Gestion des connexions Active Directory, chapitre Workspace.
Plages réseau	Sélectionnez **Paramètres > Plages réseau** pour configurer les plages réseau de votre organisation de sorte à pouvoir associer des plages d'adresses IP à des instances de fournisseurs d'identité. Voir « Ajout ou modification d'une plage réseau », page 17.
Méthodes d'authentification	Sélectionnez **Paramètres > Méthodes d'authentification** pour configurer les méthodes d'authentification par défaut ou pour ajouter des méthodes d'authentification non directement prises en charge par Workspace, mais prises en charge indirectement par le biais de fournisseurs d'identité tiers. Voir « Ajouter ou modifier une méthode d'authentification d'utilisateur », page 18.

Paramètre	Description
Fournisseurs d'identité	Sélectionnez **Paramètres > Fournisseurs d'identité** pour modifier une instance de fournisseur d'identité ou pour en ajouter une. L'installation initiale de Workspace inclut un déploiement de fournisseur d'identité par défaut. Modifiez la configuration du fournisseur d'identité par défaut pour sélectionner des méthodes d'authentification et ajouter des plages d'adresses réseau. Ajoutez des instances de fournisseur d'identité supplémentaires à votre déploiement d'Workspace à des fins de haute disponibilité. Lorsque la page Fournisseurs d'identité répertorie plusieurs instances de fournisseur d'identité, vous pouvez modifier l'ordre des instances. L'ordre est important lorsque des adresses IP sont attribuées à plusieurs instances de fournisseur d'identité. Pour obtenir des détails sur l'ajout ou la modification d'instances de fournisseur d'identité et sur la modification de l'ordre de ces instances, reportez-vous à « Ajouter et configurer une instance de fournisseur d'identité », page 20.
Accès à distance à l'application	Sélectionnez **Paramètres > Accès aux applications distantes** pour créer des clients ou des modèles qui permettent aux applications de s'enregistrer auprès d'Workspace.
Certificat SAML	Sélectionnez **Paramètres > Certificat SAML** pour voir le certificat à signature SAML. Si une application Web nécessite l'utilisation d'assertions SAML pour authentifier les utilisateurs, Workspace et l'application Web doivent disposer de copies locales du même certificat à signature SAML.
Approbations	Sélectionnez **Paramètres > Approbations** pour activer ou désactiver l'approbation de licences. L'activation de l'approbation des licences s'applique lorsque vous intégrez votre système de gestion des licences dans Workspace.
Audit	Sélectionnez **Paramètres > Audit** pour activer ou désactiver la collecte d'informations pour les rapports d'événements audités, qui sont accessibles dans l'onglet **Rapports**.
Application publiée Citrix	Sélectionnez **Paramètres > Application publiée Citrix** afin de modifier les paramètres globaux de livraison d'applications d'Workspace pour les applications Citrix disponibles dans le catalogue d'Workspace. Pour obtenir des instructions sur la modification des paramètres d'une seule application Citrix, reportez-vous à *Configuration des ressources dans le Guide de VMware Workspace Portal* .
Informations de marque personnalisées	Sélectionnez **Paramètres > Informations de marque personnalisées** pour personnaliser les informations de marque sur les interfaces d'Workspace. Voir « Personnaliser les informations de marque d'Workspace », page 56.

Personnaliser les informations de marque d' Workspace

Vous pouvez personnaliser les logos, les polices, les clips Web et l'arrière-plan qui s'affichent dans diverses interfaces, par exemple la Console d'administration Workspace, les écrans d'ouverture de session de l'utilisateur et de l'administrateur, la vue Web du portail des applications et la vue Web du portail des applications sur appareils mobiles.

Vous pouvez personnaliser les informations de marque utilisées dans la vue Web du portail des applications et dans la Console d'administration Workspace.

Procédure

1 Connectez-vous à Console d'administration Workspace.

2 Sélectionnez **Paramètres > Informations de marque personnalisées**.

3 Modifiez les paramètres du formulaire comme nécessaire.

Tableau 10-1. Configuration des informations de marque personnalisées

Élément de formulaire	Description
	Noms de marque et logos
Logo	L'option Logo vous permet de modifier le logo qui s'affiche dans le portail des applications de l'utilisateur et dans la console d'administration. La taille de page maximale recommandée pour le téléchargement est de 350 x 100 px. Si vous téléchargez des images supérieures à 350 x 100 px, elles sont redimensionnées à la taille 350 x 100 px. Le format peut être JPEG, PNG ou GIF. Cliquez sur **Modifier** pour télécharger une nouvelle image qui remplacera le logo actuel. Lorsque vous cliquez sur **Confirmer**, la modification s'applique immédiatement.
Icône Favorite	L'option Icône Favorite vous permet de modifier l'icône favorite utilisée dans les navigateurs Web. Cette option s'applique aux postes de travail et aux périphériques mobiles. La taille maximale de l'image d'icône favorite est de 16 x 16 pixels. Le format peut être JPEG, PNG, GIF ou ICO. Cliquez sur **Modifier** pour télécharger une nouvelle image qui remplacera l'icône favorite actuelle. Un message vous demande de confirmer la modification. Si vous cliquez sur **Confirmer**, la modification s'effectue immédiatement.
Nom de l'entreprise	L'option Nom de l'entreprise s'applique aux postes de travail et aux périphériques mobiles. Elle vous permet de modifier le nom de l'entreprise qui s'affiche avant le nom du produit dans le titre de l'écran du navigateur Web. Tapez un nom d'entreprise sur le nom existant pour le modifier.
Nom du produit	L'option Nom du produit s'applique aux postes de travail et aux périphériques mobiles. Elle vous permet de modifier le nom du produit qui s'affiche après le nom de l'entreprise dans le titre de l'écran du navigateur Web. Tapez un nom de produit sur le nom existant pour le modifier.
	Écran d'ouverture de session
Couleur d'arrière-plan	Couleur d'arrière-plan des écrans d'ouverture de session. Tapez un nouveau code couleur hexadécimal sur le code existant pour changer la couleur d'arrière-plan. Cochez **Mise en surbrillance de l'arrière-plan** pour accentuer la couleur de l'arrière-plan. Cochez **Modèle d'arrière-plan** pour définir le modèle de triangle préconçu dans la couleur d'arrière-plan.
Couleur du titre générique	Couleur de la zone de titre des écrans d'ouverture de session. Tapez un nouveau code de couleur hexadécimal sur le code existant pour modifier la couleur du titre générique. Cochez **Modèle du titre générique** pour définir le modèle de triangle préconçu dans la couleur du titre générique.
Image (en option)	Pour ajouter une image à l'arrière-plan plutôt qu'une couleur, téléchargez une image. La taille maximale de l'image est de 1 400 x 900 pixels. Le format peut être JPEG, PNG ou GIF.
Logo	Cliquez sur **Télécharger** pour télécharger un nouveau logo afin de remplacer le logo actuel dans les écrans d'ouverture de session. Lorsque vous cliquez sur **Confirmer**, la modification s'applique immédiatement. La taille de page maximale recommandée pour le téléchargement est de 350 x 100 px. Si vous téléchargez des images supérieures à 350 x 100 px, elles sont redimensionnées à la taille 350 x 100 px. Le format peut être JPEG, PNG ou GIF.
	Portail (vue Web)

Tableau 10-1. Configuration des informations de marque personnalisées (suite)

Élément de formulaire	Description
Couleur d'arrière-plan	Couleur d'arrière-plan de l'écran du portail Web. Tapez un nouveau code couleur hexadécimal sur le code existant pour changer la couleur d'arrière-plan. Pour montrer la couleur que prendra l'arrière-plan du portail des applications, celle-ci change dans l'aperçu du portail des applications lorsque vous tapez un nouveau code de couleur. Cependant, si la case **Inclure l'image d'arrière-plan** est cochée, la couleur d'arrière-plan ne sera peut-être pas visible dans l'aperçu. Cochez **Mise en surbrillance de l'arrière-plan** pour accentuer la couleur de l'arrière-plan. Cochez **Modèle d'arrière-plan** pour définir le modèle de triangle préconçu dans la couleur d'arrière-plan.
Nom et couleur des icônes	Couleur de la police utilisée pour les noms de ressources répertoriés dans l'écran du portail des applications. Le nom de la ressource se trouve directement sous l'icône de la ressource. Tapez un code de couleur hexadécimal sur le code existant pour modifier la couleur de la police. Lorsque vous tapez un nouveau code de couleur, le texte du nom de l'application change de couleur dans l'aperçu du portail des applications.
Effet de lettrage	Sélectionnez le type de lettrage à utiliser pour le texte dans l'écran Mes applications.
Image (en option)	Pour ajouter une image plutôt qu'une couleur à l'arrière-plan sur l'écran du portail des applications, téléchargez une image.
	Portail (vues Mobile et Tablette)
Couleur d'arrière-plan	Tapez un code de couleur hexadécimal sur le code existant pour modifier la couleur de l'arrière-plan de l'écran Mes applications visible sur un appareil mobile.
Couleur de la barre de titre	Tapez un code de couleur hexadécimal sur le code existant pour modifier la couleur de la barre de titre visible sur un appareil mobile. Sélectionnez **Modèle de la barre de titre** pour définir le modèle de triangle préconçu dans la couleur de la barre de titre.
Couleur du titre	Tapez un code de couleur hexadécimal sur le code existant pour modifier la couleur de la police utilisée dans le titre de la barre de titre.
Couleur du nom	Couleur de la police utilisée pour les noms de ressources répertoriés dans l'écran du portail des applications. Le nom de la ressource se trouve directement sous l'icône de la ressource. Tapez un code de couleur hexadécimal sur le code existant pour modifier la couleur de la police des noms des applications.
Effet de lettrage	Sélectionnez le type de lettrage à utiliser pour le texte dans l'écran Mes applications.
Utilisez les mêmes valeurs pour le Lanceur et le Catalogue	Si vous souhaitez utiliser la même conception d'informations de marque pour la vue de l'écran Centre d'applications que pour la vue de l'écran Mes applications sur les appareils mobiles, cochez cette case. Si vous souhaitez concevoir différemment l'écran Centre d'applications, laissez cette case non cochée et configurez l'arrière-plan, la couleur de la barre de titre et la couleur du titre de l'écran Centre d'applications.
	Visite de l'utilisateur débutant
Visite de l'utilisateur débutant	Lorsque les utilisateurs lancent le portail d'applications pour la première fois, un diaporama sur les fonctionnalités de Workspace leur est présenté. Vous pouvez supprimer la coche pour désactiver cette fonctionnalité.
	Périphériques mobiles

Tableau 10-1. Configuration des informations de marque personnalisées (suite)

Élément de formulaire	Description
Icône de clip Web	Icône Workspace, qui s'affiche lorsque les utilisateurs enregistrent l'URL du portail des applications comme signet de l'écran d'accueil de leur appareil mobile. Cette icône de clip Web lance le portail des applications de Workspace. La taille maximale de l'image est de 512 x 512 pixels. Le format peut être JPEG ou PNG. Cliquez sur **Modifier** pour télécharger une nouvelle image qui remplacera l'icône de clip Web actuelle. Un message vous demande de confirmer la modification. Si vous cliquez sur **Confirmer**, la modification s'effectue immédiatement.
Titre du clip Web	Le titre qui accompagne l'icône de clip Web d'Workspace. Le titre doit comporter moins de 20 caractères.

4 Cliquez sur **Enregistrer**.

Les mises à jour des informations de marque à Workspace sont appliquées dans un délai de cinq minutes après que vous avez cliqué sur Enregistrer.

Suivant

Vérifiez l'effet que produisent les modifications des informations de marque dans les diverses interfaces.

Index