Administratorhandbuch für VMware Workspace Portal

Workspace Portal 2.1

Dieses Dokument unterstützt die aufgeführten Produktversionen sowie alle folgenden Versionen, bis das Dokument durch eine neue Auflage ersetzt wird. Die neuesten Versionen dieses Dokuments finden Sie unter http://www.vmware.com/de/support/pubs.

DE-001537-00

vmware®

Die neueste technische Dokumentation finden Sie auf der VMware-Website unter:

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

Auf der VMware-Website finden Sie auch die aktuellen Produkt-Updates.

Falls Sie Anmerkungen zu dieser Dokumentation haben, senden Sie Ihre Kommentare und Vorschläge an:

docfeedback@vmware.com

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

VMware Global, Inc.
Zweigniederlassung Deutschland
Freisinger Str. 3
85716 Unterschleißheim/Lohhof
Germany
Tel.: +49 (0) 89 3706 17000
Fax: +49 (0) 89 3706 17333
www.vmware.com/de

Inhalt

1 Grundlegendes zum Administratorhandbuch für VMware Workspace Portal 5

2 Einführung in Workspace für Administratoren 7

3 Überwachen von Benutzern, Ressourcen und Appliance-Systemzustand mithilfe von Dashboards der Workspace-Verwaltungskonsole 11
- Verfolgen von Benutzern und in Workspace verwendeten Ressourcen 11
- Überwachen von Workspace -Systeminformationen und -Systemzustand 12

4 Konfigurieren der Workspace -Benutzerauthentifizierung 15
- Überblick über die Workspace -Benutzerauthentifizierung 15
- Hinzufügen oder Bearbeiten eines Netzwerkbereichs 17
- Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode 18
- Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz 20
- Überblick über das Konfigurieren von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz 22
  - Abrufen der zum Konfigurieren einer externen Identitätsanbieter-Instanz erforderlichen Workspace -SAML-Informationen 23
- Bearbeiten des Standardrichtliniensatzes für den Zugriff 24

5 Verwalten von Richtliniensätzen für den Zugriff 27
- Überblick über Einstellungen für Zugriffsrichtlinien 28
- Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen 29
- Bearbeiten eines Richtliniensatzes für den Zugriff 30
- Hinzufügen eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen 32
- Anwenden eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen 33

6 Verwalten von Benutzern und Gruppen 35
- Benutzer- und Gruppentypen von Workspace 35
- Verwalten von Workspace -Gruppen 36
  - Ändern der Workspace -Gruppenmitgliedschaft 36
  - Workspace-Gruppeninformationen 39
- Verwalten von Workspace -Benutzern 41
  - Workspace -Benutzerinformationen 41
- Ändern von Benutzern und Gruppen, die aus Active Directory synchronisieren 44
  - Ändern von Einstellungen, die Benutzer für Workspace auswählen 44

7 Verwalten des Workspace -Katalogs 47
- Übersicht über Workspace -Ressourcentypen 48
- Übersicht über die Verwendung von Ressourcenkategorien 49
  - Erstellen einer Ressourcenkategorie 49

Anwenden einer Kategorie auf Ressourcen 50
Entfernen oder Löschen einer Kategorie 50
Zugriff auf Workspace -Ressourcen 51
Hinzufügen von Ressourcen zu Ihrem Katalog 52

8 Suchen nach Benutzern, Gruppen oder Katalogressourcen 55

9 Anzeigen von Workspace -Berichten 57
Generieren eines Audit-Ereignisberichts 57

10 Konfigurieren der Workspace -Einstellungen für Administratoren 59
Übersicht über administrative Einstellungen in Workspace 59
Anpassen des Workspace -Brandings 60

Index 65

Grundlegendes zum Administratorhandbuch für VMware Workspace Portal

1

Das *Administratorhandbuch für VMware Workspace Portal* bietet Informationen und Anweisungen zur Verwendung und Verwaltung von VMware Workspace™ Portal. Mit Workspace können Sie einen Katalog mit Ressourcen für die Anwendungen Ihrer Organisation anpassen und den sicheren, vom Benutzer verwalteten Zugriff von mehreren Geräten aus auf diese Ressourcen ermöglichen. Solche Ressourcen können Web-Anwendungen, als ThinApp-Pakete erfasste Windows-Anwendungen, Citrix-basierte Anwendungen und View™-Desktop- und -Anwendungspools sein. Workspace bietet Benutzern eine einheitliche Umgebung und Ihrer IT-Abteilung geräteübergreifend eine einheitliche Sicherheit und Verwaltung für alle Dienste und Anwendungen.

Angesprochene Zielgruppe

Das Administratorhandbuch für *VMware Workspace Portal* ist für Enterprise-Administratoren bestimmt. Die Informationen sind für erfahrene Windows- oder Linux-Systemadministratoren bestimmt, die mit der VM-Technologie, dem Identitätsmanagement, Kerberos und den Verzeichnisdiensten vertraut sind. Kenntnisse anderer Technologien, wie z. B. VMware ThinApp, ®View, virtualisierte Citrix-Anwendungen, RSA SecurID, sind hilfreich, wenn Sie diese Funktionen implementieren möchten.

Administratorhandbuch für Workspace – Überblick

Verwenden Sie das Administratorhandbuch für *VMware Workspace Portal* nach dem Installieren von Workspace.

Zum Administrieren von Workspace verwenden Sie Workspace-Verwaltungskonsole.

Die Hauptaufgabe in Workspace-Verwaltungskonsole besteht darin, Benutzern den Zugriff auf Ressourcen zu ermöglichen. Andere Aufgaben unterstützen diese Hauptaufgabe, indem sie Ihnen mehr Kontrolle darüber bieten, welche Benutzer bzw. Gruppen unter welchen Bedingungen Berechtigungen für welche Ressourcen haben.

Die Aufgaben, die Sie als Administrator durchführen, variieren je nach den Ressourcentypen, die Sie zu verwalten beabsichtigen. Sie können View-Desktop- und -Anwendungspools, Windows-Anwendungen (ThinApp-Pakete), DaaS-Desktops, Citrix-basierte Anwendungen und Web-Anwendungen verwalten. Die tatsächlichen Ressourcentypen, die Sie verwalten, variieren je nach den Erfordernissen Ihrer Organisation. Um Berechtigungen für einen Ressourcentyp zu erteilen, müssen Sie zuerst die entsprechenden Aufgaben zur Vorabkonfiguration durchführen, die in der Dokumentation „Einrichten von Ressourcen in VMware Workspace Portal“ beschrieben sind.

Einführung in Workspace für Administratoren 2

Workspace stellt Ihnen eine zentralisierte Management-Konsole zur Verfügung, mit der Sie den Katalog Ihrer Organisation anpassen und Berechtigungen für Ressourcen in diesem Katalog verwalten können. Ihr Katalog enthält die Anwendungen und Ressourcen Ihrer Organisation.

Workspace erkennt Attribute von Benutzern und setzt Richtlinien anwendungsübergreifend durch. Der Arbeitsbereich eines Benutzers besteht aus ihrem Satz berechtigter Ressourcen. Für jeden Benutzer können Sie die Übermittlung von Windows-, Web- und Software-as-a-Service-Anwendungen (SaaS) so anpassen, dass der Zugriff auf diese Anwendungen von einem einzelnen Portal aus möglich ist, und Benutzern gleichzeitig Self-Service-Zugriff auf Anwendungen bieten.

Workspace -Verwaltungsdienste

Sie verwalten Workspace-Benutzergruppen und Ressourcen, die Authentifizierung, die Konfiguration der Synchronisierung und die Verbindungen zur Datenbank über verschiedene Verwaltungsdienste in Workspace.

- Über die Workspace-Verwaltungskonsole richten Sie den Ressourcenkatalog ein und verwalten Benutzer und Gruppen, Berechtigungen und die Berichterstellung. Sie können das Dashboard für Benutzerbindung und das Systemdiagnose-Dashboard anzeigen, um Benutzer, Ressourcennutzung und den Systemzustand der Workspace-Appliance zu überwachen. Sie melden sich mit der in Active Directory zugewiesenen Administrator-Benutzerrolle ein. Die URL für die direkte Anmeldung an der Verwaltungskonsole lautet „https://*WorkspaceFQDN*/SAAS/admin“.
- Auf den Connector Services-Administrator-Seiten konfigurieren Sie das Verzeichnis, richten Authentifizierungsbroker ein und verwalten andere integrierte Unternehmensressourcen wie virtuelle Desktops und Remote-Anwendungen. Dies umfasst das Einrichten der Integration in den View-Verbindungsserver, des ThinApp-Repositorys und der von Citrix veröffentlichte Anwendungen. Auf diesen Seiten sehen Sie auch den Status und die Alarme der Verzeichnissynchronisierung. Sie melden sich als Workspace-Administrator an und verwenden den Benutzernamen **`admin`** und das beim Einrichten von Workspace erstellte Administratorkennwort. Einen Link zu den Connector Services-Administrator-Seiten finden Sie unter „https://*Workspace_FQDN*.com:8443“.
- Sie können über die Appliance-Konfigurator-Seiten die Workspace-Datenbank verwalten, Zertifikate aktualisieren, Syslog aktivieren, die Kennwörter für Workspace und das System ändern sowie andere Infrastrukturfunktionen verwalten. Sie melden sich als Workspace-Administrator an und verwenden den Admin-Benutzernamen und das beim Einrichten von Workspace erstellte Admin-Kennwort. Einen Link zu den Appliance-Konfigurator-Seiten finden Sie unter „https://*Workspace_FQDN*.com:8443“. Sie können die Seiten von Appliance Configurator auch in der Workspace-Verwaltungskonsole über die Seite Einstellungen > VA-Konfiguration aufrufen.

Komponenten für Endbenutzer von Workspace

Benutzer haben über das Workspace App-Portal (einen Client ohne Agenten) Zugriff auf Ressourcen, für die sie Berechtigungen haben, und über Workspace für Windows Zugriff auf virtualisierte Windows-Anwendungen, die als ThinApp-Pakete erfasst wurden.

Tabelle 2-1. Workspace -Benutzer-Client-Komponenten

Workspace-Benutzerkomponente	Beschreibung	Verfügbare Endpunkte
Workspace App-Portal	Das App-Portal von Workspace ist eine webbasierte Anwendung ohne Agenten. Es ist die Standardschnittstelle, die verwendet wird, wenn Benutzer mit einem Browser auf die Objekte in ihrem berechtigten Arbeitsbereich zugreifen und diese verwenden. Mithilfe dieses Portals können Benutzer auf ihre View-Desktops und Workspace-Web-Anwendungen zugreifen. Wenn ein Endbenutzer in einem Windows-System, in dem das Workspace für Windows-Programm installiert und aktiv ist, über Berechtigungen für ThinApp-Anwendungen verfügt, kann er seine berechtigten ThinApp-Pakete von diesem App-Portal aus anzeigen und starten. Auf iOS-Geräten können Benutzer dieses Portal in einer Browser-App wie Safari öffnen, um auf ihre View-Desktops sowie Workspace-Web-Anwendungen und Citrix-basierten Anwendungen zuzugreifen und diese zu verwenden.	Das webbasierte App-Portal ist auf allen unterstützten Systemendpunkten verfügbar, z. B. auf Windows-Systemen, Mac-Systemen, iOS-Geräten und Android-Geräten.
Workspace für Windows	Wenn dieses Programm auf Windows-Systemen installiert ist, können die Benutzer mit ihren als ThinApp-Pakete erfassten virtualisierten Windows-Anwendungen arbeiten.	Windows-Systeme

Unterstützte Webbrowser für Workspace

Die Workspace-Administratorkonsole ist eine webbasierte Anwendung, die bei der Installation von Workspace ebenfalls installiert wird. Der Zugriff auf und die Verwendung von Workspace-Verwaltungskonsole ist über folgende Browser möglich:

- Internet Explorer 10 und 11 für Windows-Systeme
- Google Chrome 34.0 oder höher für Windows- und Mac-Systeme
- Mozilla Firefox 28 oder höher für Windows- und Mac-Systeme
- Safari 6.1.3 oder höher für Mac-Systeme

Endbenutzer können über folgende Browser auf ihr Workspace-App-Portal zugreifen:

- Mozilla Firefox (neueste Version)
- Google Chrome (neueste Version)
- Safari (neueste Version)
- Internet Explorer 8 oder höher
- Integrierter Browser und Google Chrome auf Android-Geräten
- Safari auf iOS-Geräten

Wenn Sie Workspace-Seiten mit Internet Explorer 8 anzeigen, werden möglicherweise nicht alle Elemente auf der Seite korrekt dargestellt. Um die beste Anzeigequalität zu erhalten, sollten Benutzer auf eine neuere Version aktualisieren.

Überwachen von Benutzern, Ressourcen und Appliance-Systemzustand mithilfe von Dashboards der Workspace-Verwaltungskonsole

3

Die Workspace-Verwaltungskonsole enthält ein Dashboard für Benutzerengagement und ein Systemdiagnose-Dashboard, mit denen Sie Benutzer, Ressourcennutzung und Systemzustand der Workspace-Appliance überwachen können.

Dieses Kapitel behandelt die folgenden Themen:

- „Verfolgen von Benutzern und in Workspace verwendeten Ressourcen“, auf Seite 11
- „Überwachen von Workspace-Systeminformationen und -Systemzustand“, auf Seite 12

Verfolgen von Benutzern und in Workspace verwendeten Ressourcen

Im Dashboard für Benutzerbindung werden Informationen über Benutzer und Ressourcen angezeigt. Dort wird angezeigt, wer sich angemeldet hat, welche Ressourcen verwendet werden und wie oft Zugriff auf die Anwendungen erfolgt. Sie können Berichte erstellen, um Benutzer- und Gruppenaktivitäten sowie die Ressourcennutzung zu verfolgen.

Die im Dashboard für Benutzerbindung angezeigte Zeit basiert auf der für den Browser eingestellten Zeitzone. Das Dashboard wird jede Minute aktualisiert.

Vorgehensweise

- In der Kopfzeile wird die Anzahl der eindeutigen Benutzer angezeigt, die sich am aktuellen Tag angemeldet haben, sowie eine Zeitachse mit der Anzahl der Anmeldungen pro Tag über einen Zeitraum von sieben Tagen. Die Zahl für „Heute angemeldete Benutzer“ ist von einem Kreis umgeben, der den Prozentsatz der angemeldeten Benutzer angibt. Im horizontalen Balkendiagramm der Anmeldungen werden die während der Woche eingetretenen Anmeldeereignisse angezeigt. Zeigen Sie auf einen der Punkte im Diagramm, um die Anzahl der Anmeldungen am betreffenden Tag anzuzeigen.
- Im Abschnitt „Benutzer und Gruppen“ wird die Anzahl der Benutzerkonten und -gruppen angezeigt, die in Workspace eingerichtet sind. Es werden die Benutzer angezeigt, die sich zuletzt angemeldet haben. Sie können auf **Vollständigen Bericht anzeigen** klicken, um einen Überwachungsereignisbericht zu erstellen, in dem die Benutzer angezeigt werden, die sich während einer Spanne von Tagen angemeldet haben.
- Im Abschnitt „App-Popularität“ wird ein Balkendiagramm angezeigt, das nach App-Typ gruppiert darstellt, wie oft Apps in einem Zeitraum von sieben Tagen gestartet wurden. Zeigen Sie auf einen bestimmten Tag, um eine QuickInfo anzuzeigen, in der die Typen der verwendeten Apps und die Anzahl der an diesem Tag gestarteten Apps angegeben werden. In der Liste unter dem Diagramm wird angezeigt, wie oft die betreffenden Apps gestartet wurden. Klicken Sie auf den Pfeil des Dropdown-Menüs auf der rechten Seite, um diese Informationen für einen Zeitraum von einem Tag, einer Woche, einem Monat oder von 12 Wochen anzuzeigen. Sie können auf **Vollständigen Bericht anzeigen** klicken, um einen Ressourcennutzungsbericht zu erstellen, in dem App, Ressourcentyp und Anzahl der Benutzeraktivitäten während eines Zeitraums angezeigt werden.

- Im Abschnitt „App-Verwendung“ wird ein Balkendiagramm angezeigt, das den Prozentsatz der Personen darstellt, die die Apps geöffnet haben, für die sie über eine Berechtigung verfügen. Zeigen Sie auf die App, um die QuickInfo anzuzeigen, in der die Anzahl der Verwendungen und Berechtigungen als absolute Zahl angegeben wird.
- Im Kreisdiagramm „Gestartete Apps“ werden die gestarteten Ressourcen als Prozentsatz sämtlicher Ressourcen angezeigt. Zeigen Sie auf einen bestimmten Abschnitt im Kreisdiagramm, um die Anzahl nach Ressourcentyp anzuzeigen. Klicken Sie auf den Pfeil des Dropdown-Menüs auf der rechten Seite, um diese Informationen für einen Zeitraum von einem Tag, einer Woche, einem Monat oder von 12 Wochen anzuzeigen.
- Im Abschnitt „Workspace-Clients“ wird die Anzahl der verwendeten Windows-Clients für Workspace angezeigt.

Weiter

Klicken Sie auf das Dropdown-Menü „Dashboard“, um das Systemdiagnose-Dashboard anzuzeigen.

Überwachen von Workspace -Systeminformationen und -Systemzustand

Im Systemdiagnose-Dashboard von Workspace werden eine ausführliche Übersicht über den Systemzustand der Workspace-Appliances in der Umgebung und Informationen über die Workspace-Dienste angezeigt. Sie können den allgemeinen Systemzustand der Workspace-Datenbankserver, der workspace-va-VMs und der auf den einzelnen virtuellen Maschinen verfügbaren Dienste anzeigen.

Im Systemdiagnose-Dashboard können Sie die zu überwachende workspace-va-VM auswählen und den Status der Dienste auf dieser virtuellen Maschine, einschließlich der installierten Version von Workspace, anzeigen. Wenn in der Datenbank oder auf einer virtuellen Maschine Probleme auftreten, wird in der Kopfzeilenleiste der Maschinenstatus in Rot angezeigt. Zum Anzeigen der Probleme können Sie die virtuelle Maschine auswählen, die in Rot angezeigt wird.

Vorgehensweise

- Ablauf des Benutzerkennworts. Hier wird das jeweilige Ablaufdatum der Kennwörter für die Root- und Remote-Anmeldung bei der Workspace-Appliance angezeigt. Wenn ein Kennwort abläuft, öffnen Sie die Seite „Einstellungen“ und wählen Sie **VA-Konfiguration** aus. Öffnen Sie die Seite **Systemsicherheit**, um das Kennwort zu ändern.
- Zertifikate. Hier werden Aussteller, Startdatum und Enddatum des Zertifikats angezeigt. Um das Zertifikat zu verwalten, öffnen Sie die Seite „Einstellungen“ und wählen Sie **VA-Konfiguration** aus. Öffnen Sie die Seite **Zertifikat installieren**.
- Konfigurator - Bereitstellungsstatus der Anwendung. Hier werden Informationen zu den Diensten von Appliance Configurator angezeigt. Auf der Seite „Webserverstatus“ wird angezeigt, ob der Tomcat-Server ausgeführt wird. Auf der Seite „Webanwendungsstatus“ wird angezeigt, ob Zugriff auf die Appliance Configurator-Seite möglich ist. Die Appliance-Version gibt die Version der installierten Workspace-Appliance an.
- Application Manager - Bereitstellungsstatus der Anwendung. Hier wird der Verbindungsstatus der Workspace-Appliance angezeigt.
- Connector - Bereitstellungsstatus der Anwendung. Hier wird der Connector Services-Administrator-Verbindungsstatus angezeigt. Wenn „Verbindung erfolgreich“ angezeigt wird, haben Sie Zugriff auf die Connector Services-Administrator-Seiten.
- Workspace-FQDN. Zeigt den vollqualifizierten Domänennamen an, den Benutzer für den Zugriff auf das Portal der Workspace-App eingeben. Der Workspace-FQDN verweist auf den Lastausgleichsdienst, sofern ein solcher verwendet wird.

- Application Manager - Integrierte Komponenten. Hier werden Informationen zur Workspace-Datenbankverbindung, zu Überwachungsdiensten und zur Verbindung mit dem Analysedienst angezeigt.
- Connector - Integrierte Komponenten. Hier werden Informationen über Dienste angezeigt, die auf den Seiten des Administrators für Connector-Dienste verwaltet werden. Es werden Informationen über ThinApp-, View- und von Citrix veröffentlichte Apps angezeigt.
- Module. Zeigt Ressourcen an, die in Workspace aktiviert sind. Klicken Sie auf **Aktiviert**, um die Seite des Administrators für Connector-Dienste für diese Ressource zu öffnen.

Konfigurieren der Workspace - Benutzerauthentifizierung 4

Workspace-Benutzerauthentifizierung erfordert die Verwendung mindestens einer Identitätsanbieter-Instanz. Dabei kann es sich um eine Workspace-Instanz (Standard), externe Identitätsanbieter-Instanzen oder eine Kombination beider Arten handeln. Die Identitätsanbieter-Instanzen authentifizieren Benutzer mit Active Directory innerhalb des Unternehmensnetzwerks

Um Identitätsanbieter-Instanzen zu konfigurieren und zu Ihrer Workspace-Bereitstellung hinzuzufügen, müssen verschiedene Voraussetzungen erfüllt sein, um sicherzustellen, dass Workspace ordnungsgemäß auf Ihre Active Directory-Bereitstellung zugreifen kann.

Dieses Kapitel behandelt die folgenden Themen:

- „Überblick über die Workspace-Benutzerauthentifizierung“, auf Seite 15
- „Hinzufügen oder Bearbeiten eines Netzwerkbereichs“, auf Seite 17
- „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18
- „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20
- „Überblick über das Konfigurieren von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz“, auf Seite 22
- „Bearbeiten des Standardrichtliniensatzes für den Zugriff“, auf Seite 24

Überblick über die Workspace -Benutzerauthentifizierung

Workspace versucht, Benutzer basierend auf den Authentifizierungsmethoden, dem Standardrichtliniensatz für den Zugriff, den Netzwerkbereichen und den Identitätsanbieter-Instanzen, die Sie konfiguriert haben, zu authentifizieren.

Von den Identitätsanbieter-Instanzen, die Sie mit Workspace verwenden, wird eine Verbundautorität im Netzwerk erstellt, die mit Workspace über SAML 2.0-Assertions kommuniziert. Die Identitätsanbieter-Instanzen authentifizieren den Benutzer mit Active Directory innerhalb des Unternehmensnetzwerks.

Workspace unterstützt die Benutzerauthentifizierungsmethoden Active Directory-Kennwort, Kerberos und RSA SecurID. Allerdings kann es sein, dass Ihr externer Identitätsanbieter weitere Authentifizierungsmethoden unterstützt, z. B. chipkartenbasierte Authentifizierung, die Sie für Ihre Workspace-Bereitstellung verwenden können.

Standardmäßig unterstützte Workspace-Authentifizierungstypen	Beschreibung
Kennwort	Ohne weitere Konfiguration unterstützt Workspace die Active Directory-Kennwortauthentifizierung. Diese Methode authentifiziert Benutzer direkt anhand des Active Directory.
Kerberos	Die Kerberos-Authentifizierung bietet Domänenbenutzern den Single Sign On-Zugriff (SSO) auf Workspace, d. h., Domänenbenutzer brauchen sich nach der Anmeldung beim Unternehmensnetzwerk nicht nochmals bei Workspace anzumelden. Die Identitätsanbieter-Instanz validiert die Anmeldedaten für den Benutzer-Desktop mithilfe von Kerberos-Tickets, die vom Key Distribution Center (KDC) verteilt werden.
RSA SecurID	Bei der RSA SecurID-Authentifizierung müssen die Benutzer ein Token-basiertes Authentifizierungssystem verwenden. RSA SecurID ist die empfohlene Authentifizierungsmethode für Benutzer, die von außerhalb des Unternehmensnetzwerks auf Workspace zugreifen.

Um Kerberos-Authentifizierung oder RSA SecurID-Authentifizierung zu implementieren, können Sie eine vorhandene Identitätsanbieter-Instanz verwenden oder, abhängig von Ihrer Bereitstellung, eine oder mehrere zusätzliche Identitätsanbieter-Instanzen bereitstellen.

Wenn ein Benutzer versucht, sich anzumelden, muss Workspace ermitteln, mit welcher Identitätsanbieter-Instanz der Benutzer authentifiziert werden soll.

Während des Entscheidungsprozesses evaluiert Workspace den Standardrichtliniensatz für den Zugriff, um auszuwählen, welche Richtlinie des Satzes angewendet wird. Die angewendete Richtlinie gibt die erforderliche Mindestauthentifizierungsbewertung für dieses Anmeldeereignis vor. Workspace filtert und sortiert die verfügbaren Authentifizierungsmethoden anschließend basierend auf der erforderliche Mindestauthentifizierungsbewertung und der Reihenfolge der Methoden, die Sie zur Erfüllung der Anforderungen Ihres Unternehmens als erforderlich festlegen können. Workspace wählt die erste Identitätsanbieter-Instanz, die die Authentifizierungsmethode und Netzwerkbereichsanforderungen des Richtlinie erfüllt, und leitet die Benutzerauthentifizierungsanforderung zur Authentifizierung an diese Instanz weiter. Falls die Authentifizierung fehlschlägt, wird der nächste Identitätsanbieter in der Liste herangezogen.

Wichtig Wenn Sie eine Identitätsanbieter-Instanz entfernen oder zurücksetzen, müssen Sie den Namen des entsprechenden Identitätsanbieters von der Seite „Identitätsanbieter“ entfernen.

Sie können Workspace so bereitstellen, dass der Vorgang der Identitätsanbieterauswahl auf verschiedene Arten erfolgt. Eine Möglichkeit ist im folgenden Beispiel zusammengefasst.

Beispiel für eine externe RSA SecurID- und interne Kennwortauthentifizierung oder höher

Hierbei handelt es sich um eine mögliche Methode zur Konfiguration von Workspace, damit die Active Directory-Kennwort- oder Kerberos-Authentifizierungsmethode für externe Benutzer in derselben Workspace-Bereitstellung verwendet wird.

- Interne Richtlinie – Sie verwenden Workspace Verwaltungskonsole, um eine Richtlinie im standardmäßigen Zugriffsrichtliniensatz zu erstellen. Hierbei muss die Authentifizierungspunktzahl mindestens das Active Directory-Kennwort als Authentifizierungsmethode akzeptieren. Um sicherzustellen, dass Workspace versucht, Benutzer zunächst mit der Kerberos-Authentifizierung zu authentifizieren, geben Sie für die Kerberos-Methode eine höhere Authentifizierungspunktzahl als für die Kennwortmethode ein und setzen Sie Kerberos auf der Seite „Authentifizierungsmethoden“ an die oberste Stelle der Liste. Sie weisen außerdem einen Netzwerkbereich für interne Benutzer zu.

- Externe Richtlinie – Sie verwenden Workspace Verwaltungskonsole, um eine Richtlinie im Standardrichtliniensatz für den Zugriff mit einer Mindestauthentifizierungsbewertung zu erstellen, die sicherstellt, dass die RSA SecurID-Authentifizierungsmethode zum Authentifizieren von Benutzern verwendet wird. Sie weisen außerdem einen Netzwerkbereich zu, der alle möglichen Benutzer umfasst, 0.0.0.0 bis 255.255.255.255.

Das Ergebnis dieser Konfiguration: Benutzer, die innerhalb des Unternehmensnetzwerks versuchen, auf Workspace zuzugreifen, werden an eine Identitätsanbieter-Instanz weitergeleitet, die Kerberos-Authentifizierung oder Kennwort-Authentifizierung durchführt, während Benutzer außerhalb des Unternehmensnetzwerks an eine Identitätsanbieter-Instanz weitergeleitet werden, die RSA SecurID-Authentifizierung durchführt. Interne und externe Benutzer können an dieselbe Identitätsanbieter-Instanz oder an unterschiedliche Identitätsanbieter-Instanzen gesendet werden, je nach Ihrer Konfiguration der Authentifizierungsmethoden.

Hinzufügen oder Bearbeiten eines Netzwerkbereichs

Sie können einen Netzwerkbereich mit IP-Adressen hinzufügen, die Sie zu einer bestimmten Identitätsanbieter-Instanz umleiten möchten.

Der Standard-Netzwerkbereich, als ALLE BEREICHE bezeichnet, enthält alle im Internet verfügbaren IP-Adressen, d. h. 0.0.0.0 bis 255.255.255.255. Selbst wenn Ihre Workspace-Bereitstellung eine einzige Identitätsanbieter-Instanz enthält, müssen Sie eventuell den Standardbereich konfigurieren und weitere Bereiche hinzufügen, um bestimmte IP-Adressen ein- oder auszuschließen. Sie müssen mehrere Netzwerkbereiche definieren, wenn Ihre Bereitstellung mehrere Identitätsanbieter-Instanzen mit unterschiedlichen Authentifizierungsmethoden enthält. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.

Hinweis Der Name des Standardnetzwerkbereichs („ALLE BEREICHE“) und seine Beschreibung („ein Netzwerk für alle Bereiche“) können bearbeitet werden. Sie können den Namen und die Beschreibung mit der Funktion **Bearbeiten** auf der Seite „Netzwerkbereiche“ bearbeiten, beispielweise den Text in einer anderen Sprache anzeigen.

Voraussetzungen

Führen Sie die notwendige Netzwerkbereichsplanung durch.

- Ermitteln Sie die beste Möglichkeit, Workspace den Anforderungen Ihrer Organisation entsprechend in Active Directory zu integrieren. Diese Planung betrifft die Anzahl der Identitätsanbieter-Instanzen in Ihrer Bereitstellung und somit auch die Anzahl der benötigten Netzwerkbereiche.
- Definieren Sie basierend auf Ihrer Netzwerktopologie Netzwerkbereiche für Ihre Workspace-Bereitstellung.
- Um einen Netzwerkbereich hinzuzufügen, notieren Sie sich die Horizon Client-Zugriffs-URL und -Portnummer für den Netzwerkbereich, während das View-Modul aktiviert ist. Weitere Informationen finden Sie in der Dokumentation zu View.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Einstellungen > Netzwerkbereiche**.

3 Bearbeiten Sie einen vorhandenen Netzwerbereich oder fügen Sie einen neuen Netzwerkbereich hinzu.

Option	Beschreibung
Vorhandenen Bereich bearbeiten	Klicken Sie für den Bereich, den Sie bearbeiten möchten, auf **Bearbeiten**.
Bereich hinzufügen	Klicken Sie auf **+ Netzwerkbereich**, um einen neuen Bereich hinzuzufügen.

4 Füllen Sie das Formular aus.

Formularelement	Beschreibung
Name	Geben Sie einen Namen für den Netzwerkbereich ein.
Beschreibung	Geben Sie eine Beschreibung für den Netzwerkbereich ein.
View-Pods	Die Option „View-Pods“ wird nur angezeigt, wenn das View-Modul aktiviert ist. Host der Client-Zugriffs-URL Geben Sie die korrekte Horizon Client-Zugriffs-URL für den Netzwerkbereich ein. Client-Zugriffsport Geben Sie den korrekten Horizon Client-Zugriffsport für den Netzwerkbereich ein. Weitere Informationen finden Sie in *Setting Up Resources in VMware Workspace Portal Guide*, Kapitel „Gewähren des Zugriffs auf View-Desktop- und -Anwendungspools“.
IP-Bereiche	Bearbeiten Sie IP-Bereiche oder fügen Sie IP-Bereiche hinzu, bis alle gewünschten IP-Adressen ein- und alle unerwünschten IP-Adressen ausgeschlossen sind.

Weiter

- Verknüpfen Sie die einzelnen Netzwerkbereiche jeweils mit einer Identitätsanbieter-Instanz. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.
- Weisen Sie Netzwerkbereiche entsprechend Zugriffsrichtliniensätzen zu. Siehe Kapitel 5, „Verwalten von Richtliniensätzen für den Zugriff“, auf Seite 27.

Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode

Sie können vorhandene Benutzerauthentifizierungsmethoden bearbeiten. Wenn Sie einen externen Identitätsanbieter hinzufügen, können Sie Benutzerauthentifizierungsmethoden konfigurieren, die Workspace nicht standardmäßig unterstützt. Sie können auch Zugriffsrichtlinien erstellen, um Authentifizierungsmethoden mit bestimmten Web-Anwendungen zu verknüpfen.

Workspace unterstützt die Benutzerauthentifizierungsmethoden Active Directory-Kennwort, Kerberos und RSA SecurID. Durch das Hinzufügen eines externen Identitätsanbieters, der eine andere Authentifizierungsmethode (z.˚B. chipkartenbasierte Authentifizierung) unterstützt, können Sie dafür sorgen, dass Workspace die betreffende Authentifizierungsmethode erzwingen kann. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20. Eine vollständige Liste mit Aufgaben bezüglich der Konfiguration von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz finden Sie unter „Überblick über das Konfigurieren von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz“, auf Seite 22 .

Die Mindest-Authentifizierungspunktzahl einer Methode und die Reihenfolge der Methode auf der Seite „Authentifizierungsmethoden“ sind entscheidend für den Vorgang, dem Workspace folgt, um eine Identitätsanbieter-Instanz für die Benutzerauthentifizierung auszuwählen. Informationen darüber, wie Sie Benutzer dazu verpflichten, für den Zugriff auf eine Web-Anwendung eine Authentifizierungsmethode mit einer bestimmten Mindestauthentifizierungspunktzahl zu verwenden, finden Sie unter „Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 29.

Die Anzahl der Versuche, die Workspace mit einer bestimmten Authentifizierungsmethode unternimmt, variiert. Workspace unternimmt mit Kerberos nur einen Authentifizierungsversuch. Wenn Kerberos bei der Anmeldung des Benutzers nicht erfolgreich ist, wird ein neuer Versuch mit der nächsten Authentifizierungsmethode in der Liste durchgeführt. Die maximale Anzahl fehlgeschlagener Anmeldeversuche mit Active Directory-Kennwort oder RSA SecurID-Authentifizierung ist fünf. Wenn der Benutzer fünf fehlgeschlagene Anmeldeversuche unternommen hat, versucht Workspace, den Benutzer mit der nächsten Authentifizierungsmethode in der Liste anzumelden. Wenn alle Authentifizierungsmethoden angewendet wurden, gibt Workspace eine Fehlermeldung aus.

Voraussetzungen

- Stellen Sie die Authentifizierungssysteme bereit, die Sie in Workspace integriert werden sollen. Wenn Sie beispielsweise vorhaben, RSA SecurID in Ihre Workspace-Bereitstellung zu integrieren, müssen Sie überprüfen, ob RSA SecurID auf Ihrem Netzwerk installiert und konfiguriert ist.
- Legen Sie die Sicherheitsstufen (von 1 = niedrigste Sicherheitsstufe bis 5 = höchste Sicherheitsstufe) für die Authentifizierungsmethoden fest, die Sie in Ihrer Workspace-Bereitstellung verwenden möchten.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Einstellungen > Authentifizierungsmethoden**.

3 Bearbeiten Sie eine vorhandene Authentifizierungsmethode oder fügen Sie eine neue Authentifizierungsmethode hinzu.

Option	Beschreibung
Bearbeiten einer vorhandenen Authentifizierungsmethode	Klicken Sie für die vorhandene Authentifizierungsmethode, die konfiguriert werden soll, auf **Bearbeiten**.
Hinzufügen einer neuen Authentifizierungsmethode	Klicken Sie auf **+ Authentifizierungsmethode hinzufügen**, um eine neue Authentifizierungsmethode hinzuzufügen. Wenn zum Beispiel eine neue externe Identitätsanbieter-Instanz zu Ihrer Bereitstellung hinzugefügt wird.

4 Bearbeiten Sie die Einstellungen für die Authentifizierungsmethode.

Formularelement	Beschreibung
Name	Geben Sie einen Namen für diese Identitätsanbieter-Instanz ein.
SAML-Kontext	Wählen Sie den geeigneten SAML-Kontext aus dem Dropdown-Menü aus. Die Liste enthält SAML-Authentifizierungskontexte, die derzeit gemäß den SAML 2.0-Spezifikationen unterstützt werden.

Formular-element	Beschreibung
Authentifizierungsbewertung	Wenn Sie Zugriffsrichtlinien entweder für den Standard-Zugriffsrichtliniensatz oder für Richtliniensätze für spezifische Web-Anwendungen erstellen, konfigurieren Sie eine Mindest-Authentifizierungspunktzahl. Bei den Richtlinien müssen sich Benutzer über eine Authentifizierungsmethode mit der angegebenen Authentifizierungspunktzahl oder höher authentifizieren, um im Fall einer Standardzugriffsrichtlinie auf Workspace oder im Fall einer Richtlinie für spezifische Web-Anwendungen auf eine Web-Anwendung zuzugreifen. Wenden Sie eine Authentifizierungsbewertung anhand Ihrer vordefinierten Sicherheitsstufen für Authentifizierungsmethoden an.
Standardmethode	Wählen Sie **Standardmethode**, um die Authentifizierungsmethode als Standardeinstellung festzulegen. Die Option **Standardmethode** bezieht sich auf die Option „SAML-Kontext“. Im folgenden Beispiel wird eine Situation beschrieben, in der Workspace die Authentifizierungsmethode verwendet, die Sie als Standardmethode festgelegt haben. Beim Hinzufügen einer Authentifizierungsmethode wählen Sie einen SAML-Kontext aus. Später stimmt der SAML-Kontext, den die externe Identitätsanbieter-Instanz sendet, nicht mit dem SAML-Kontext überein, den Sie für diese Identitätsanbieter-Instanz ausgewählt haben, und Workspace erkennt den gesendeten SAML-Kontext nicht. Anstatt den Authentifizierungsversuch zu beenden, versucht Workspace, den Benutzer mit der Authentifizierungsmethode zu authentifizieren, die Sie als Standardmethode ausgewählt haben.

5 Klicken Sie auf **Speichern**.

Weiter

- Verknüpfen Sie jede Authentifizierungsmethode mit der entsprechenden Identitätsanbieter-Instanz. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.
- Verknüpfen Sie Zugriffsrichtlinien mit Authentifizierungsmethoden, indem Sie die entsprechende Mindest-Authentifizierungspunktzahl für jede Zugriffsrichtlinie festlegen.

Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz

Durch Hinzufügen und Konfigurieren von Identitätsanbieter-Instanzen für Ihre Workspace-Bereitstellung können Sie Hochverfügbarkeit bereitstellen, zusätzliche Benutzerauthentifizierungsmethoden unterstützen und höhere Flexibilität bei der Verwaltung des Benutzerauthentifizierungsvorgangs auf der Basis von Benutzer-IP-Adressbereichen erlangen.

Fügen Sie zum Zwecke hoher Verfügbarkeit weitere Identitätsanbieter-Instanzen zu Ihrer Workspace-Bereitstellung hinzu.

Voraussetzungen

- Führen Sie die notwendige Planung aus.
  - Ermitteln Sie die beste Möglichkeit, Workspace den Anforderungen Ihrer Organisation entsprechend in Active Directory zu integrieren. Sie können eine einzelne Domäne oder eine Multidomänenstruktur konfigurieren.
  - Legen Sie die für die Anforderungen Ihrer Organisation erforderlichen Authentifizierungstypen fest. Sie können z.˚B. Kerberos-Authentifizierung für Benutzer innerhalb Ihrer Organisation und RSA SecurID-Authentifizierung für Benutzer außerhalb Ihrer Organisation konfigurieren. Sie können diese Art der Konfiguration unter Verwendung einer einzigen Identitätsanbieter-Instanz für beide Authentifizierungsmethoden oder unter Verwendung einer separaten Identitätsanbieter-Instanz für jede Authentifizierungsmethode einrichten.
- Stellen Sie Workspace mit einer einzelnen Active Directory-Domäne während der Machbarkeitsnachweis-Phase Ihrer Bereitstellung bereit.

- Bereiten Sie weitere Identitätsanbieter-Instanzen für Ihre Workspace-Bereitstellung vor.
  - Zum Hinzufügen einer externen Identitätsanbieter-Instanz führen Sie die folgenden Aufgaben aus: Eine vollständige Liste mit Aufgaben bezüglich der Konfiguration von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz finden Sie unter „Überblick über das Konfigurieren von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz“, auf Seite 22 .
    - Prüfen Sie, ob die externen Instanzen SAML 2.0-konform sind und ob Workspace diese erreichen kann.
    - Bestimmen Sie, wie Workspace die Metadaten von der externen Instanz erhält, und kopieren und speichern Sie die entsprechenden Metadateninformationen der externen Instanz, um sie während der Konfiguration in Workspace-Verwaltungskonsole einfügen zu können. Die Metadateninformationen, die Sie von der externen Instanz erhalten, sind entweder die URL zu den Metadaten oder die Metadaten selbst.
    - Wenn Sie Workspace in die Lage versetzen möchten, weitere Authentifizierungsmethoden zu verwenden, können Sie diese mithilfe von Verwaltungskonsole konfigurieren. Siehe „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18.
- Konfigurieren Sie Netzwerkbereiche mit Verwaltungskonsole. Weitere Informationen hierzu finden Sie unter „Hinzufügen oder Bearbeiten eines Netzwerkbereichs“, auf Seite 17

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Einstellungen > Identitätsanbieter**.

3 Klicken Sie auf **Identitätsanbieter hinzufügen**. Mit dieser Option werden Sie zur Eingabe von Informationen aufgefordert, mit denen Workspace eine vorhandene externe Identitätsanbieter-Instanz registrieren kann.

4 Bearbeiten Sie die Einstellungen für die Identitätsanbieter-Instanz.

Formularelement	Beschreibung
Typ	Wählen Sie für externe Identitätsanbieter-Instanzen die Einstellung **Manuell**. **Hinweis** Verwenden Sie die Option „Automatisch“ nur, wenn Sie vom technischen Support von VMware dazu aufgefordert werden.
Anbietername	Geben Sie einen Namen für diese Identitätsanbieter-Instanz ein.
Beschreibung	Geben Sie eine Beschreibung für diese Identitätsanbieter-Instanz ein.
Benutzerspeicher	Das Textfeld „Benutzerspeicher“ enthält eine Liste der Benutzerspeicher, die in Ihrer Workspace-Bereitstellung verfügbar sind. Wählen Sie alle Benutzerspeicher aus, die Sie mit dieser Identitätsanbieter-Instanz verknüpfen möchten.
Authentifizierungsmethoden	Das Textfeld „Authentifizierungsmethoden“ enthält eine Liste der Authentifizierungsmethoden, die in Ihrer Workspace-Bereitstellung verfügbar sind. Die Liste enthält die Standard-Authentifizierungsmethoden und vorher von Ihnen hinzugefügten Zusatzmethoden zur Unterstützung von externen Identitätsanbietern. Das Hinzufügen von zusätzlichen Authentifizierungsmethoden wird als Voraussetzung für diese Aufgabe beschrieben. Wenn die Authentifizierungsmethode, die Sie auswählen möchten, nicht in der Liste aufgeführt ist, fügen Sie sie wie in der Voraussetzung beschrieben hinzu. Wählen Sie die Authentifizierungsmethoden für Workspace aus, die bei Anmeldeversuchen von Benutzern, die mit dieser Identitätsanbieter-Instanz verknüpft sind, angewendet werden sollen. **Hinweis** Stellen Sie sicher, dass die ausgewählten Authentifizierungsmethoden aktiviert und richtig konfiguriert sind. Siehe *Installieren und Konfigurieren von Workspace*.

Formular-element	Beschreibung
Konfigurieren über	Die Option „Konfigurieren über“ ist nur verfügbar, wenn Sie eine externe Identitätsanbieter-Instanz hinzufügen und als Identitätsanbieter-Typ die Einstellung „Manuell“ wählen. Wählen Sie eine URL-Bezeichnermethode aus. ■ Wählen Sie „Auto-Erkennungs-URL“ aus, damit Workspace Metadaten der externen Identitätsanbieter-Instanz für Registrierungszwecke empfangen kann, geben Sie die URL zu den Metadaten in das Textfeld **Auto-Erkennung** ein. ■ Wählen Sie „Metadaten-XML“ aus, kopieren Sie die XML-Metadaten von der Identitätsanbieter-Instanz und fügen Sie sie in das Textfeld **Metadaten-XML** ein.
Netzwerkbereiche	Das Textfeld „Netzwerkbereiche“ enthält eine Liste der Netzwerkbereiche, die in Ihrer Workspace-Bereitstellung verfügbar sind. Wählen Sie die Netzwerkbereiche der Benutzer aufgrund ihrer IP-Adressen aus, die Sie zu dieser Identitätsanbieter-Instanz für die Authentifizierung umleiten möchten.

5 Klicken Sie auf **Speichern**.

6 Ändern Sie bei Bedarf die Reihenfolge der Identitätsanbieter-Instanzen.

Workspace sucht in der Liste der Identitätsanbieter-Instanzen von oben nach unten nach einer IP-Adresse. Falls eine IP-Adresse mehr als einer Identitätsanbieter-Instanz zugewiesen ist, erkennt Workspace die erste Instanz, also die Identitätsanbieter-Instanz, die in der Liste ganz oben erscheint.

a Klicken Sie auf **Reihenfolge der Identitätsanbieter bearbeiten**.

b Verschieben Sie eine Identitätsanbieter-Instanz mithilfe der Pfeile nach oben und nach unten an die gewünschte Position.

c Klicken Sie auf **Speichern**.

Weiter

- Wenn Sie Workspace für eine Multistrukturumgebung konfigurieren, informieren Sie Ihre Workspace-Benutzer über ihre jeweiligen Domänen. Erläutern Sie, dass sie bei der Anmeldung eine Domäne aus dem Dropdown-Menü auswählen müssen. Informieren Sie die Benutzer darüber, dass sie das Kontrollkästchen **Diese Einstellung speichern** aktivieren können, damit die Eingabeaufforderung nicht bei jeder Anmeldung erneut angezeigt wird.
- Falls Sie eine externe Identitätsanbieter-Instanz hinzugefügt haben, kopieren und speichern Sie die Workspace-Informationen, die für die Konfiguration einer externen Identitätsanbieter-Instanz erforderlich sind. Siehe „Abrufen der zum Konfigurieren einer externen Identitätsanbieter-Instanz erforderlichen Workspace-SAML-Informationen“, auf Seite 23.

Überblick über das Konfigurieren von Workspace zur Verwendung einer externen Identitätsanbieter-Instanz

Um Workspace zur Verwendung einer externen Identitätsanbieter-Instanz zu konfigurieren, müssen Sie mehrere bestimmte Schritte während der Konfiguration durchführen.

Vor der Konfiguration

Führen Sie folgende Schritte aus, bevor Sie Workspace Verwaltungskonsole verwenden, um eine externe Identitätsanbieter-Instanz hinzuzufügen.

1 Prüfen Sie, ob die externen Instanzen SAML 2.0-konform sind und ob Workspace diese erreichen kann.

2 Bestimmen Sie, wie Workspace die Metadaten von der externen Instanz erhält, und kopieren und speichern Sie die entsprechenden Metadateninformationen der externen Instanz, um sie während der Konfiguration in Workspace Verwaltungskonsole einfügen zu können. Die Metadateninformationen, die Sie von der externen Instanz erhalten, sind entweder die URL zu den Metadaten oder die Metadaten selbst.

3 Um Workspace zu ermöglichen, Authentifizierungsmethoden zu verwenden, die vom externen Identitätsanbieter unterstützt werden, verwenden Sie Verwaltungskonsole, um die zusätzlichen Authentifizierungsmethoden zu konfigurieren. Weitere Informationen hierzu finden Sie unter „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18

4 Bearbeiten Sie die Authentifizierungsmethoden, indem Sie das Kontrollkästchen **Standardmethode** aktivieren. Durch diese Aktion kann Workspace diese Authentifizierungsmethode im Falle eines Problems mit der externen Authentifizierungsmethode verwenden. Siehe „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18.

Konfiguration

Wenn Sie eine Identitätsanbieter-Instanz hinzufügen, führen Sie die folgenden Schritte spezifisch für den externen Identitätsanbieter durch. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.

1 Klicken Sie auf der Verwaltungskonsole-Seite „Einstellungen > Identitätsanbieter“ auf die Schaltfläche **+ Identitätsanbieter hinzufügen** und wählen Sie **Manuell** aus dem Dropdown-Menü **Typ** aus.

2 Wählen Sie die Authentifizierungsmethoden aus, die vom externen Identitätsanbieter unterstützt werden und die Sie für Workspace verwenden möchten.

3 Verwenden Sie die Option **Konfigurieren über**, um auszuwählen, wie Sie die Metadaten der externen Identitätsanbieter-Instanz an Workspace übertragen möchten, entweder durch die Verwendung einer auf die Metadaten verweisenden URL oder durch Kopieren und Einfügen der Metadaten.

Nach der Konfiguration

Sammeln Sie die SAML-Informationen von Workspace und wenden Sie sie auf die externe Identitätsanbieter-Instanz an. Siehe „Abrufen der zum Konfigurieren einer externen Identitätsanbieter-Instanz erforderlichen Workspace-SAML-Informationen“, auf Seite 23.

1 Verwenden Sie Workspace Verwaltungskonsole, um die SAML-Informationen zu sammeln, die zur Konfiguration der externen Identitätsanbieter-Instanz erforderlich sind.

2 Konfigurieren Sie die externe Identitätsanbieter-Instanz durch Anwendung der SAML-Informationen, die Sie aus Workspace erhalten haben.

Abrufen der zum Konfigurieren einer externen Identitätsanbieter-Instanz erforderlichen Workspace -SAML-Informationen

Wird Workspace mit einer externen Identitätsanbieter-Instanz integriert, müssen Sie, nachdem Sie die Konfiguration auf der Workspace-Seite durchgeführt haben, die erforderlichen SAML-Zertifikatinformationen kopieren und vorbereiten, um die Konfiguration auf der Seite der externen Identitätsanbieter-Instanz vorzunehmen.

Vorgehensweise

1 Melden Sie sich bei Verwaltungskonsole an.

2 Wählen Sie **Einstellungen > SAML-Zertifikat** aus.

3 Kopieren und speichern Sie das SAML-Signierungszertifikat, das in Workspace angezeigt wird.

   a Kopieren Sie die Zertifikatinformationen im Abschnitt „Signierungszertifikat“.

   b Speichern Sie die Zertifikatinformationen zur späteren Verwendung in einer Textdatei, wenn Sie die externe Identitätsanbieter-Instanz konfigurieren.

4 Stellen Sie die Metadaten des SAML-Dienstanbieters (SP) der externen Identitätsanbieter-Instanz bereit.

   a Klicken Sie auf der Seite „SAML-Zertifikat herunterladen“ auf **Metadaten des Dienstanbieters (SP)**.

   b Kopieren und speichern Sie die angezeigten Informationen mithilfe der Methode, die für Ihre Organisation am besten geeignet ist.

   Verwenden Sie diese kopierten Informationen später, wenn Sie die externe Identitätsanbieter-Instanz konfigurieren.

Methode	Beschreibung
URL der Seite kopieren	Kopieren und speichern Sie die URL der Seite „Metadaten des Dienstanbieters (SP)“
XML auf der Seite kopieren	Kopieren und speichern Sie den Inhalt der Seite in einer Textdatei.

5 Legen Sie die Benutzerzuordnung von der externen Identitätsanbieter-Instanz zu Workspace fest.

   Wenn Sie den externen Identitätsanbieter konfigurieren, bearbeiten Sie die SAML-Assertions im externen Identitätsanbieter zur Zuordnung von Workspace-Benutzern.

NameID-Format	Benutzerzuordnung
urn:oasis:names:tc:SAML:2.0:nameid-format:emailAddress	Der Wert „NameID“ in der SAML-Assertion wird dem E-Mail-Adressattribut in Workspace zugeordnet.
urn:oasis:names:tc:SAML:2.0nameid-format:unspecified	Der Wert „NameID“ in der SAML-Assertion wird dem Benutzernamen-Attribut in Workspace zugeordnet.

Weiter

Wenden Sie die für diese Aufgabe kopierten Informationen nach Bedarf an, um die externe Identitätsanbieter-Instanz zu konfigurieren.

Bearbeiten des Standardrichtliniensatzes für den Zugriff

Workspace enthält einen Standardrichtliniensatz für den Zugriff, der den Benutzerzugriff auf das Apps-Portal von Workspace steuert. Sie können den Richtliniensatz bei Bedarf bearbeiten, um Richtlinien zu ändern.

Jede Richtlinie im Standardrichtliniensatz für den Zugriff erfordert, dass eine Reihe von Kriterien erfüllt ist, bevor Workspace den Zugriff auf das Apps-Portal zulässt. Siehe Kapitel 5, „Verwalten von Richtliniensätzen für den Zugriff“, auf Seite 27.

Der folgende Richtliniensatz für den Zugriff dient als Beispiel dafür, wie Sie den Standardrichtliniensatz für den Zugriff zur Steuerung des Zugriffs auf das Apps-Portal von Workspace konfigurieren können. Weitere Anweisungen finden Sie im Abschnitt „Bearbeiten eines Richtliniensatzes für den Zugriff“, auf Seite 30.

Beispiel eines Standardrichtliniensatzes für den Zugriff

Dieses Beispiel verdeutlicht, wie Sie den Standardrichtliniensatz für den Zugriff bearbeiten können.

Name der Richtlinie	Netzwerk	Mindest-Authentifizierungsbewertung	TTL (Stunden)
Intern	Interner Bereich	1	8
Extern	Alle Bereiche	3	4

Die Richtlinien werden in der vorgenannten Reihenfolge ausgewertet. Sie können eine Richtlinie in einem Richtliniensatz nach oben oder nach unten ziehen, um die Priorität bei der Auswertung zu ändern.

Der Richtliniensatz aus dem obigen Beispiel gilt für den folgenden Anwendungsfall.

Standardzugriffsrichtlinie, Anwendungsfall mit Browser

1
- Intern. Damit Benutzer über ein internes Netzwerk (Interner Bereich) auf Workspace zugreifen können, verfügt Workspace über die Active Directory-Kennwortauthentifizierungsmethode. Um sicherzustellen, dass Workspace versucht, Benutzer zunächst mit der Kerberos-Authentifizierung zu authentifizieren, geben Sie für die Kerberos-Methode eine höhere Authentifizierungspunktzahl als für die Kennwortmethode ein und setzen Sie Kerberos auf der Seite „Authentifizierungsmethoden“ an die oberste Stelle der Liste. Sie weisen außerdem einen Netzwerkbereich für interne Benutzer zu. Der Benutzer meldet sich über einen Browser an und hat nun acht Stunden lang Zugriff auf das Benutzerportal.
- Extern. Für den Zugriff auf Workspace von einem externen Netzwerk (alle Bereiche) aus muss sich der Benutzer mit SecurID anmelden, welches in diesem Beispiel der Authentifizierungspunktzahl 3 entspricht. Der Benutzer meldet sich über einen Browser an und hat nun vier Stunden lang Zugriff auf das Apps-Portal.

2 Wenn ein Benutzer auf eine Ressource (mit Ausnahme einer Web-Anwendung, für die ein Richtliniensatz für spezifische Web-Anwendungen gilt) zuzugreifen versucht, gilt der Standardrichtliniensatz für den Portalzugriff.

   Die Time-to-Live (TTL) für solche Ressourcen stimmt beispielsweise mit der TTL des Standardrichtliniensatzes für den Zugriff auf das Portal überein. Wenn die TTL für einen Benutzer, der sich beim Apps-Portal anmeldet, gemäß dem Standardrichtliniensatz für den Zugriff auf das Portal 8 Stunden beträgt und der Benutzer versucht, während der TTL-Sitzung eine Ressource zu starten, wird die Anwendung gestartet, ohne dass sich der Benutzer erneut authentifizieren muss.

Verwalten von Richtliniensätzen für den Zugriff

5

Sie können den Standardrichtliniensatz für den Zugriff konfigurieren, um Kriterien festzulegen, die die Benutzer erfüllen müssen, um auf Workspace App-Portal zugreifen zu können. Sie können auch Richtliniensätze für den Zugriff auf spezifische Web-Anwendungen erstellen, um Kriterien festzulegen, die die Benutzer erfüllen müssen, um bestimmte Web-Anwendungen starten zu können.

Um eine Zugriffsrichtlinie anzuwenden, erstellen Sie die Richtlinie als Teil eines Richtliniensatzes für den Zugriff. Jede Richtlinie in einem Richtliniensatz für den Zugriff kann folgende Angaben enthalten.

- Von wo aus Benutzer sich anmelden dürfen, z.°B. von innerhalb oder von außerhalb des Unternehmensnetzwerks.
- Die Mindest-Authentifizierungspunktzahl, welche die Authentifizierungsmethoden definiert, die für diese Richtlinie zulässig sind.
- Anzahl der für die Benutzer bereitgestellten Stunden für den Zugriff.

Hinweis Workspace-Zugriffsrichtlinien steuern nicht die Dauer einer Web-Anwendungssitzung. Sie steuern, wie viel Zeit Benutzern zum Starten einer Web-Anwendung zur Verfügung steht.

Workspace hat einen Standardrichtliniensatz, den Sie bearbeiten können. Dieser Richtliniensatz für den Zugriff steuert den Zugriff auf Workspace insgesamt. Siehe „Bearbeiten des Standardrichtliniensatzes für den Zugriff“, auf Seite 24. Um den Zugriff auf bestimmte Web-Anwendungen zu steuern, können Sie zusätzliche Richtliniensätze für den Zugriff erstellen. Wenn Sie keinen Richtliniensatz für den Zugriff auf eine Web-Anwendung anwenden, gilt der Standardrichtliniensatz für den Zugriff.

Dieses Kapitel behandelt die folgenden Themen:

- „Überblick über Einstellungen für Zugriffsrichtlinien“, auf Seite 28
- „Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 29
- „Bearbeiten eines Richtliniensatzes für den Zugriff“, auf Seite 30
- „Hinzufügen eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 32
- „Anwenden eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 33

Überblick über Einstellungen für Zugriffsrichtlinien

Ein Richtliniensatz für den Zugriff enthält mindestens eine Zugriffsrichtlinie. Jede Zugriffsrichtlinie besteht aus Einstellungen, die Sie zur Verwaltung des Benutzerzugriffs auf Workspace App-Portal als Ganzes oder auf bestimmte Webanwendungen konfigurieren können.

Jede Zugriffsrichtlinie verknüpft einen Netzwerkbereich mit einer Authentifizierungspunktzahl. Ein Benutzer, der sich von einer IP-Adresse innerhalb des von der Richtlinie bestimmten Netzwerkbereichs aus anmeldet, erhält eine Authentifizierungsmethode, die gleich oder höher als die Mindest-Authentifizierungspunktzahl der Richtlinie ist. Jede Identitätsanbieter-Instanz in IhrerWorkspace-Bereitstellung verknüpft ebenfalls Netzwerkbereiche mit Authentifizierungsmethoden. Beim Konfigurieren einer Zugriffsrichtlinie müssen Sie darauf achten, dass die erstellte Zuordnung zwischen Netzwerkbereich und Authentifizierungsbewertung durch eine vorhandene Identitätsanbieter-Instanz abgedeckt ist.

Wenn Sie eine Zugriffsrichtlinie erstellen, können Sie die folgenden Einstellungen konfigurieren.

Netzwerk

Für jede Zugriffsrichtlinie legen Sie die Benutzerbasis fest, indem Sie einen Netzwerkbereich angeben. Ein Netzwerkbereich besteht aus mindestens einem IP-Adressenbereich. Sie können Netzwerkbereiche auf der Seite „Netzwerkbereiche“ in Verwaltungskonsole erstellen, bevor Sie die Richtliniensätze für den Zugriff konfigurieren.

Mindest-Authentifizierungsbewertung

Sie weisen jeder Authentifizierungsmethode eine Authentifizierungsbewertung zu, wenn Sie die Seite „Authentifizierungsmethoden“ in Verwaltungskonsole konfigurieren, bevor Sie die Richtliniensätze für den Zugriff konfigurieren.

Workspace unterstützt standardmäßig die Authentifizierungsmethoden Active Directory-Kennwort, Kerberos und RSA SecurID. Wenn Sie externe Identitätsanbieter-Instanzen in Ihre Workspace-Bereitstellung integrieren, unterstützt Workspace die weiterer Authentifizierungsmethoden, die von den externen Identitätsanbietern unterstützt werden.

Wenn sich ein Benutzer bei Workspace anmeldet, zeichnet Workspace die Zeit und die Methode der Authentifizierung auf.

Wenn der Benutzer dann versucht, auf eine Web-Anwendung zuzugreifen, der ein Richtliniensatz für den Zugriff zugeordnet wurde, vergleicht Workspace die aktuelle Authentifizierungsbewertung des Benutzers mit der Authentifizierungsbewertung, die für den Zugriff auf die Web-Anwendung erforderlich ist. Wenn die aktuelle Authentifizierungsbewertung des Benutzers niedriger ist als die erforderliche Mindestauthentifizierungsbewertung für die angeforderte Anwendung, leitet Workspace den Benutzer zu einer Identitätsanbieter-Instanz um, die die stärkere Authentifizierung ermöglicht. Wenn die aktuelle Authentifizierungspunktzahl des Benutzers gleich oder höher als die erforderliche Mindest-Authentifizierungspunktzahl für die angeforderte Anwendung ist, startet Workspace die Anwendung nach Bestätigung des Time-to-Live-Wertes. Eine Erklärung zu Time-to-Live finden Sie im Folgenden. Workspace verweigert die Zugangsanforderung zum App-Portal oder die Anforderung, eine Webanwendung zu starten, unter den folgenden Bedingungen.

- Für die Anforderung wurde keine Richtlinie definiert.
- Für die Mindest-Authentifizierungspunktzahl wurde keine Authentifizierungs-Identitätsanbieter-Instanz definiert.
- Der Benutzer konnte sich mit keiner der Authentifizierungsmethoden authentifizieren.

Time-To-Live

Für jede Zugriffsrichtlinie weisen Sie einen TTL-Wert (Time-to-Live) zu. Der TTL-Wert bestimmt, wie viel Zeit den Benutzern seit ihrem letzten Authentifizierungsereignis maximal für den Zugriff auf Workspace oder zum Starten einer bestimmten Web-Anwendung zur Verfügung steht. Mit einem TTL-Wert von 4 in einer Web-Anwendungsrichtlinie werden für die Benutzer vier Stunden zum Starten der Web-Anwendung bereitgestellt, sofern sie kein weiteres Authentifizierungsereignis initiieren, das den TTL-Wert erhöht.

Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen

Sie können Zugriffsrichtlinien für spezifische Web-Anwendungen erstellen. Beispielsweise können Sie eine Zugriffsrichtlinie für eine Web-Anwendung erstellen, die angibt, welche IP-Adressen Zugriff auf die Anwendung haben, welche Authentifizierungsmethoden diese verwenden müssen und nach welchem Intervall eine erneute Authentifizierung erforderlich ist.

ACHTUNG Als bewährte Vorgehensweise wird empfohlen, die Mindest-Authentifizierungspunktzahl von Web-Anwendungs-spezifischen Richtlinien so zu konfigurieren, dass sie gleich oder höher als die Mindest-Authentifizierungspunktzahl von Richtlinien im Standardzugriffsrichtliniensatz ist, die entsprechende Netzwerkbereiche aufweisen.

Der folgende Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen ist ein Beispiel für einen Richtliniensatz, den Sie erstellen können, um den Zugriff auf spezifische Web-Anwendungen zu steuern. Siehe Kapitel 5, „Verwalten von Richtliniensätzen für den Zugriff“, auf Seite 27.

Beispiel 1: Web-Anwendungs-spezifischer Richtliniensatz

Dieses Beispiel veranschaulicht einen Richtliniensatz, den Sie erstellen und auf eine sensible Anwendung anwenden könnten.

Name der Richtlinie	Netzwerk	Mindest-Authentifizierungsbewertung	TTL (Stunden)
Intern	Interner Bereich	1	8
Extern	Alle Bereiche	3	4

Die Richtlinien werden in der vorgenannten Reihenfolge ausgewertet. Sie können eine Richtlinie in einem Richtliniensatz nach oben oder nach unten ziehen, um die Priorität bei der Auswertung zu ändern.

Der Richtliniensatz im obigen Beispiel gilt für die folgenden Anwendungsfälle.

Strenger Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen, Anwendungsfall mit Browser

1. Um von außerhalb des Unternehmensnetzwerks auf Workspace zuzugreifen, muss sich der Benutzer mit der RSA SecurID anmelden, welche in diesem Beispiel der Mindest-Authentifizierungspunktzahl 3 entspricht. Siehe das Beispiel für die Richtlinie „Extern“ in „Bearbeiten des Standardrichtliniensatzes für den Zugriff“, auf Seite 24. Der Benutzer meldet sich mit einem Browser an und hat jetzt für eine vierstündige Sitzung Zugriff auf das App-Portal, entsprechend den Einstellungen im Standardrichtliniensatz für den Zugriff.
2. Nach vier Stunden versucht der Benutzer, eine Web-Anwendung zu starten, für die der Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen aus Beispiel 1 angewendet wird.
3. Workspace prüft die Richtlinien in dem Richtliniensatz von Beispiel 1 und wendet die Richtlinie „Extern“ mit dem „Alle Bereiche“-Netzwerkbereich an, da die Benutzeranforderung von einem Webbrowser und aus dem „Alle Bereiche“-Netzwerkbereich kommt.

Der Benutzer wird mit der Mindest-Authentifizierungspunktzahl 3 angemeldet. Diese weist die geeignete Authentifizierungspunktzahl auf, um die sensible Anwendung zu starten, aber die TTL der Richtlinie ist soeben abgelaufen. Daher wird der Benutzer zur erneuten Authentifizierung umgeleitet. Mit der erneuten Authentifizierung kann der Benutzer eine weitere vierstündige Sitzung beginnen und die Anwendung nun starten. Für die nächsten vier Stunden kann der Benutzer die Anwendung weiterhin starten, ohne sich erneut authentifizieren zu müssen.

Beispiel 2: Web-Anwendungs-spezifischer Richtliniensatz

Dieses Beispiel veranschaulicht einen Richtliniensatz, den Sie für eine besonders sensible Anwendung erstellen und anwenden könnten.

Name der Richtlinie	Netzwerk	Mindest-Authentifizierungsbewertung	TTL (Stunden)
ExtraSensitive	Alle Bereiche	Stufe 3	1

Der Richtliniensatz aus dem obigen Beispiel gilt für den folgenden Anwendungsfall.

Anwendungsfall mit besonders strengem Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen

1 Der Benutzer meldet sich mit der Authentifizierungsmethode „Kennwort“ innerhalb des Unternehmensnetzwerks an, welches in diesem Beispiel der Authentifizierungsstufe 1 entspricht. Siehe das Beispiel für die Richtlinie „Intern“ in „Bearbeiten des Standardrichtliniensatzes für den Zugriff“, auf Seite 24.

   Jetzt hat der Benutzer acht Stunden lang Zugriff auf das App-Portal.

2 Der Benutzer versucht daraufhin sofort, eine Web-Anwendung zu starten, auf die der Richtliniensatz aus Beispiel 2 angewendet wird. Für diesen Richtliniensatz ist mindestens die Authentifizierungsstufe 3 erforderlich.

3 Der Benutzer wird zu einem Identitätsanbieter umgeleitet, der eine Authentifizierungsstärke ab Stufe 3 anbietet, die die Authentifizierung mit RSA SecurID erfordert.

4 Nachdem sich der Benutzer erfolgreich angemeldet hat, startet Workspace die Anwendung und speichert das Authentifizierungsereignis.

   Der Benutzer kann diese Anwendung eine Stunde lang starten, wird aber nach einer Stunde aufgefordert, sich erneut zu authentifizieren, es sei denn, der hat innerhalb einer Stunde nach dem Start ein Authentifizierungsereignis der Stufe 3 oder höher initiiert, wie von der Richtlinie verlangt.

Bearbeiten eines Richtliniensatzes für den Zugriff

Sie können diesen Standardrichtliniensatz für den Zugriff, bei dem es sich um einen vordefinierten Richtliniensatz handelt, der den Benutzerzugriff auf Workspace insgesamt steuert, oder zuvor manuell erstellte Richtliniensätze für spezifische Web-Anwendungen bearbeiten.

Sie können einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen jederzeit entfernen. Der Standardrichtliniensatz für den Zugriff ist dauerhaft. Sie können ihn bearbeiten, aber nicht entfernen.

Sie können einen vorhandenen Standardrichtliniensatz für den Zugriff (entweder den Standardrichtliniensatz für den Zugriff oder einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen) bearbeiten, indem Sie vorhandene Richtlinien aus dem Satz entfernen, vorhandene Richtlinien ändern oder neue Richtlinien zum Satz hinzufügen. Einen Überblick über Richtliniensätze für den Zugriff finden Sie unter Kapitel 5, „Verwalten von Richtliniensätzen für den Zugriff“, auf Seite 27.

Informationen über und Beispiele für Richtliniensätze finden Sie in dem entsprechenden Thema.

- „Bearbeiten des Standardrichtliniensatzes für den Zugriff“, auf Seite 24.

- „Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 29.

Voraussetzungen

- Konfigurieren Sie die geeigneten Identitätsanbieter für Ihre Bereitstellung. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.
- Konfigurieren Sie die geeigneten Netzwerkbereiche für Ihre Workspace-Bereitstellung. Siehe „Hinzufügen oder Bearbeiten eines Netzwerkbereichs“, auf Seite 17.
- Konfigurieren Sie die geeigneten Authentifizierungsmethoden für Ihre Bereitstellung. Siehe „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Richtlinien > Richtliniensätze für den Zugriff** aus.

3 (Optional) Um einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen dauerhaft zu löschen, klicken Sie für den Richtliniensatz auf **Entfernen**.

Die Option **Entfernen** ist für den Standardrichtliniensatz für den Zugriff nicht verfügbar. Der Standardrichtliniensatz für den Zugriff kann nicht gelöscht werden.

4 Klicken Sie für den vorhandenen Richtliniensatz, der konfiguriert werden soll, auf **Bearbeiten**.

5 (Optional) Ändern Sie bei Bedarf in den entsprechenden Textfeldern den Namen und die Beschreibung des Richtliniensatzes.

HINWEIS Workspace zeigt den Text in den Textfeldern „Name des Richtliniensatzes“ und „Beschreibung“ in Englisch an. Sie können diesen Text bearbeiten. Es besteht z.˚B. die Möglichkeit, den Text in einer anderen Sprache anzuzeigen.

6 (Optional) Bei Bedarf können Sie eine vorhandene Richtlinie bearbeiten oder entfernen oder eine neue Richtlinie hinzufügen.

Als bewährte Vorgehensweise wird empfohlen, die Mindest-Authentifizierungspunktzahl von Web-Anwendungs-spezifischen Richtlinien so zu konfigurieren, dass sie gleich oder höher als die Mindest-Authentifizierungspunktzahl von Richtlinien im Standardzugriffsrichtliniensatz ist, die entsprechende Netzwerkbereiche aufweisen.

Option	Beschreibung
Bearbeiten einer vorhandenen Richtlinie	a Klicken Sie auf den Namen der Richtlinie, die Sie konfigurieren möchten. b Nehmen Sie die entsprechenden Änderungen an den Richtlinieneinstellungen vor. c Klicken Sie auf **Übernehmen**.
Entfernen einer vorhandenen Richtlinie	a Klicken Sie auf den Namen der Richtlinie, die Sie entfernen möchten. b Klicken Sie auf **Entfernen**.
Hinzufügen einer neuen Richtlinie	a Klicken Sie auf **+ Zugriffsrichtlinie**, um eine neue Richtlinie hinzuzufügen. b Nehmen Sie die entsprechende Konfiguration der Richtlinieneinstellungen vor. c Klicken Sie auf **Hinzufügen**.

7 Klicken Sie auf **Speichern**.

Der bearbeitete Zugriffsrichtliniensatz wird sofort wirksam.

Weiter

Wenn es sich bei dem Richtliniensatz um einen noch nicht angewendeten Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen handelt, wenden Sie den Richtliniensatz auf mindestens eine Web-Anwendung an.

Hinzufügen eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen

Sie können Richtliniensätze für den Zugriff auf spezifische Web-Anwendungen erstellen, um den Benutzerzugriff auf spezifische Web-Anwendungen zu steuern.

Einen Überblick über Richtliniensätze für den Zugriff finden Sie unter Kapitel 5, „Verwalten von Richtliniensätzen für den Zugriff“, auf Seite 27. Informationen und Beispiele für Richtliniensätze für den Zugriff auf spezifische Web-Anwendungen finden Sie unter „Verwalten von Richtliniensätzen für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 29.

Voraussetzungen

- Konfigurieren Sie die geeigneten Identitätsanbieter für Ihre Bereitstellung. Siehe „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.
- Konfigurieren Sie die geeigneten Netzwerkbereiche für Ihre Workspace-Bereitstellung. Siehe „Hinzufügen oder Bearbeiten eines Netzwerkbereichs“, auf Seite 17.
- Konfigurieren Sie die geeigneten Authentifizierungsmethoden für Ihre Bereitstellung. Siehe „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18.
- Insbesondere bei der Erstkonfiguration von Workspace sollten Sie, wenn Sie planen, den Standardrichtliniensatz für den Zugriff auf das Portal zu bearbeiten (um den Benutzerzugriff auf Workspace insgesamt zu steuern), diesen konfigurieren, bevor Sie Richtliniensätze für den Zugriff auf spezifische Web-Anwendungen erstellen.

Vorgehensweise

1. Melden Sie sich bei Workspace-Verwaltungskonsole an.
2. Wählen Sie **Richtlinien > Richtliniensätze für den Zugriff** aus.
3. Klicken Sie auf **+ Richtliniensatz für den Zugriff**, um einen neuen Richtliniensatz hinzuzufügen.
4. Fügen Sie in den entsprechenden Textfeldern einen Namen und eine Beschreibung des Richtliniensatzes ein.
5. Klicken Sie auf **+ Zugriffsrichtlinie**, um die erste Richtlinie hinzuzufügen.
6. Nehmen Sie die entsprechende Konfiguration der Richtlinieneinstellungen vor.

ACHTUNG Als bewährte Vorgehensweise wird empfohlen, die Mindest-Authentifizierungspunktzahl von Web-Anwendungs-spezifischen Richtlinien so zu konfigurieren, dass sie gleich oder höher als die Mindest-Authentifizierungspunktzahl von Richtlinien im Standardzugriffsrichtliniensatz ist, die entsprechende Netzwerkbereiche aufweisen.

7. Klicken Sie auf **Hinzufügen**.
8. (Optional) Wiederholen Sie die Schritte zum Hinzufügen von Richtlinien, bis die Richtliniensätze den Anforderungen Ihrer Organisation entsprechen.
9. Klicken Sie auf **Speichern**, um den Richtliniensatz zu speichern.

Weiter

Wenden Sie den Richtliniensatz auf eine oder mehrere Web-Anwendungen an.

Anwenden eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen

Nachdem Sie einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen erstellt haben, können Sie diesen auf spezifische Web-Anwendungen anwenden, um den Benutzerzugriff auf diese Anwendungen zu steuern.

Workspace wendet den Standard-Zugriffsrichtliniensatz auf alle neuen Web-Anwendungen an. Sie müssen einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen auf eine Web-Anwendung anwenden, um den Standard-Zugriffsrichtliniensatz zu überschreiben.

Voraussetzungen

Falls noch nicht geschehen, erstellen Sie einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen, um den Benutzerzugriff auf eine spezifische Web-Anwendung zu steuern. Weitere Informationen hierzu finden Sie unter „Hinzufügen eines Richtliniensatzes für den Zugriff auf spezifische Web-Anwendungen“, auf Seite 32

Vorgehensweise

1 Klicken Sie auf die Registerkarte **Katalog**.

2 Klicken Sie auf **Jeder Anwendungstyp > Web-Anwendungen**.

3 Klicken Sie auf die Web-Anwendung, auf die Sie einen Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen anwenden möchten.

   Die Informationsseite der Web-Anwendung wird angezeigt. Dabei ist standardmäßig die Registerkarte **Berechtigungen** ausgewählt.

4 Klicken Sie auf **Zugriffsrichtlinien**.

5 Wählen Sie aus dem Dropdown-Menü „Richtliniensatz für den Zugriff“ den Richtliniensatz für den Zugriff auf spezifische Web-Anwendungen aus, der für die Anwendung gelten soll.

6 Klicken Sie auf **Speichern**.

Der Richtliniensatz für den Zugriff steuert jetzt den Benutzerzugriff auf die Anwendung.

Verwalten von Benutzern und Gruppen

6

Sie können Benutzer und Gruppen verwalten und überwachen, einschließlich von Active Directory importierte Benutzer und Gruppen, Gastbenutzer und Workspace-Gruppen.

In Workspace Verwaltungskonsole bietet die Seite „Benutzer & Gruppen“ eine auf Benutzer und Gruppen ausgerichtete Ansicht von Workspace. Beispielsweise können Sie von der Seite „Berechtigungen“ eines Benutzers aus diesem Benutzer Berechtigungen für eine Ressource und von der Seite „Berechtigungen“ einer Gruppe aus dieser Gruppe Berechtigungen für eine Ressource erteilen. Alternativ bietet die Katalogseite eine auf Ressourcen ausgerichtete Ansicht von Workspace. Beispielsweise können Sie von der Seite „Berechtigungen“ einer Ressource aus dieser Ressource Berechtigungen für einen Benutzer oder eine Gruppe erteilen.

Dieses Kapitel behandelt die folgenden Themen:

- „Benutzer- und Gruppentypen von Workspace“, auf Seite 35
- „Verwalten von Workspace-Gruppen“, auf Seite 36
- „Verwalten von Workspace-Benutzern“, auf Seite 41
- „Ändern von Benutzern und Gruppen, die aus Active Directory synchronisieren“, auf Seite 44

Benutzer- und Gruppentypen von Workspace

Mithilfe von Workspace Verwaltungskonsole können Sie Benutzer, Gastbenutzer und Gruppen verwalten.

Benutzer

Workspace-Benutzer sind solche, die von Active Directory importiert wurden. Die Workspace-Benutzerbasis wird gemäß dem Zeitplan für die Synchronisierung Ihres Verzeichnisservers aktualisiert.

Gruppen

Die Gruppentypen, die in Workspace-Verwaltungskonsole angezeigt werden können, sind von Ihrem Verzeichnisserver importierte Gruppen sowie Workspace-Gruppen, bei denen es sich um von Ihnen unter Verwendung von Workspace selbst erstellte Gruppen handelt.

Gruppen-typ	Beschreibung
Verzeich-nisserver-gruppen	Sie verwenden die Connector Services-Administrator-Seite „Verzeichnissynchronisierung, Gruppen auswählen“, um Gruppen aus Active Directory in Workspace zu importieren. In Verwaltungskonsole gibt ein Sperrsymbol neben dem Namen einer Gruppe an, dass es sich bei ihr um eine Verzeichnisservergruppe handelt. Sie können Workspace nicht zum Bearbeiten oder Löschen von Verzeichnisservergruppen verwenden. Importierte Verzeichnisservergruppen werden in Workspace gemäß dem Zeitplan für die Synchronisierung Ihres Verzeichnisservers aktualisiert.
Work-space-Gruppen	Sie verwenden Workspace-Verwaltungskonsole zum Erstellen von Workspace-Gruppen. Dabei handelt es sich um Gruppen, die Sie für die optimale Verwendung von Workspace innerhalb Ihres Unternehmens anpassen. Sie können Workspace-Gruppen erstellen, indem Sie eine Kombination von Benutzern und Gruppen hinzufügen. Bei den Gruppen, die Sie hinzufügen, kann es sich um vorhandene Workspace-Gruppen oder um Gruppen handeln, die aus Ihrem Verzeichnisserver importiert wurden. In Verwaltungskonsole gibt ein Kontrollkästchen neben dem Namen einer Gruppe an, dass es sich um eine Workspace-Gruppe handelt. Sie können Workspace zum Löschen einer Workspace-Gruppe oder zum Ändern der Benutzer in der Gruppe verwenden.

Sie können die Ressourcen angeben, auf die die Gruppenmitglieder zugreifen und die sie verwenden dürfen. Anstatt Berechtigungen für jeden einzelnen Benutzer zu definieren, können Sie sie mehreren Benutzern zuweisen, indem Sie der Gruppe die Berechtigungen erteilen. Ein Benutzer kann mehreren Gruppen angehören. Wenn Sie beispielsweise die Gruppen „Vertrieb“ und „Geschäftsführung“ erstellen, kann der Vertriebsleiter beiden Gruppen angehören. Sie können festlegen, welche mobile Richtlinieneinstellungen auf die Mitglieder der Gruppe angewendet werden.

Verwalten von Workspace -Gruppen

Das Erstellen von Gruppen, Ändern von Gruppenmitgliedschaften und Löschen von Gruppen sind Aufgaben, die Sie in Workspace durchführen können und die nur für Workspace-Gruppen gelten. Die Berechtigung von Gruppen für Ressourcen ist eine Aufgabe, die Sie sowohl für Workspace-Gruppen als auch für Active Directory-Gruppen durchführen können.

Vorgehensweise

- Um eine Workspace-Gruppe zu erstellen, wählen Sie **Benutzer & Gruppen > Gruppen**, klicken auf **Gruppe erstellen** und geben den Gruppennamen und eine Beschreibung an.
- Um eine oder mehrere Workspace-Gruppen zu löschen, wählen Sie **Benutzer & Gruppen > Gruppen**, aktivieren die Kontrollkästchen für die entsprechenden Workspace-Gruppen, die Sie löschen möchten, und klicken auf **Gruppen löschen**.

  Sie können nur Workspace-Gruppen löschen. Ein Sperrsymbol wird neben den Namen der Active Directory-Gruppen angezeigt, das angibt, dass die Gruppe eine Active Directory-Gruppe ist und Sie Workspace nicht verwenden können, um die Gruppe zu bearbeiten oder zu löschen.

Ändern der Workspace -Gruppenmitgliedschaft

Sie können die Workspace-Gruppenmitgliedschaft ändern.

Verwenden Sie Gruppen, um gleichzeitig mehreren Benutzern die Berechtigungen für dieselben Ressourcen zu erteilen, anstatt jedem Benutzer die Berechtigung einzeln zu erteilen.

Sie verwenden Gruppenregeln, um festzulegen, welche Benutzer Mitglieder einer bestimmten Workspace-Gruppe sind. Ein Benutzer kann mehreren Gruppen angehören. Wenn Sie beispielsweise die Gruppen „Vertrieb“ und „Geschäftsführung“ erstellen, kann der Vertriebsleiter Mitglied beider Gruppen sein.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Benutzer & Gruppen > Gruppen**.

- Ein Kontrollkästchen neben dem Namen einer Gruppe gibt an, dass es sich um eine Workspace-Gruppe handelt.
- Ein Sperrsymbol neben einem Gruppennamen gibt an, dass es sich bei der Gruppe um eine Verzeichnisservergruppe handelt. Sie verwalten Verzeichnisservergruppen direkt im Verzeichnisserver. Sie können Workspace nicht zum Definieren der Mitgliedschaft von Verzeichnisservergruppen verwenden.

3 Klicken Sie auf den Namen der Workspace-Gruppe, deren Mitgliedschaft Sie ändern möchten.

4 Klicken Sie auf die Registerkarte **Benutzer in dieser Gruppe**.

Das System zeigt die Liste der Benutzer an, die aktuell Mitglieder der Gruppe sind.

5 Klicken Sie auf **Benutzer in dieser Gruppe ändern**.

6 Wählen Sie aus dem Dropdown-Menü eine Option aus.

Option	Aktion
Eine der folgenden Optionen	Gewährt die Gruppenmitgliedschaft, wenn mindestens eine der Voraussetzungen für die Gruppenmitgliedschaft erfüllt ist. Diese Option funktioniert wie eine ODER-Bedingung. Wenn Sie beispielsweise **Eine der folgenden Optionen** für die Regeln „Gruppe ist Vertrieb“ und „Gruppe ist Marketing“ auswählen, wird sowohl Vertriebs- als auch Marketing-Mitarbeitern die Mitgliedschaft in dieser Gruppe gewährt.
Alle der folgenden Optionen	Gewährt die Gruppenmitgliedschaft, wenn alle Voraussetzungen für die Gruppenmitgliedschaft erfüllt sind. Diese Option funktioniert wie eine UND-Bedingung. Wenn Sie beispielsweise **Alle der folgenden Optionen** für die Regeln „Gruppe ist Vertrieb“ und „E-Mail beginnt mit 'western_region'“ auswählen, wird nur Vertriebsmitarbeitern in der Region West die Mitgliedschaft in dieser Gruppe gewährt. Vertriebsmitarbeitern aus anderen Regionen wird die Mitgliedschaft in dieser Gruppe nicht gewährt.

7 Konfigurieren Sie eine oder mehrere Regeln für Ihre Workspace-Gruppe.

Sie können Regeln verschachteln.

Option	Aktion
Gruppe	■ Wählen Sie **Ist**, um eine Gruppe auszuwählen, die dieser Workspace-Gruppe zugeordnet werden soll. Geben Sie im Textfeld einen Gruppennamen ein. Bei der Eingabe wird eine Liste mit Gruppennamen angezeigt. ■ Wählen Sie **Ist nicht**, um eine Gruppe auszuwählen, die von dieser Workspace-Gruppe ausgeschlossen werden soll. Geben Sie im Textfeld einen Gruppennamen ein. Bei der Eingabe wird eine Liste mit Gruppennamen angezeigt.
Attributregeln	Die folgenden Regeln gibt es für alle Attribute, einschließlich Standardattributen und aller zusätzlichen benutzerdefinierten Attribute, die von Ihrem Unternehmen konfiguriert wurden. E-Mail und Telefon sind Beispiele für Attribute. **Hinweis** Bei Regeln wird die Groß-/Kleinschreibung nicht beachtet. ■ Wählen Sie **Übereinstimmungen**, um Verzeichnisservereinträgen, die mit den von Ihnen eingegebenen Kriterien genau übereinstimmen, die Gruppenmitgliedschaft zu gewähren. Beispiel: Ihre Organisation hat möglicherweise eine Abteilung für Geschäftsreisen, bei der alle Mitarbeiter eine zentrale Telefonnummer teilen. Wenn Sie allen Mitarbeitern, die diese Telefonnummer teilen, den Zugriff auf eine Reisebuchungsanwendung gewähren möchten, können Sie eine Regel erstellen, z. B. „Telefon entspricht (555) 555-1000“. ■ Wählen Sie **Stimmt nicht überein**, um allen Verzeichnisservereinträgen mit Ausnahme der Einträge, die mit den von Ihnen eingegebenen Kriterien übereinstimmen, die Gruppenmitgliedschaft zu gewähren. Wenn beispielsweise alle Mitarbeiter einer Abteilung eine Telefonnummer teilen, können Sie für die Abteilung den Zugriff auf eine Social Network-Anwendung sperren, indem Sie eine Regel erstellen, z. B. „Telefon entspricht nicht (555) 555-2000“. Verzeichnisservereinträge mit anderen Telefonnummern können auf die Anwendung zugreifen. ■ Wählen Sie **Beginnt mit**, um Verzeichnisservereinträgen, die mit den von Ihnen eingegebenen Kriterien beginnen, die Gruppenmitgliedschaft zu gewähren. Beispiel: Die E-Mail-Adressen Ihrer Organisation beginnen mit dem Abteilungsnamen, z. B. vertrieb_benutzername@example.com. Wenn Sie allen Mitarbeitern des Vertriebs den Zugriff auf eine Anwendung gewähren möchten, können Sie eine Regel erstellen, z. B. „E-Mail beginnt mit vertrieb_“. ■ Wählen Sie **Beginnt nicht mit**, um allen Verzeichnisservereinträgen mit Ausnahme der Einträge, die mit den von Ihnen eingegebenen Kriterien beginnen, die Gruppenmitgliedschaft zu gewähren. Beispiel: Die E-Mail-Adressen der Personalabteilung weisen das Muster hr_benutzername@example.com. Sie können den Zugriff auf eine Anwendung sperren, indem Sie eine Regel einrichten, z. B. „E-Mail beginnt nicht mit hr_“. Verzeichnisservereinträge mit anderen E-Mail-Adressen können auf die Anwendung zugreifen.

Option	Aktion
Eine der folgenden Optionen	Die Gruppenmitgliedschaft wird gewährt, wenn für diese Regel mindestens eine der Voraussetzungen für die Gruppenmitgliedschaft erfüllt ist. Dies ist eine Möglichkeit, Regeln zu verschachteln. Beispiel: Sie können eine Regel erstellen, bei der alle der folgenden Bedingungen erfüllt werden müssen: Gruppe ist Vertrieb; Gruppe ist Kalifornien. Für „Gruppe ist Kalifornien“, eine der folgenden Bedingungen: Telefon beginnt mit 415; Telefon beginnt mit 510. Das Gruppenmitglied muss Mitarbeiter des Vertriebs in Kalifornien sein und seine Telefonnummer muss mit 415 oder 510 beginnen.
Alle der folgenden Optionen	Alle Bedingungen, die für diese Regel erfüllt werden müssen. Dies ist eine Möglichkeit, Regeln zu verschachteln. Sie können beispielsweise eine Regel erstellen, für die mindestens eine der folgenden Bedingungen erfüllt werden muss: Gruppe ist Manager; Gruppe ist Kundendienst. Für „Gruppe ist Kundendienst“, alle der folgenden Bedingungen: E-Mail beginnt mit cs_; Telefon beginnt mit 555. Die Gruppenmitglieder können entweder Manager oder Kundendienstmitarbeiter sein, dabei müssen jedoch die Kundendienstmitarbeiter eine E-Mail-Adresse haben, die mit „cs_“, und eine Telefonnummer, die mit „555“ beginnt.

8 (Optional) Geben Sie die einzelnen Benutzer an, die zu dieser Workspace-Gruppe hinzugefügt bzw. von ihr ausgeschlossen werden sollen, indem Sie das entsprechende Kontrollkästchen aktivieren und die Benutzernamen eingeben.

9 Klicken Sie auf **Weiter** und anschließend auf **Speichern**.

Workspace-Gruppeninformationen

Sie können detaillierte Informationen zu einer Gruppe, wie beispielsweise ihre berechtigten Ressourcen, ihre Mitgliedschaft und ihre angewandten mobilen Richtliniensätze, über Workspace Verwaltungskonsole anzeigen.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf **Benutzer und Gruppen > Gruppen**.

Die Seite zeigt eine Liste aller Gruppen in Ihrer Workspace-Bereitstellung mit einigen wichtigen Informationen über jede Gruppe an.

- Ein Kontrollkästchen neben dem Namen einer Gruppe gibt an, dass es sich um eine Workspace-Gruppe handelt. Sie definieren und verwalten Workspace-Gruppen innerhalb von Workspace.
- Ein Sperrsymbol neben einem Gruppennamen gibt an, dass es sich bei der Gruppe um eine Verzeichnisservergruppe handelt. Sie verwalten Verzeichnisservergruppen auf dem Verzeichnisserver Ihres Unternehmens.
- Die Seite zeigt die folgenden Informationen über jede Gruppe an.

Informationstyp	Beschreibung
Anzahl Benutzer	Die Anzahl der Benutzer in der Gruppe.
Anzahl Anwendungen	Die Anzahl der Ressourcen, für welche die Gruppe als Ganzes Berechtigungen hat.
Benutzerspeicher	Der Benutzerspeicher, mit der eine Active Directory-Gruppe verbunden ist. Wenn Workspace nicht in einer Active Directory-Umgebung mit mehreren Gesamtstrukturen bereitgestellt wurde, hat die Bereitstellung einen einzigen Benutzerspeicher mit der Bezeichnung „default“.

3 Klicken Sie auf den Namen einer Gruppe.

Die Detailseite der Gruppe wird mit dem Namen der Gruppe oben auf der Seite angezeigt.

4 Klicken Sie auf die Registerkarte, die den Informationen entspricht, die Sie anzeigen möchten.

Option	Beschreibung
Berechtigungen	Die Berechtigungsseite der Gruppe wird angezeigt. Auf dieser Seite können Sie Folgendes tun: ■ Anzeigen der Liste der Ressourcen, für die die Benutzer der Gruppe Berechtigungen haben. ■ Klicken Sie auf **Berechtigung hinzufügen**, um den Benutzern der Gruppe Berechtigungen für Ressourcen zu erteilen, die in Ihrem Katalog verfügbar sind. ■ Klicken Sie auf den Namen einer aufgelisteten berechtigten Ressource, um die Bearbeitungsseite dieser Ressource anzuzeigen. ■ Sie können für Ressourcentypen, die über eine **Bearbeiten**-Schaltfläche verfügen, auf diese Schaltfläche klicken, um den Benutzern der Gruppe Berechtigungen für Ressourcen dieses Typs zu erteilen bzw. zu entziehen oder um die Optionen für jede Ressource, für die die Benutzer Berechtigungen besitzen, zu ändern. Sie können auf der Seite „Berechtigungen“ die folgenden Änderungen durchführen: ■ Für Web-Anwendungen klicken Sie auf **Bearbeiten**, um die Berechtigung der Gruppe für die Web-Anwendungen oder den Typ der Bereitstellung für jede Web-Anwendung festzulegen, für die die Gruppe Berechtigungen besitzt. Wählen Sie **Automatisch** aus, wenn die Web-Anwendung standardmäßig im Benutzerportal angezeigt werden soll. Wählen Sie **Vom Benutzer aktiviert**, damit Benutzer die Web-Anwendung aus der Sammlung für sie verfügbarer Anwendungen im App Center zu ihrem Bereich „Meine Apps“ hinzufügen dürfen. ■ Bei View-Desktop- und -Anwendungspools können Sie die vorhandenen Berechtigungen der Gruppe für die in Ihr Workspace-System integrierten View-Pools anzeigen. Berechtigungen für View-Desktop- und -Anwendungspools werden in den View-Verbindungsserver-Instanzen konfiguriert, die in Ihr Workspace-System integriert sind. Sie können die Berechtigungen für View-Pools nicht über die Seite „Berechtigungen“ der Gruppe ändern. ■ Für ThinApp-Pakete klicken Sie auf **Bearbeiten**, um die Berechtigung der Gruppe für die ThinApp-Pakete oder den Typ der Bereitstellung für die ThinApp-Pakete, für die die Gruppe Berechtigungen besitzt, festzulegen. Wählen Sie **Automatisch** aus, wenn das ThinApp-Paket standardmäßig im Bereich „Meine Apps“ des Benutzerportals angezeigt werden soll. Wählen Sie **Vom Benutzer aktiviert** aus, um Benutzern zu ermöglichen, das ThinApp-Paket manuell aus dem App-Katalog zu ihrem Bereich „Meine Apps“ hinzuzufügen. ■ Bei mit Citrix veröffentlichten Anwendungen können Sie die vorhandenen Berechtigungen der Gruppe auf die in Ihr Workspace-System integrierten mit Citrix veröffentlichten Anwendungen anzeigen. Berechtigungen für mit Citrix veröffentlichte Anwendungen werden in den in Ihr Workspace-System integrierten Citrix-Bereitstellungen konfiguriert. Sie können die Berechtigungen für mit Citrix veröffentlichte Anwendungen nicht über die Seite „Berechtigungen“ der Gruppe ändern. ■ Bei Ressourcentypen, die über eine Schaltfläche **Berechtigung entziehen** verfügen, können Sie auf diese Schaltfläche klicken, um der Gruppe den Zugriff auf die Ressource zu sperren. **Hinweis** Die Spalte „Bereitstellungsstatus“ wird nicht verwendet. Standardmäßig ist die Anzeige der Spalte „Bereitstellungsstatus“ für die Tabellenreihen, die ausgefüllte Einträge auf dieser Seite haben, nicht aktiviert, und dieser Wert kann nicht geändert werden.
Benutzer in dieser Gruppe	Die Mitgliedschaftsseite der Gruppe wird angezeigt. Auf dieser Seite können Sie Folgendes tun: ■ Die Liste der Benutzer anzeigen, die zur Gruppe gehören.

Option	Beschreibung
	■ Auf den Namen eines Benutzers klicken, um die Detailseite dieses Benutzers anzuzeigen. ■ Klicken Sie auf **Benutzer in dieser Gruppe ändern**, um die Regeln anzuzeigen und zu konfigurieren, die die Mitgliedschaft in der Workspace-Gruppe definieren. Die Option **Benutzer in dieser Gruppe ändern** ist für Workspace-Gruppen verfügbar, aber nicht für Verzeichnisservergruppen.

Verwalten von Workspace -Benutzern

Sie können vom Active Directory importierte Benutzer über Workspace-Verwaltungskonsole verwalten.

Die Verwaltung von Benutzern in Workspace beinhaltet Aufgaben wie beispielsweise die Zuweisung der Benutzer zu Ressourcen, das Hinzufügen von Benutzern zu den entsprechenden Workspace-Gruppen und die Verwaltung des Status der bereitgestellten Arbeitsbereiche von Benutzern.

Workspace -Benutzerinformationen

Sie können detaillierte Informationen zu einem Benutzer wie beispielsweise berechtigte Ressourcen, Gruppenzugehörigkeiten und bereitgestellte Desktop-Systeme und mobile Endgeräte über Workspace-Verwaltungskonsole anzeigen.

Benutzerattribute befinden sich unter den Benutzerinformationen, die Sie anzeigen können, wie beispielsweise das Attribut des Hostnamens für Datenknoten und zusätzliche Attribute, dass Sie Workspace so konfiguriert haben, dass sie während der Synchronisierungen von Ihrem Verzeichnisserver abgerufen werden. Der Nutzen der Anzeige der zusätzlichen Verzeichnisserverattribute für einen einzelnen Benutzer hängt davon ab, wie Sie solche Attribute in Ihrer Bereitstellung verwenden. Sie können diese zusätzlichen Attribute folgendermaßen verwenden:

- Sie können die Mitgliedschaft einer Workspace-Gruppe ändern. Wenn Sie beispielsweise das Managerattribut in Active Directory verwenden, können Sie das Managerattribut auf Workspace abbilden. Sie können eine Gruppe erstellen, in der die Gruppenregeln die Mitgliedschaft auf Benutzer mit dem Managerattribut in ihrem Workspace-Benutzerdatensatz beschränken.
- Damit Benutzer Zugriff auf Web-Anwendungen mit bestimmten Attributsanforderungen haben. Beispielsweise könnte eine Finanzanwendung möglicherweise den Zugriff auf Benutzer mit dem Mitarbeiter-ID-Attribut in ihrem Workspace-Benutzerdatensatz beschränken.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Benutzer & Gruppen > Benutzer** aus.

Die Seite zeigt eine Liste all Ihrer Workspace-Benutzer.

3 Klicken Sie auf den Namen eines Benutzers.

Die Detailseite des Benutzers wird angezeigt. Der Name, die E-Mail-Adresse und die Rolle des Benutzers werden oben auf der Seite aufgelistet.

4 (Optional) Klicken Sie auf den Namen der angezeigten Rolle, also **Benutzer** oder **Administrator**, um die Rolle des Benutzers zu ändern.

Sie können Benutzer auf die Administratorrolle hochstufen und ihnen so ermöglichen, auf Workspace Verwaltungskonsole zuzugreifen. Einzelpersonen mit zugewiesener Administratorrolle können nach wie vor über das Internet als Benutzer auf ihr App-Portal zugreifen. Die URL für den Zugriff auf Verwaltungskonsole unterscheidet sich von der URL für den Zugriff auf das App-Portal.

Ersetzen Sie für die folgenden URLs den Platzhalter *WorkspaceFQDN* durch den tatsächlichen Wert.

Webschnittstelle	Erforderliche Rolle	URL-Beispiel
Workspace-Verwaltungskonsole	Administrator	https://*WorkspaceFQDN*/admin
Workspace App-Portal	Benutzer	https://*WorkspaceFQDN*/web

5 (Optional) Klicken Sie auf **Zusätzliche Attribute anzeigen**, um zusätzliche Attribute, die dem Benutzer zugewiesen sind, anzuzeigen. Dazu gehören beispielsweise Verzeichnisserverattribute.

6 Klicken Sie auf die Registerkarte, die den Informationen entspricht, die Sie anzeigen möchten.

Option	Beschreibung
Berechtigungen	Die Seite „Berechtigungen“ des Benutzers wird angezeigt. Auf dieser Seite können Sie Folgendes tun: ■ Anzeigen der Liste der Ressourcen, für die der Benutzer Berechtigungen hat. ■ Klicken Sie auf **Berechtigung hinzufügen**, um dem Benutzer Berechtigungen für in Ihrem Katalog verfügbare Ressourcen zu erteilen. ■ Klicken Sie auf den Namen einer aufgelisteten berechtigten Ressource, um die Bearbeitungsseite dieser Ressource anzuzeigen. ■ Sie können für Ressourcentypen, die über eine **Bearbeiten**-Schaltfläche verfügen, auf diese Schaltfläche klicken, um den Benutzern der Gruppe Berechtigungen für Ressourcen dieses Typs zu erteilen bzw. zu entziehen oder um die Optionen für jede Ressource, für die die Benutzer Berechtigungen besitzen, zu ändern. Sie können auf der Seite „Berechtigungen“ die folgenden Änderungen durchführen: ■ Für Web-Anwendungen klicken Sie auf **Bearbeiten**, um die Berechtigung des Benutzers für die Web-Anwendungen oder den Typ der Bereitstellung für jede Web-Anwendung festzulegen, für die der Benutzer Berechtigungen besitzt. Wählen Sie **Automatisch** aus, wenn die Web-Anwendung standardmäßig im Benutzerportal angezeigt werden soll. Wählen Sie **Vom Benutzer aktiviert**, damit der Benutzer die Web-Anwendung von der Sammlung für ihn verfügbarer Anwendungen im App Center zu seinem Bereich „Meine Apps“ hinzufügen darf. ■ Bei View-Desktop- und -Anwendungspools können Sie die vorhandenen Berechtigungen des Benutzers für die in Ihr Workspace-System integrierten View-Pools anzeigen. Berechtigungen für View-Desktop- und -Anwendungspools werden in den View-Verbindungsserver-Instanzen konfiguriert, die in Ihr Workspace-System integriert sind. Sie können die Berechtigungen für View-Pools nicht über die Seite „Berechtigungen“ des Benutzers ändern. ■ Für ThinApp-Pakete klicken Sie auf **Bearbeiten**, um die Berechtigungen des Benutzers für die ThinApp-Pakete oder den Typ der Bereitstellung für die ThinApp-Pakete, für die der Benutzer Berechtigungen besitzt, festzulegen. Wählen Sie **Automatisch** aus, wenn das ThinApp-Paket standardmäßig im Bereich „Meine Apps“ des Benutzerportals angezeigt werden soll. Wählen Sie **Vom Benutzer aktiviert** aus, um dem Benutzer zu ermöglichen, das ThinApp-Paket manuell aus dem App-Katalog zum Bereich „Meine Apps“ hinzuzufügen. ■ Bei mit Citrix veröffentlichten Anwendungen können Sie die vorhandenen Berechtigungen des Benutzers auf die in Ihr Workspace-System integrierten mit Citrix veröffentlichten Anwendungen anzeigen. Berechtigungen für mit Citrix veröffentlichte Anwendungen werden in den in Ihr Workspace-System integrierten Citrix-Bereitstellungen konfiguriert. Sie können die Berechtigungen für mit Citrix veröffentlichte Anwendungen nicht über die Seite „Berechtigungen“ des Benutzers ändern. ■ Bei Ressourcentypen, die über eine Schaltfläche **Berechtigung entziehen** verfügen, können Sie auf diese Schaltfläche klicken, um dem Benutzer den Zugriff auf die Ressource zu sperren. **Hinweis** Die Spalte „Bereitstellungsstatus“ wird nicht verwendet. Standardmäßig ist die Anzeige der Spalte „Bereitstellungsstatus“ für die Tabellenreihen, die ausgefüllte Einträge auf dieser Seite haben, nicht aktiviert, und dieser Wert kann nicht geändert werden.
Gruppenzugehörigkeiten	Es wird eine Liste der Gruppen angezeigt, zu denen der Benutzer gehört. Jeder Gruppenname steht für eine Gruppe, bei der der Benutzer Mitglied ist. Sie können auf den Namen einer Gruppe klicken, um die Detailseite für diese Gruppe anzuzeigen.
Arbeitsbereiche	Die Seite „Arbeitsbereiche“ des Benutzers wird angezeigt. Auf dieser Seite können Sie die Desktop-Arbeitsbereiche anzeigen, die auf den Desktop-

Option	Beschreibung
	Systemen der Benutzer bereitgestellt wurden, einschließlich des jeweiligen Status der einzelnen Arbeitsbereiche. ■ Wenn Sie für ein Desktop-System auf **Löschen** klicken, wird das entsprechende System aus Workspace entfernt. Auf diese Weise können Sie z. B. verloren gegangene, gestohlene oder nicht mehr verwendete Systeme aus Workspace entfernen.

Ändern von Benutzern und Gruppen, die aus Active Directory synchronisieren

Während des Einrichtens von Workspace haben Sie die Informationen für die Verbindung mit dem Active Directory-Server eingegeben, Active Directory-Benutzerattribute und Filter ausgewählt, um festzulegen, welche Benutzer im Workspace-Verzeichnis synchronisiert sind, und ausgewählt, welche Active Directory-Gruppen hinzugefügt werden sollen. Sie können diese Einstellungen in Connector Services-Administratorauf den Seiten von „Verzeichnissynchronisierung“ ändern.

Auf diesen Seiten durchgeführte und gespeicherte Seiten werden nach der nächsten Verzeichnissynchronisierung automatisch in Workspace aktualisiert. Weitere Informationen hierzu finden Sie unter „Ändern von Einstellungen, die Benutzer für Workspace auswählen“, auf Seite 44

Ändern der Seite „Benutzerattribute zuordnen“

Die Seite „Benutzerattribute zuordnen“ zeigt die Zuordnung von Attributen in Active Directory und Attributen in Workspace. Wenn Sie zusätzliche Informationen aus Active Directory über Benutzer hinzufügen möchten, können Sie die Benutzerattribute auf der Seite „Benutzerattribute zuordnen“ hinzufügen.

Eines der Standard-Benutzerattribute, die auf der Seite „Benutzerattribute zuordnen“ zugeordnet werden, ist das Attribut zum Deaktivieren eines Kontos. Das Attribut „UserAccountControl“ wird dem Attribut „Workspace deaktiviert“ zugeordnet. Benutzer werden im Workspace-Verzeichnis deaktiviert, wenn das Active Directory-Attribut UserAccountControl auf UF_Account_Disable gesetzt ist.

Wenn ein Konto deaktiviert ist, können sich Benutzer nicht mehr anmelden, um auf ihre Anwendungen und Ressourcen zuzugreifen. Die Ressourcen, für deren Nutzung die Benutzer berechtigt sind, werden aus dem Konto nicht entfernt. Wenn die Deaktivierungsmarkierung vom Konto entfernt wird, können sich Benutzer wieder anmelden und auf die Ressourcen zugreifen, für die sie Berechtigungen haben.

Ändern von Einstellungen, die Benutzer für Workspace auswählen

Während des Workspace-Setups geben Sie das Active Directory, Benutzerattribute und Filter zur Auswahl der Active Directory-Benutzer an, die Sie mit Workspace verwenden möchten. Sie können diese Einstellungen über die Connector Services-Administrator-Seiten aktualisieren.

Voraussetzungen

Stellen Sie sicher, dass Sie über die erforderlichen Informationen für die gewünschten Änderungen verfügen, z. B. den neuen Basis-DN, die einzuschließenden Benutzerattribute, die einzuschließenden Gruppen usw.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator mit dem Workspace-Administratorkennwort an.

2 Führen Sie die entsprechende Aktion aus.

Option	Aktion
Ändern Sie die Active Directory-Serverinformationen, z. B. den Server-Host, den Port, den Basis-DN, den Bind-DN, das Bind-Kennwort usw.	a Klicken Sie auf **Verzeichnis**. b Nehmen Sie Ihre Änderungen vor. c Klicken Sie auf **Speichern**.
Ändern Sie die Zuordnung zwischen den Workspace-Benutzerattributen und den Active Directory-Benutzerattributen.	a Klicken Sie auf **Benutzerattribute zuordnen**. b Nehmen Sie Ihre Änderungen vor. c Klicken Sie auf **Speichern**.
Erstellen Sie Filter, um bestimmte Active Directory-Benutzer von der Synchronisierung mit Workspace auszuschließen, und aktualisieren Sie Active Directory-Gruppen, die mit Workspace synchronisiert sind.	a Klicken Sie auf **Verzeichnissynchronisierung**. b Klicken Sie auf **Regeln für die Verzeichnissynchronisierung bearbeiten**. c Nehmen Sie die gewünschten Änderungen auf der Seite „Benutzer auswählen“ vor und klicken Sie auf **Speichern**. d Nehmen Sie die gewünschten Änderungen auf der Seite „Gruppen auswählen“ vor und klicken Sie auf **Speichern**. e Klicken Sie auf **An Workspace weitergeben**. f Klicken Sie auf **Speichern und fortsetzen**.

Verwalten des Workspace -Katalogs 7

Ihr Workspace-Katalog ist das Repository aller Ressourcen, für die Benutzern Berechtigungen erteilt werden können. Die Verfügbarkeit von bestimmten Ressourcentypen in Ihrem Katalog wird von den Modulen gesteuert, die in Ihrem Workspace-System aktiviert sind.

Um den Katalog anzuzeigen, klicken Sie im Workspace Verwaltungskonsole auf die Registerkarte **Katalog**. Sie können auf der Seite „Katalog“ die folgenden Aufgaben ausführen:

- Hinzufügen von neuen Ressourcen zu Ihrem Katalog
- Anzeigen der Ressourcen, für die Sie zurzeit Benutzern Berechtigungen erteilen können
- Abrufen von Informationen zu jeder Ressource in Ihrem Katalog

Je nach Typ können manche Ressourcen über die Seite „Katalog“ direkt Ihrem Katalog hinzugefügt werden. Für andere Ressourcentypen müssen Sie Maßnahmen außerhalb von Verwaltungskonsole ergreifen. Informationen zum Einrichten von Ressourcen finden Sie im *Setting Up Resources in VMware Workspace Portal Guide*.

Ressource	Ressource in Ihrem Katalog anzeigen
Web-Anwendung	Aktivieren Sie das Web-Anwendungsmodul. Verwenden Sie Verwaltungskonsole, um auf der Seite „Katalog“ den Anwendungstyp **Webanwendungen** auszuwählen.
Virtualisierte Windows-Anwendung, die als ThinApp-Paket erfasst wurde	Auf der Connector Services-Administrator-Seite „App-Pakete - ThinApp“ können Sie ThinApp-Pakete mit dem Katalog synchronisieren. Verwenden Sie Verwaltungskonsole, um auf der Seite „Katalog“ den Anwendungstyp **ThinApp-Pakete** auszuwählen.
View-Desktop-Pool	Auf der Connector Services-Administrator-Seite „View-Pools“ können Sie View-Pools mit dem Katalog synchronisieren. Verwenden Sie Verwaltungskonsole, um auf der Seite „Katalog“ den Anwendungstyp **View-Desktop-Pools** auszuwählen.
Gehostete View-Anwendungen	Auf der Connector Services-Administrator-Seite „View-Pools“ können Sie gehostete View-Anwendungen mit dem Katalog synchronisieren. Verwenden Sie Verwaltungskonsole, um auf der Seite „Katalog“ den Anwendungstyp **Gehostete View-Anwendungen** auszuwählen.
Citrix-basierte Anwendung	Auf der Connector Services-Administrator-Seite „Veröffentlichte Apps - Citrix“ können Sie Citrix-basierte Anwendungen mit dem Katalog synchronisieren. Verwenden Sie Verwaltungskonsole, um auf der Seite „Katalog“ den Anwendungstyp **Mit Citrix veröffentlichte Anwendungen** auszuwählen.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht über Workspace-Ressourcentypen“, auf Seite 48
- „Übersicht über die Verwendung von Ressourcenkategorien“, auf Seite 49
- „Zugriff auf Workspace-Ressourcen“, auf Seite 51

- „Hinzufügen von Ressourcen zu Ihrem Katalog“, auf Seite 52

Übersicht über Workspace -Ressourcentypen

Zu den Arten von Ressourcen, die Sie in Ihrem Katalog für Berechtigungen und Verteilungen an Benutzer definieren können, gehören Web-Anwendungen, als VMware ThinApp-Pakete erfasste Windows-Anwendungen, Citrix-basierte Anwendungen, VMware View-Desktop-Pools und gehostete View-Anwendungen.

Bevor Sie Ihren Benutzern Berechtigungen für eine bestimmte Ressource erteilen können, müssen Sie diese Ressource in Ihren Katalog aufnehmen. Die Methode, die Sie zum Aufnehmen einer Ressource in Ihren Katalog verwenden, hängt vom Typ der Ressource ab.

Informationen zu diesen Ressourcen, insbesondere zu den Anforderungen, zu ihrer Installation und Konfiguration finden Sie im *Setting Up Resources in VMware Workspace Portal Guide*

Web-Anwendungen

Sie können Web-Anwendungen direkt auf der Seite „Katalog“ von Workspace Verwaltungskonsole in den Katalog aufnehmen. Wenn Sie auf der Seite „Katalog“ auf eine Web-Anwendung klicken, werden Informationen zur Anwendung angezeigt. Sie können die Web-Anwendung von der angezeigten Seite aus konfigurieren, zum Beispiel durch Angabe der entsprechenden SAML-Attribute, um Single Sign On zwischen Workspace und der Ziel-Web-Anwendung zu konfigurieren. Wenn die Web-Anwendung konfiguriert ist, können Sie dann Benutzern und Gruppen die Berechtigung für diese Web-Anwendung erteilen. Siehe „Hinzufügen von Ressourcen zu Ihrem Katalog“, auf Seite 52.

ThinApp-Pakete

Sie können Windows-Anwendungen, die als ThinApp-Pakete erfasst wurden, in Ihren Katalog aufnehmen, indem Sie die folgenden Aufgaben ausführen.

1. Falls die ThinApp-Pakete, für die Sie Benutzern den Zugriff gewähren möchten, nicht bereits vorhanden sind, erstellen Sie ThinApp-Pakete, die mit Workspace kompatibel sind. Weitere Informationen hierzu finden Sie in der VMware ThinApp-Dokumentation.
2. Erstellen Sie eine Netzwerkfreigabe und bestücken Sie sie mit den kompatiblen ThinApp-Paketen.
3. Konfigurieren Sie Workspace so, dass das Programm in die Pakete der Netzwerkfreigabe integriert ist.

Nach Ausführung dieser Aufgaben stehen die virtualisierten Windows-Anwendungen – die ThinApp-Pakete, die Sie zur Netzwerkfreigabe hinzugefügt haben – als Ressourcen in Ihrem Katalog zur Verfügung. Sie können dann Benutzern die Berechtigung für diese Ressourcen erteilen.

Um die von Workspace verteilten und verwalteten ThinApp-Pakete zu starten und auszuführen, muss auf den Windows-Systemen der Benutzer Workspace für Windows installiert sein.

Mit Citrix veröffentlichte Anwendungen

Sie können Citrix-basierte Anwendungen in Ihren Katalog aufnehmen, indem Sie die folgenden Aufgaben ausführen.

1. Stellen Sie Citrix-Server bereit (sofern nicht bereits ausgeführt) und erteilen Sie den Benutzern Berechtigungen für Citrix-basierte Anwendungen. Weitere Informationen hierzu finden Sie in der Citrix-Dokumentation.
2. Integrieren Sie die Bereitstellung von Workspace in die Citrix-Server.

Nach der Durchführung dieser Aufgaben stehen die Citrix-basierten Anwendungen, deren Berechtigungen Sie Benutzern mit Citrix-Servern erteilt haben, als Ressourcen im Katalog zur Verfügung.

View -Desktop-Pools

Sie können Ihren Katalog mit View-Desktop-Pools und den entsprechenden View-Desktops füllen, indem Sie folgende Aufgaben ausführen.

1 Sofern nicht bereits ausgeführt, stellen Sie die View-Desktop-Pools in VMware View bereit, wozu auch das Erteilen der Berechtigungen für Desktops an die Benutzer gehört. Weitere Informationen hierzu finden Sie in der Dokumentation zu VMware View.

2 Integrieren Sie die Bereitstellung von Workspace in VMware View.

Nach der Durchführung dieser Aufgaben stehen die View-Desktops, für die Sie Berechtigungen für Benutzer in VMware View erteilt haben, als Ressourcen in Ihrem Katalog zur Verfügung.

Gehostete View -Anwendungen

Sie können gehostete View-Anwendungspools in Ihren Katalog aufnehmen, indem Sie die folgenden Aufgaben ausführen:

1 Stellen Sie sicher, dass Anwendungspools in View als Remote-Desktop-Dienst bereitgestellt werden. Weitere Informationen hierzu finden Sie in der Dokumentation zu View.

2 Integrieren Sie die Bereitstellung von Workspace in View.

Nach der Durchführung dieser Aufgaben stehen die gehosteten Anwendungspools, für die Sie Berechtigungen für Benutzer in View erteilt haben, als Ressourcen in Ihrem Katalog zur Verfügung.

Übersicht über die Verwendung von Ressourcenkategorien

Die Standardmethode zum Suchen nach Katalogressourcen ist nach Ressourcentyp. Sie können nach Kategorie suchen.

Um eine Suche von Workspace-Katalogressourcen nach Kategorie zu aktivieren, erstellen Sie Kategorien und wenden sie auf Ressourcen an.

Erstellen einer Ressourcenkategorie

Sie können eine Workspace-Ressourcenkategorie hinzufügen, ohne sie sofort anzuwenden; Sie können aber auch eine Kategorie erstellen und sie gleichzeitig anwenden.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Katalog**.

3 Aktivieren Sie das Kontrollkästchen einer oder mehrerer Ressourcen.

Durch eine aktivierte Ressource wird die Schaltfläche **Kategorien anwenden** aktiviert. Dies ist Voraussetzung für das Erstellen einer Kategorie. Um Kategorien zu erstellen und gleichzeitig anzuwenden, klicken Sie auf die Kontrollkästchen aller Ressourcen, auf die die neue Kategorie angewendet werden soll. Wenn Sie eine Kategorie erstellen möchten, ohne sie sofort anzuwenden, macht die ausgewählte Ressource keinen Sinn. In dieser Situation können Sie auf das Kontrollkästchen einer beliebigen Ressource im Katalog klicken.

4 Klicken Sie auf **Kategorien anwenden**.

5 Geben Sie einen neuen Kategorienamen im Textfeld **Kategorien suchen** ein.

6 Klicken Sie auf **Kategorie hinzufügen...**.

Workspace erstellt die neue Kategorie, wendet sie jedoch nicht an.

7 (Optional) Um die Kategorie auf die ausgewählten Ressourcen anzuwenden, klicken Sie auf das Kontrollkästchen für den neuen Kategorienamen.

Workspace wendet die Kategorie auf die ausgewählten Ressourcen an.

Weiter

Wenden Sie, falls zutreffend, die Kategorie auf Ressourcen an. Siehe „Anwenden einer Kategorie auf Ressourcen“, auf Seite 50.

Anwenden einer Kategorie auf Ressourcen

Nachdem Sie eine Kategorie erstellt haben, können Sie diese Kategorie auf alle Ressourcen im Katalog anwenden.

Voraussetzungen

Erstellen Sie eine Ressourcen-Kategorie.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Katalog**.

3 Aktivieren Sie die Kontrollkästchen aller Ressourcen, auf die Sie die Kategorie anwenden möchten.

4 Klicken Sie auf **Kategorien anwenden** und wählen Sie den Namen der Kategorie, die Sie anwenden möchten.

Die Kategorie wird auf die ausgewählten Kategorien angewendet.

Entfernen oder Löschen einer Kategorie

Sie können die Zuweisung einer Kategorie zu einer Ressource aufheben und eine Kategorie dauerhaft aus dem Katalog entfernen.

Sie können die Kategoriebezeichnung entfernen, um die Zuweisung der Kategorie zur Ressource aufzuheben. Sie können die Kategorie auch dauerhaft aus dem Katalog löschen. Wenn Sie eine Kategorie dauerhaft löschen, wird diese aus dem Katalog entfernt. Sie wird nicht mehr im Dropdown-Menü **Beliebige Kategorie** oder als Bezeichnung zu einer Ressource angezeigt, auf die Sie sie vorher angewendet hatten.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Katalog**.

3 Aktivieren Sie das Kontrollkästchen einer oder mehrerer Ressourcen.

Durch eine aktivierte Ressource wird die Schaltfläche **Kategorien anwenden** aktiviert. Dies ist Voraussetzung für das Entfernen und Löschen einer Kategorie. Um eine Kategoriebezeichnung aus einer oder mehreren Ressourcen zu entfernen, aktivieren Sie die Kontrollkästchen aller Ressourcen, von denen die Kategoriebezeichnung entfernt werden soll. Falls Sie eine Kategorie dauerhaft löschen möchten, macht die ausgewählte Ressource keinen Sinn. In dieser Situation können Sie auf das Kontrollkästchen einer beliebigen Ressource im Katalog klicken.

4 Klicken Sie auf **Kategorien anwenden**.

Option	Beschreibung
Kategorie von Ressourcen entfernen	Das Kontrollkästchen der Bezeichnung ist ausgewählt. Klicken Sie auf dieses Kontrollkästchen, um die Kategoriebezeichnung von der ausgewählten Ressource zu entfernen.
Kategorie dauerhaft löschen	Bewegen Sie die Maus über die Kategorie. Es wird ein „X“-Symbol angezeigt. Klicken Sie auf dieses Symbol, um die Kategorie dauerhaft aus dem Katalog zu entfernen.

Zugriff auf Workspace -Ressourcen

Greifen Sie auf den Katalog zu, um Informationen zu den Ressourcen anzuzeigen, für die Sie Benutzern Berechtigungen erteilen können, wie beispielsweise zu Workspace-Web-Anwendungen, ThinApp-Paketen, Citrix-basierten Anwendungen und View-Desktop-Pools. Sie können Ressourcen nach Anwendungstyp oder nach Kategorie anzeigen lassen.

Voraussetzungen

- Aktivieren Sie die Ressourcenmodule, die zu den Ressourcentypen gehören, für die Sie Benutzern Berechtigungen erteilen möchten. Das Modul „Web-Anwendungen“, das Modul „Mobiles Management“, das View-Modul, das Modul „ThinApp-Pakete“ und das Modul „Mit Citrix veröffentlichte Anwendungen“ sind verfügbar.
- Fügen Sie Ressourcen zum Katalog hinzu, um den Bedürfnissen Ihres Unternehmens gerecht zu werden. Siehe Kapitel 7, „Verwalten des Workspace-Katalogs“, auf Seite 47.
- Um Ressourcen nach Anwendung anzuzeigen, erstellen und wenden Sie Kategorien an. Siehe „Übersicht über die Verwendung von Ressourcenkategorien“, auf Seite 49.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Katalog**.

Workspace führt alle Ressourcen im Katalog auf.

3 (Optional) Um die Sortierungsmethode zu ändern, klicken Sie auf **Anwendung** oder **Anwendungstyp**.

4 (Optional) Um Ressourcen nach einem bestimmten Typ anzeigen zu lassen, wählen Sie einen Ressourcentyp aus dem Dropdown-Menü **Jeder Anwendungstyp** aus.

Anwendungstypen, die Sie nicht zu Workspace hinzugefügt haben, werden im Dropdown-Menü nicht angezeigt.

Option	Beschreibung
Jeder Anwendungstyp	Listet alle Ressourcen in Ihrem Katalog auf.
Web-Anwendungen	Listet nur Web-Anwendungen in Ihrem Katalog auf. Web-Anwendungen beinhalten SaaS-Anwendungen und Web-Anwendungen, die intern von Ihrem Unternehmen verwaltet werden.
ThinApp-Pakete	Listet nur Windows-Anwendungen auf, die als ThinApp-Pakete erfasst sind. ThinApp-Pakete werden in Ihrem Katalog angezeigt, wenn Sie sie während der Konfiguration von Workspace zu Ihrer Bereitstellung hinzufügen, bevor Sie auf Verwaltungskonsole zugreifen.
Desktop-Pools anzeigen	Listet nur die View-Desktop-Pools auf. View-Desktop-Pools werden in Ihrem Katalog angezeigt, wenn Sie Workspace in VMware View integrieren, bevor Sie auf Workspace-Verwaltungskonsole zugreifen.

Option	Beschreibung
Gehostete View-Anwendungen	Listet nur die gehosteten View-Anwendungen auf. Gehostete View-Anwendungen werden in Ihrem Katalog angezeigt, wenn Sie Workspace in View integrieren, bevor Sie auf Verwaltungskonsole zugreifen.
Mit Citrix veröffentlichte Anwendungen	Listet nur Citrix-basierte Anwendungen auf. Citrix-basierte Anwendungen werden im Katalog angezeigt, wenn Sie Workspace mit Ihrer Citrix-Bereitstellung vor dem Zugriff auf Verwaltungskonsole integrieren.

5 (Optional) Um Ressourcen nach einer bestimmten Kategorie anzeigen zu lassen, wählen Sie eine oder mehrere Kategorienamen aus dem Dropdown-Menü **Jede Kategorie** aus.

Workspace führt alle Ressourcen auf, die den von Ihnen gewählten Kriterien entsprechen.

- Wenn Sie eine Kategorie wählen, führt Workspace alle Kategorien auf, die mit dieser Kategoriebezeichnung markiert sind.
- Wenn Sie mehr als eine Kategorie wählen, führt Workspace nur Kategorien mit allen dieser Kategoriebezeichnungen auf.

6 Klicken Sie auf das Symbol für eine bestimmte Ressource, um die Details zu dieser Ressource anzuzeigen.

Hinzufügen von Ressourcen zu Ihrem Katalog

Über die Seite „Katalog“ von WorkspaceVerwaltungskonsole können Web-Anwendungen direkt dem Katalog hinzugefügt werden.

Detaillierte Anleitungen zum Hinzufügen einer Web-Anwendung zu Ihrem Katalog finden Sie im Kapitel „Gewähren des Zugriffs auf Web-Anwendungen“ in der Dokumentation „Einrichten von Ressourcen in VMware Workspace Portal“.

Die folgenden Anweisungen bieten eine Übersicht über die Schritte zum Hinzufügen dieser Ressourcentypen zu Ihrem Katalog.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Klicken Sie auf die Registerkarte **Katalog**.

3 Klicken Sie auf **+ Anwendung hinzufügen**.

4 Klicken Sie abhängig vom Ressourcentyp und Speicherort der Anwendung auf eine Option. Beim Importieren eines Android-Arbeitsbereichs-Images müssen Sie in diesem Schritt nicht auf eine Option klicken.

Link Name	Ressourcentyp	Beschreibung
Web-Anwendung ... Aus dem Cloud-Anwendungskatalog	Web-Anwendung	Workspace bietet Zugriff auf mehrere, im Cloud-Anwendungskatalog verfügbare Standard-Web-Anwendungen, die Sie Ihrem Katalog als Ressource hinzufügen können.
Web-Anwendung ... Neue erstellen	Web-Anwendung	Durch Ausfüllen des entsprechenden Formulars können Sie einen Anwendungsdatensatz für die Web-Anwendungen erstellen, die Sie als Ressourcen Ihrem Katalog hinzufügen möchten.
Web-Anwendung ... ZIP- oder JAR-Datei importieren	Web-Anwendung	Sie können eine Web-Anwendung importieren, die Sie zuvor in Workspace konfiguriert haben. Sie können diese Methode verwenden, um für die Workspace-Bereitstellung ein Rollout von der Einstufung zur Produktion vorzunehmen. Exportieren Sie in solch einer Situation eine Web-Anwendung von der Einstufungsbereitstellung als ZIP-Datei. Importieren Sie dann die ZIP-Datei in die Produktionsbereitstellung.

5 Folgen Sie den Anweisungen, um das Hinzufügen von Ressourcen zum Katalog abzuschließen.

Suchen nach Benutzern, Gruppen oder Katalogressourcen

8

Im Textfeld der Suche in Workspace-Verwaltungskonsole können Sie nach Workspace-Benutzern, -Gruppen oder -Ressourcen in Ihrem Katalog suchen.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Geben Sie eine Zeichenfolge in das Textfeld für die Suche ein.

   Um z. B. alle Benutzer mit der E-Mail-Adresse meinefirma.com zu suchen, geben Sie **`meinefirma.com`** ein.

Auf der Seite mit den Suchergebnissen werden die gefundenen Ergebnisse entsprechend den folgenden Regeln auf drei Registerkarten angezeigt:

Registerkarte Benutzer	Die eingegebene Zeichenfolge stimmt mit den ersten Zeichen eines beliebigen Worts innerhalb des Vornamens, Nachnamens oder Prinzipalnamens eines Workspace-Benutzers überein.
Registerkarte Gruppen	Die eingegebene Zeichenfolge stimmt mit den ersten Zeichen eines beliebigen Worts innerhalb des Namens oder der Beschreibung der Gruppe überein.
Registerkarte Katalog	Die eingegebene Zeichenfolge stimmt mit den ersten Zeichen eines beliebigen Worts innerhalb des Namens oder der Beschreibung der Katalogressource überein.

HINWEIS Bis zu 100 Ergebnisse werden für jeden Datensatztyp ausgegeben. Wenn also eine Zeichenfolge in den Datensätzen von über 100 Benutzern vorkommt, werden maximal 100 Ergebnisse auf der Registerkarte **Benutzer** aufgeführt. Sie können diesen Höchstwert nicht ändern.

Anzeigen von Workspace -Berichten 9

Workspace erzeugt verschiedene Berichte wie beispielsweise Berichte zu Benutzern, Ressourcen und Überwachungsereignissen. Sie können die Berichte auf der Registerkarte **Berichte** von Workspace-Verwaltungskonsole anzeigen.

Sie können mit Workspace unterschiedliche Berichte generieren.

Tabelle 9-1. Workspace -Berichtstypen

Workspace-Bericht	Beschreibung
Aktuelle Aktivitäten	Dieser Bericht listet auf, welche Aktionen der Benutzer am vergangenen Tag, im letzten Monat oder in den letzten 12 Wochen in Workspace ausgeführt hat. Sie können auf **Ereignisse anzeigen** klicken, um Datum, Uhrzeit und Benutzerdaten für die jeweilige Aktivität anzuzeigen.
Ressourcennutzung	Dieser Bericht listet all Ihre Ressourcen mit entsprechenden Details zu jeder Ressource auf, zum Beispiel Anzahl der Benutzer und Lizenzen.
Ressourcenberechtigungen	Dieser Bericht listet die Benutzerberechtigungen für eine von Ihnen angegebene Ressource auf.
Gruppenmitgliedschaft	Dieser Bericht listet die Mitglieder einer von Ihnen angegebenen Gruppe auf.
Benutzer	Dieser Bericht listet all Ihre Workspace-Benutzer auf und liefert Details zu jedem Benutzer wie beispielsweise die E-Mail-Adresse, die Rolle und die Gruppenzugehörigkeiten des Benutzers.
Gleichzeitige Benutzer	Dieser Bericht listet die Anzahl der Benutzersitzungen auf, die zur gleichen Zeit geöffnet wurden.
Überwachungsereignisse	Dieser Bericht listet die Überwachungsereignisse bezüglich einer von Ihnen angegebenen Suche auf, wie beispielsweise Benutzeranmeldungen der letzten 30 Tage. Diese Funktion ist für die Fehlerbehebung nützlich. Siehe „Generieren eines Audit-Ereignisberichts“, auf Seite 57.

Generieren eines Audit-Ereignisberichts

Sie können einen Bericht zu Überwachungsereignissen generieren, die Sie angeben.

Berichte zu Audit-Ereignissen können als Methode zur Fehlerbehebung nützlich sein.

Voraussetzungen

Aktivieren Sie die Überwachung. Siehe „Übersicht über administrative Einstellungen in Workspace“, auf Seite 59.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Berichte > Überwachungsereignisse**

3 Wählen Sie Kriterien für Überwachungsereignisse.

Kriterien für Überwachungsereignisse	Beschreibung
Benutzer	Mit diesem Textfeld können Sie die Suche nach Überwachungsereignissen auf Ereignisse einschränken, die von einem bestimmten Benutzer generiert wurden.
Typ	Mit dieser Dropdown-Liste können Sie die Suche nach Überwachungsereignissen auf einen bestimmten Überwachungsereignistyp eingrenzen. Die Dropdown-Liste zeigt nicht alle potenziellen Überwachungsereignistypen an. Die Liste zeigt nur Ereignistypen an, die in Ihrer Workspace-Bereitstellung aufgetreten sind. Überwachungsereignistypen, die mit Großbuchstaben aufgelistet sind, sind Zugriffsereignisse, wie beispielsweise LOGIN und LAUNCH, die keine Änderungen in der Datenbank generieren. Andere Überwachungsereignistypen generieren Änderungen in der Datenbank.
Aktion	Mit dieser Dropdown-Liste können Sie Ihre Suche nach bestimmten Aktionen eingrenzen. Die Liste zeigt Ereignisse an, die bestimmte Änderungen in der Datenbank hervorrufen. Wenn Sie ein Zugriffsereignis in der Dropdown-Liste „Typ“ auswählen (Ereignis ohne Aktion), geben Sie keine Aktion in der Dropdown-Liste „Aktion“ an.
Objekt	Mit diesem Textfeld können Sie die Suche nach einem bestimmten Objekt eingrenzen. Beispiele von Objekten sind Gruppen, Benutzer und Geräte. Objekte werden durch einen Namen oder eine ID-Nummer identifiziert.
Datumsbereich	Mit diesen Textfeldern können Sie Ihre Suche auf einen Datumsbereich im Format „Von vor ___ Tagen bis vor ___ Tagen“ eingrenzen. Der maximale Datumsbereich ist 30 Tage. Von vor 90 Tagen bis vor 60 Tagen ist z. B. ein gültiger Zeitraum, während von vor 90 Tagen bis vor 45 Tagen ein ungültiger Zeitraum ist, weil er den Höchstwert von 30 Tagen überschreitet.

4 Klicken Sie auf **Anzeigen**.

Ein Bericht zu Audit-Ereignissen wird gemäß den von Ihnen angegebenen Kriterien angezeigt.

HINWEIS Beim Neustart des Überwachungssubsystems kann es mitunter vorkommen, dass auf der Überwachungsereignisseite eine Fehlermeldung ausgegeben und der Bericht nicht korrekt angezeigt wird. Warten Sie bei Ausgabe dieser Fehlermeldung einige Minuten, und versuchen Sie es dann erneut.

5 Um weitere Informationen zu einem Überwachungsereignis anzuzeigen, klicken Sie für dieses Überwachungsereignis auf **Details anzeigen**.

Konfigurieren der Workspace - Einstellungen für Administratoren 10

Nachdem Sie Workspace installiert und die Erstkonfiguration durchgeführt haben, können Sie verschiedene administrative Einstellungen konfigurieren.

Dieses Kapitel behandelt die folgenden Themen:

- „Übersicht über administrative Einstellungen in Workspace“, auf Seite 59
- „Anpassen des Workspace-Brandings“, auf Seite 60

Übersicht über administrative Einstellungen in Workspace

Sie können verschiedene administrative Einstellungen in Workspace konfigurieren.

Sie greifen über Workspace-Verwaltungskonsole auf die administrativen Einstellungen zu.

Einstellung	Beschreibung
VA-Konfiguration	Wählen Sie **Einstellungen > VA-Konfiguration**aus, um die Seiten von Appliance Configurator aufzurufen. Auf diesen Seiten können Sie Einstellungen für die Workspace-Datenbank, SSL-Zertifikate sowie externe Syslog-Server aktualisieren und ändern, Workspace- und Systemkennwörter ändern und Protokolldateien anzeigen.
Lizenz	Wählen Sie **Einstellungen > Lizenz** aus, um den Workspace-Lizenzschlüssel einzugeben.
SMTP	Wählen Sie **Einstellungen > SMTP** aus, um die SMTP-Einstellungen einzugeben.
Kennwortwiederherstellung	Wählen Sie **Einstellungen > Kennwortwiederherstellung**, um festzulegen, was bei einem Klick auf den Link „Kennwort vergessen“ geschieht, der im Benutzerprotokoll auf der Seite erscheint, auf der der Benutzer auf „Kennwort vergessen“ geklickt hat.
Benutzerspeicher	Wählen Sie **Einstellungen > Benutzerspeicher** aus, um Benutzerspeicher für Active Directory-Multistrukturbereitstellungen mit Vertrauensverhältnissen zu konfigurieren. Siehe das Kapitel „Verwalten von Active Directory-Verbindungen mit Workspace“ im *Installieren und Konfigurieren von Workspace*-Handbuch.
Netzwerkbereiche	Wählen Sie **Einstellungen > Netzwerkbereiche**, um Netzwerkbereiche für Ihre Organisation zu konfigurieren, sodass Sie IP-Adressenbereiche mit den Identitätsanbieter-Instanzen verknüpfen können. Siehe „Hinzufügen oder Bearbeiten eines Netzwerkbereichs“, auf Seite 17.
Authentifizierungsmethoden	Wählen Sie **Einstellungen > Authentifizierungsmethoden**, um die Standard-Authentifizierungsmethoden zu konfigurieren oder Authentifizierungsmethoden hinzuzufügen, die nicht direkt von Workspace unterstützt werden, die jedoch indirekt durch externe Identitätsanbieter unterstützt werden. Siehe „Hinzufügen oder Bearbeiten einer Benutzerauthentifizierungsmethode“, auf Seite 18.

Einstellung	Beschreibung
Identitätsanbieter	Wählen Sie **Einstellungen > Identitätsanbieter**, um eine vorhandene Identitätsanbieter-Instanz zu bearbeiten oder eine neue Identitätsanbieter-Instanz hinzuzufügen. Die erste Installation von Workspace enthält eine Standard-Identitätsanbieter-Bereitstellung. Bearbeiten Sie die Konfiguration des Workspace-Standard-Identitätsanbieters, um Authentifizierungsmethoden auszuwählen und Netzwerkadressbereiche hinzuzufügen. Fügen Sie zum Zwecke hoher Verfügbarkeit weitere Identitätsanbieter-Instanzen zu Ihrer Workspace-Bereitstellung hinzu. Wenn auf der Seite „Identitätsanbieter“ mehrere Identitätsanbieter-Instanzen aufgeführt sind, können Sie die Reihenfolge der Instanzen bearbeiten. Die Reihenfolge ist wichtig, wenn IP-Adressen mehreren Identitätsanbieter-Instanzen zugeordnet sind. Details zum Hinzufügen oder Bearbeiten von Identitätsanbieter-Instanzen und zum Bearbeiten der Reihenfolge von Identitätsanbieter-Instanzen finden Sie unter „Hinzufügen und Konfigurieren einer Identitätsanbieter-Instanz“, auf Seite 20.
Remotezugriff auf Apps	Wählen Sie **Einstellungen > Remotezugriff auf Apps** aus, um Clients oder Vorlagen zu erstellen, mit denen sich Anwendungen bei Workspace registrieren können.
SAML-Zertifikat	Wählen Sie **Einstellungen > SAML-Zertifikat** aus, um das SAML-Signierungszertifikat anzuzeigen. Wenn in einer Web-Anwendung SAML-Assertionen zur Authentifizierung von Benutzern verwendet werden müssen, müssen sowohl in Workspace als auch in der Web-Anwendung lokal Kopien desselben SAML-Signierungszertifikats verfügbar sein.
Genehmigungen	Wählen Sie **Einstellungen > Genehmigungen** aus, um die Lizenzgenehmigung zu aktivieren oder zu deaktivieren. Die Aktivierung der Lizenzgenehmigung wird angewendet, wenn Sie Ihr Lizenzverwaltungssystem in Workspace integrieren.
Überwachung	Wählen Sie **Einstellungen > Überwachung** aus, um das Zusammenstellen von Informationen für den Bericht zu Überwachungsereignissen zu aktivieren oder zu deaktivieren, der auf der Registerkarte **Berichte** abrufbar ist.
Mit Citrix veröffentlichte Anwendung	Wählen Sie **Einstellungen > Mit Citrix veröffentlichte Anwendung** aus, um die globalen Workspace-Einstellungen für die Bereitstellung von Citrix-basierten Anwendungen, die im Workspace-Katalog verfügbar sind, zu bearbeiten. Eine Anleitung zum Bearbeiten der Einstellungen für eine einzelne Citrix-basierte Anwendung finden Sie unter *Setting Up Resources in VMware Workspace Portal Guide*.
Benutzerdefiniertes Branding	Wählen Sie **Einstellungen > Benutzerdefiniertes Branding** aus, um das Branding auf Workspace-Schnittstellen anzupassen. Siehe „Anpassen des Workspace-Brandings“, auf Seite 60.

Anpassen des Workspace -Brandings

Sie können die Logos, Schriftarten, Web-Clips und den Hintergrund, die in den unterschiedlichen Schnittstellen angezeigt werden, anpassen. Dazu zählen Workspace-Verwaltungskonsole, die Anmeldebildschirme für Benutzer und Administratoren, die Web-Ansicht des App-Portals und die Web-Ansicht des App-Portals auf mobilen Endgeräten.

Sie können das Branding anpassen, das in der Web-Ansicht des App-Portals und der Workspace-Verwaltungskonsole verwendet wird.

Vorgehensweise

1 Melden Sie sich bei Workspace-Verwaltungskonsole an.

2 Wählen Sie **Einstellungen > Benutzerdefiniertes Branding**.

3 Bearbeiten Sie die Einstellung im Formular dementsprechend.

Tabelle 10-1. Konfiguration des benutzerdefinierten Brandings

Formularelement	Beschreibung
	Markennamen und Logos
Logo	Über die Logo-Option können Sie das Logo ändern, das im App-Portal des Benutzers und in der Verwaltungskonsole angezeigt wird. Die für den Upload empfohlene maximale Größe von Bildern beträgt 350 x 100 Pixel. Wenn Sie Bilder hochladen, die größer als 350 x 100 Pixel sind, wird das Bild auf 350 x 100 Pixel skaliert. Zulässige Formate sind JPEG, PNG und GIF. Klicken Sie auf **Ändern**, um ein neues Bild hochzuladen, das das aktuelle Logo ersetzt. Wenn Sie auf **Bestätigen** klicken, wird die Änderung sofort umgesetzt.
Favicon	Über die Favicon-Option können Sie das Favicon ändern, das in Webbrowsern verwendet wird. Diese Option gilt sowohl für Desktops als auch für mobile Endgeräte. Das Favicon-Bild kann eine maximale Größe von 16 x 16 Pixeln haben. Zulässige Formate sind JPEG, PNG, GIF und ICO. Klicken Sie auf **Ändern**, um ein neues Bild hochzuladen, das das aktuelle Favicon ersetzt. Sie werden aufgefordert, die Änderung zu bestätigen. Wenn Sie auf **Bestätigen** klicken, wird die Änderung sofort übernommen.
Unternehmensname	Die Option „Unternehmensname“ gilt sowohl für Desktops als auch für mobile Endgeräte. Mit dieser Option können Sie den Unternehmensnamen ändern, der im Bildschirmtitel des Webbrowsers vor dem Produktnamen angezeigt wird. Überschreiben Sie zum Ändern den bestehenden Unternehmensnamen mit einem neuen.
Produktname	Die Option „Produktname“ gilt sowohl für Desktops als auch für mobile Endgeräte. Über diese Option können Sie den Namen ändern, der im Bildschirmtitel des Webbrowsers nach dem Unternehmensnamen angezeigt wird. Überschreiben Sie zum Ändern den bestehenden Produktnamen mit einem neuen.
	Anmeldebildschirm
Hintergrundfarbe	Die Farbe, in der der Hintergrund des Anmeldebildschirms angezeigt wird. Überschreiben Sie zum Ändern der Hintergrundfarbe den bestehenden Hexadezimal-Farbcode mit einem neuen. Aktivieren Sie **Hintergrund hervorheben**, um die Hintergrundfarbe zu betonen. Aktivieren Sie **Hintergrundmuster**, um das als Vorentwurf bereitgestellte Dreiecksmuster in dieser Hintergrundfarbe einzurichten.
Titelfarbe	Die Farbe, die im Titelbereich des Anmeldebildschirms angezeigt wird. Überschreiben Sie zum Ändern der Titelfarbe den bestehenden Hexadezimal-Farbcode mit einem neuen. Aktivieren Sie **Titelmuster**, um das als Vorentwurf bereitgestellte Dreiecksmuster in dieser Titelfarbe einzurichten.
Bild (optional)	Laden Sie ein Bild hoch, um anstelle einer Farbe ein Bild zum Hintergrund hinzuzufügen. Das Bild kann eine maximale Größe von 1400 x 900 Pixeln haben. Zulässige Formate sind JPEG, PNG und GIF.
Logo	Klicken Sie auf **Hochladen**, um ein neues Logo hochzuladen und so das aktuelle Logo auf den Anmeldebildschirmen zu ersetzen. Wenn Sie auf **Bestätigen** klicken, wird die Änderung sofort umgesetzt. Die für den Upload empfohlene maximale Größe von Bildern beträgt 350 x 100 Pixel. Wenn Sie Bilder hochladen, die größer als 350 x 100 Pixel sind, wird das Bild auf 350 x 100 Pixel skaliert. Zulässige Formate sind JPEG, PNG und GIF.
	Portal (Web-Ansicht)

Tabelle 10-1. Konfiguration des benutzerdefinierten Brandings (Fortsetzung)

Formularelement	Beschreibung
Hintergrundfarbe	Die Farbe, in der der Hintergrund der Web-Ansicht des Portals angezeigt wird. Überschreiben Sie zum Ändern der Hintergrundfarbe den bestehenden Hexadezimal-Farbcode mit einem neuen. Um anzugeben, wie die Hintergrundfarbe im App-Portal aussehen wird, ändert sich die Hintergrundfarbe in der App-Portal-Vorschau, wenn Sie einen neuen Farbcode eingeben. Wenn jedoch das Kontrollkästchen **Hintergrundbild einschließen** aktiviert ist, ist möglicherweise die Hintergrundfarbe in der Vorschau nicht sichtbar. Aktivieren Sie **Hintergrund hervorheben**, um die Hintergrundfarbe zu betonen. Aktivieren Sie **Hintergrundmuster**, um das als Vorentwurf bereitgestellte Dreiecksmuster in dieser Hintergrundfarbe einzurichten.
Namens- und Symbolfarbe	Die Farbe der Schriftart, die für die in der App-Portal-Anzeige aufgeführten Ressourcennamen verwendet wird. Der Name der Ressource befindet sich direkt unter dem Symbol für die Ressource. Überschreiben Sie zum Ändern der Schriftfarbe den bestehenden Hexadezimal-Farbcode mit einem neuen. Der Text des App-Namens in der App-Portal-Vorschau ändert sich, wenn Sie einen neuen Farbcode eingeben, um anzugeben, wie der Text im App-Portal aussehen wird.
Schrifteffekt	Wählen Sie den Schriftarttyp aus, der für den Text der My Apps-Anzeige verwendet werden soll.
Bild (optional)	Laden Sie ein Bild hoch, um anstelle einer Farbe ein Bild zum Hintergrund der App-Portal-Anzeige hinzuzufügen.
	Portal (Mobil- und Tablet-Ansichten)
Hintergrundfarbe	Überschreiben Sie den bestehenden Hexadezimal-Farbcode mit einem neuen, um die Hintergrundfarbe der My Apps-Anzeige für mobile Endgeräte zu ändern.
Titelleistenfarbe	Überschreiben Sie den bestehenden Hexadezimal-Farbcode mit einem neuen, um die Farbe der Titelleiste in der Anzeige für mobile Endgeräte zu ändern. Wählen Sie **Titelleistenmuster**, um das als Vorentwurf bereitgestellte Dreiecksmuster in der Titelleistenfarbe einzurichten.
Titelfarbe	Überschreiben Sie zum Ändern der Schriftfarbe für den Titelleistenbereich den bestehenden Hexadezimal-Farbcode mit einem neuen.
Namensfarbe	Die Farbe der Schriftart, die für die in der App-Portal-Anzeige aufgeführten Ressourcennamen verwendet wird. Der Name der Ressource befindet sich direkt unter dem Symbol für die Ressource. Überschreiben Sie zum Ändern der Schriftfarbe für die Anwendungsnamen den bestehenden Hexadezimal-Farbcode mit einem neuen.
Schrifteffekt	Wählen Sie den Schriftarttyp aus, der für den Text der My Apps-Anzeige verwendet werden soll.
Gleiche Werte für Startprogramm und Katalog verwenden	Wenn Sie für die App Center-Bildschirmanzeige das gleiche Branding wie für die My Apps-Bildschirmanzeige auf mobilen Endgeräten verwenden möchten, aktivieren Sie dieses Kontrollkästchen. Wenn Sie die App Center-Anzeige anders gestalten möchten, wählen Sie dieses Kontrollkästchen nicht aus, und konfigurieren Sie den Hintergrund, die Titelleistenfarbe und die Titelfarbe für die App Center-Anzeige.
	Tour für erstmalige Benutzer
Tour für erstmalige Benutzer	Wenn Benutzer ihr App-Portal zum ersten Mal öffnen, wird eine Diashow über die Funktionen von Workspace angezeigt. Sie können diese Funktion durch Entfernen des Häkchens deaktivieren.
	Mobile Endgeräte

Tabelle 10-1. Konfiguration des benutzerdefinierten Brandings (Fortsetzung)

Formularelement	Beschreibung
Web-Clip-Symbol	Das Workspace-Symbol, das angezeigt wird, wenn Benutzer die App-Portal-URL als Lesezeichen auf der Startseite ihrer mobilen Endgeräte speichern. Dieses Web-Clip-Symbol startet das Workspace-App-Portal. Das Bild kann eine maximale Größe von 512 x 512 Pixeln haben. Zulässige Formate sind JPEG und PNG. Klicken Sie auf **Ändern**, um ein neues Bild hochzuladen, das das aktuelle Web-Clip-Symbol ersetzt. Sie werden aufgefordert, die Änderung zu bestätigen. Wenn Sie auf **Bestätigen** klicken, wird die Änderung sofort übernommen.
Web-Clip-Titel	Der Titel, der zusammen mit dem WorkspaceWeb-Clip-Symbol angezeigt wird. Der Titel muss weniger als 20 Zeichen umfassen.

4 Klicken Sie auf **Speichern**.

Aktualisierungen zum benutzerdefinierten Branding in Workspace werden innerhalb von fünf Minuten nach dem Klicken auf „Speichern“ angewendet.

Weiter

Überprüfen Sie das Erscheinungsbild der Branding-Änderungen in den unterschiedlichen Schnittstellen.

Index

A

Active Directory, Bereitstellung **20**
administrative Einstellungen **59**
Administratoreinstellungen **59**
angemeldeter Benutzer, Anzahl **11**
Anwendungen
  Mobil **52**
  Web **52**
App-Popularität **11**
App-Portal, URL **7**
Appliance-Status **12**
Arbeitsbereichs-Images **48**
Audit-Ereignisbericht **57**
Authentifizierungsmethode **18, 20**
Authentifizierungsmethoden, Beziehung zu Zugriffsrichtlinien **27, 28, 30, 32**

B

Benutzer
  Active Directory **35**
  Attribute **41**
  Benutzer zu Gruppen hinzufügen **36**
  Informationen anzeigen **41**
  suchen **55**
  Synchronisierungsfilter für Active Directory aktualisieren **44**
  Workspace **35**
Benutzer und Gruppen verwalten **44**
Benutzerauthentifizierungsmethode **18**
Benutzerbericht **57**
Benutzerkennwort, Wiederherstellung **59**
Benutzerspeicher **20, 59**
Berichte **57**
Branding **60**
Branding-Elemente **59**

C

Citrix-basierte Anwendungen **59**
Connector **15, 20**
Connector-Webschnittstelle, URL **7**

D

Dashboard **11**
Datenbank, überwachen **12**

E

Einstellungen, administrative **59**
externer Identitätsanbieter **20**

G

Gastbenutzer **7, 35**
Gruppen
  Active Directory **35, 36**
  Informationen anzeigen **39**
  Mitgliedschaftsbericht **57**
  Mitgliedschaftsregeln ändern **36**
  suchen **55**
  Workspace **35, 36**
Gruppenmitgliedschaftsbericht **57**

H

hzn-admin tool **7**

I

Identitätsanbieter
  Beziehung zu Zugriffsrichtlinien **28**
  Connector **15**
  extern **15, 22, 23**
Identitätsanbieter hinzufügen, Schaltfläche **20**
Identitätsanbieter-Instanzen
  Auswahl **15**
  bearbeiten **59**
  Hinzufügen **59**
  Reihenfolge bearbeiten **59**
Identitätsanbieter, Auswahl, konfigurieren **20**
IP-Bereich **17**

K

Katalog
  Ressourcen anzeigen **51**
  verwalten **47**
Kategorien
  anwenden **50**
  entfernen **50**
  erstellen **49**
  löschen **50**
Kennwortwiederherstellung, Benutzer **59**
Konfigurator-Webschnittstelle, Zugriff **59**
Konto deaktivieren **44**

L

Lizenz, Genehmigung **59**

M

Machbarkeitsnachweis **20**

Mobile Anwendungen, Ressourcentyp **48**

N

Netzwerkbereich **17, 20**

Netzwerkbereiche, Beziehung zu Zugriffsrichtlinien **28, 30, 32**

R

Ressourcen
- Kategorien **49, 50**
- Prozentsatz der verwendeten Typen **11**

Ressourcenberechtigungsbericht **57**

Ressourcennutzungsbericht **57**

Richtliniensatz für Zugriff
- anwenden **33**
- Portal **33**
- Standard **32, 33**

Richtliniensätze für den Zugriff
- bearbeiten **30**
- erstellen **32**
- Portal **28, 32**
- spezifische Web-Anwendungen **29, 30, 32, 33**
- Standard **24, 27, 28, 30**

Rollen **41**

S

SAML
- externe Identitätsanbieter **22**
- Metadaten **23**
- Zertifikat **23**

SAML-Zertifikat **59**

Seite „Arbeitsbereiche“ **41**

Synchronisierungszeitplan **44**

Systemdiagnose-Dashboard **12**

Systeminformationen **12**

T

ThinApp-Pakete **48**

U

Überwachen des Systemzustands von Workspace **12**

Unternehmenslogo **59**

V

Version **12**

Verzeichnisservergruppen **35**

Verzeichnissynchronisierung planen **44**

View-Desktop-Pools **48**

virtuelle Appliances, Workspace **7**

W

Web-Anwendungen **48, 52**

Windows-Anwendungen **48**

Workspace, virtuelle Appliances **7**

Workspace-Gruppen **35**

Z

Zielgruppe **5**

Zugriffsereignisse **57**

Zugriffsrichtlinien
- Authentifizierungsstärke **24**
- Beziehung zum Identitätsanbietern **28, 30, 32**
- Clienttyp **24**
- Mindest-Authentifizierungsbewertung **27–29**
- Netzwerk **24, 27–29**
- spezifische Web-Anwendungen **29, 30, 32, 33**
- TTL **24, 28, 29**

zusätzliche Benutzerattribute **41**