Installieren und Konfigurieren von 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-001538-02

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

Informationen zum Installieren und Konfigurieren von VMware Workspace Portal

1

Das *Installations- und Konfigurationshandbuch zu VMware Workspace Portal* leitet Sie durch die Installation und Konfiguration der Workspace-Appliance. Wenn die Installation abgeschlossen ist, können Sie Benutzern mithilfe von VMware Workspace™ Portal Berechtigungen für den verwalteten Zugriff auf die Anwendungen Ihrer Organisation, einschließlich Windows-Anwendungen, SaaS-Anwendungen (Software as a Service, Software als Dienst) und View-Desktops, von mehreren Geräten aus erteilen.

Angesprochene Zielgruppe

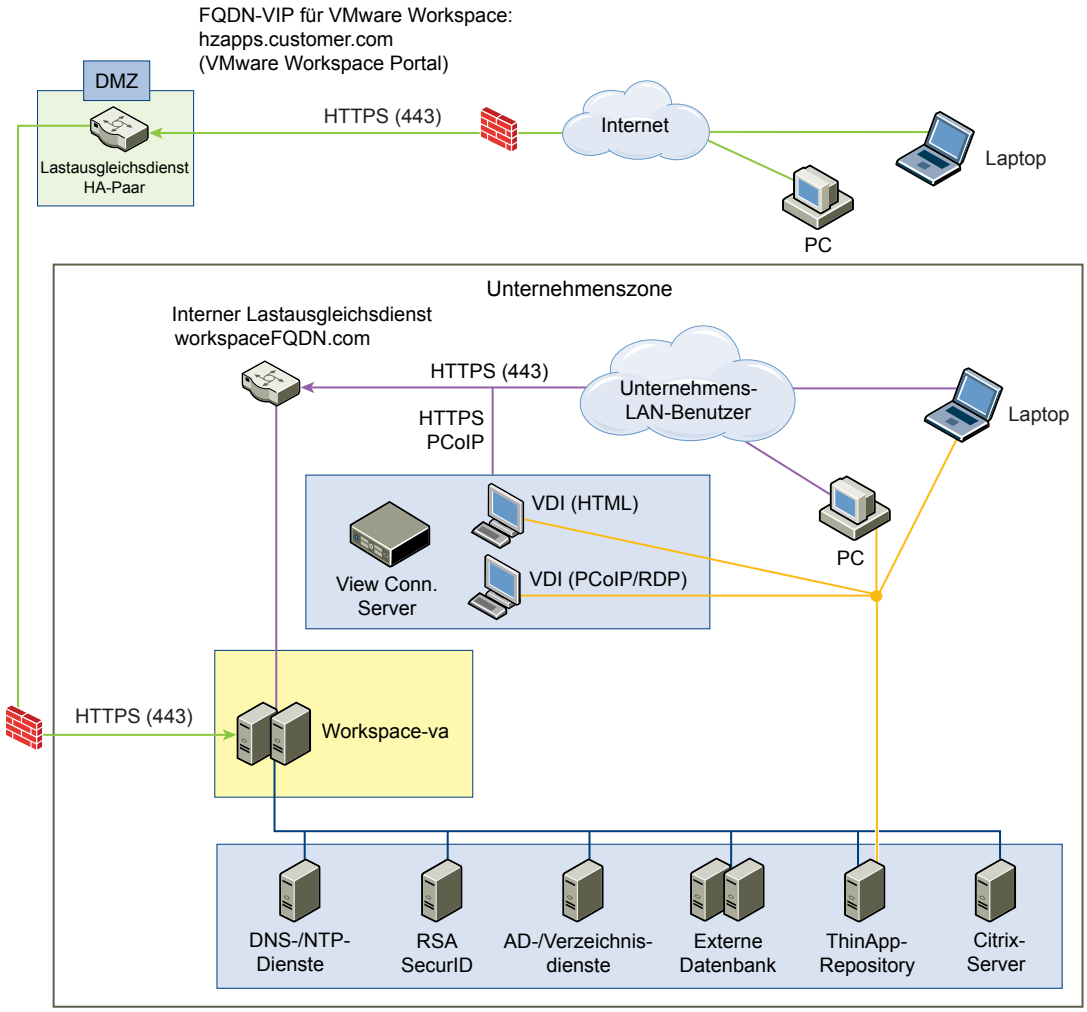
Diese Informationen sind für Systemadministratoren und funktionelle Administratoren von VMware Workspace™ Portal bestimmt. Die Informationen wurden für erfahrene Windows- und Linux-Systemadministratoren geschrieben, die mit VMware-Technologien, insbesondere vCenter™, ESX™, vSphere® und View™, Netzwerkkonzepten, Active Directory-Servern, Simple Mail Transfer Protocol (SMTP) und NTP-Servern vertraut sind. Das zugrunde liegende Betriebssystem der virtuellen Appliance ist SUSE Linux 11. Kenntnisse anderer Technologien, z. B. VMware ThinApp®, RSA SecurID und Active Directory, sind nützlich, wenn Sie planen, diese Funktionen zu implementieren.

Vorbereiten der Installation von VMware Workspace Portal

2

Vor den Aufgaben zum Bereitstellen und Einrichten von VMware Workspace Portal müssen die vorbereitenden Aufgaben ausgeführt werden, die Workspace-OVF-Datei muss bereitgestellt werden und die Einrichtung im Workspace-Einrichtungsassistenten muss abgeschlossen sein.

Abbildung 2-1. Diagramm der VMware Workspace Portal -Architektur für typische Bereitstellungen



Dieses Kapitel behandelt die folgenden Themen:

System- und Netzwerkkonfigurationen von Workspace – Anforderungen

Berücksichtigen Sie Ihre gesamte Workspace-Bereitstellung, einschließlich der Art der Integration von Workspace, wenn Sie Entscheidungen über Hardware, Ressourcen und Netzwerkanforderungen treffen.

Workspace-VAs – Anforderungen

Stellen Sie sicher, dass die den Workspace-VAs zugeordneten Ressourcen die Mindestanforderungen erfüllen.

Tabelle 2-1. VMware Workspace Portal -VA (workspace-va) – Anforderungen

Komponente	Mindestanforderung
CPU	2
RAM	6 GB
Festplattenspeicher	36 GB
Zusätzliche Hinweise	■ In der workspace-va-Konfiguration ist eine PostgreSQL-Datenbank enthalten und Sie können einen externen Datenbankserver verwenden. Informationen über bestimmte Datenbankversionen und Service Pack-Konfigurationen, die von Workspace unterstützt werden, finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter „http://www.vmware.com/resources/compatibility/sim/interop_matrix.php“. ■ Informationen zur Größe der externen Datenbank: 64 GB für die ersten 100.000 Benutzer. 20 GB je weitere 10.000 Benutzer. ■ Speicher: 32 GB

Netzwerkkonfiguration – Anforderungen

Der Workspace-Server muss der Windows-Domäne beitreten, wenn Kerberos-, View- oder ThinApp-Funktionen aktiviert sind. In diesem Fall muss sich der Workspace-Hostname in derselben Domäne wie die Active Directory-Domäne befinden, der er beitritt.

Tabelle 2-2. Netzwerkkonfiguration – Anforderungen

Komponente	Mindestanforderung
DNS-Datensätze und IP-Adresse	IP-Adresse und DNS-Datensatz
Firewall-Port	Stellen Sie sicher, dass der eingehende Firewall-Port 443 für Benutzer außerhalb des Unternehmensnetzwerks für den Zugriff auf Workspace geöffnet ist.

Port-Anforderungen

Die in Workspace verwendeten Ports werden unten beschrieben. Auf Ihre Bereitstellung trifft möglicherweise nur ein Teil davon zu. Hier sind zwei potenzielle Szenarien:

- Für die Synchronisierung von Benutzern und Gruppen muss die Workspace-VA eine Verbindung mit Active Directory herstellen.
- Für die Synchronisierung mit ThinApp muss die Workspace-VM der Active Directory-Domäne beitreten und eine Verbindung mit der ThinApp Repository-Freigabe herstellen.

Tabelle 2-3. Von Workspace verwendete Ports

Port	Quelle	Ziel	Beschreibung
443	Lastausgleichsdienst	workspace-va	Hypertext Transport Protocol over SSL (HTTPS)
443	workspace-va	workspace-va 2, 3, usw.	Hypertext Transport Protocol over SSL (HTTPS)
443	Browser	workspace-va	Hypertext Transport Protocol over SSL (HTTPS)
8443	Browser	workspace-va	Administratorport Hypertext Transport Protocol over SSL (HTTPS)
25	workspace-va	SMTP	TCP-Port zum Weiterleiten ausgehender E-Mails
389, 636, 3268, 3269	workspace-va	Active Directory	Es werden Standardwerte angezeigt. Diese Ports sind konfigurierbar.
5432	workspace-va	Datenbank	Der PostgreSQL-Standardport ist 5432. Der Oracle-Standardport ist 1521.
389, 443	workspace-va	View Server	Zugriff auf View Server
443	workspace-va	VMware ThinApp-Repository	Zugriff auf ThinApp-Repository
5500	workspace-va	RSA SecurID-System	Es wird der Standardwert angezeigt. Dieser Port ist konfigurierbar.
53	workspace-va	DNS-Server	TCP/UDP Jede workspace-va muss über Zugriff auf den DNS-Server über Port 53 verfügen und eingehenden SSH-Datenverkehr über Port 22 zulassen.
88, 465, 135	workspace-va	Domänencontroller	TCP/UDP
TCP: 9300-9400 UDP: 54328	workspace-va	workspace-va	Überwachungsanforderungen

Hardware-Anforderungen für den ESX-Server

Stellen Sie sicher, dass die Umgebung für den Host und die vSphere-Instanz, die die virtuelle Workspace-Appliance ausführt, die Mindestanforderungen an die Hardware erfüllt. Die Speicheranforderungen je Bereitstellung variieren basierend auf der Anzahl der Benutzer.

HINWEIS Sie müssen die Zeitsynchronisierung auf ESX-Host-Ebene über den NTP-Server einschalten. Andernfalls kommt es zu einer Zeitabweichung zwischen den virtuellen Appliances.

Tabelle 2-4. Mindestanforderungen an die Hardware für Workspace

Komponente	Mindestanforderung
Prozessor	2 Intel Quad Cores, 3,0 GHz, 4 MB Cache
RAM	16 GB DDR2, 1066 MHz, ECC und registriert

Tabelle 2-4. Mindestanforderungen an die Hardware für Workspace (Fortsetzung)

Komponente	Mindestanforderung
On-Board-LAN	Ein 10/100/1000Base-TX-Port
Speicher	500GB

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

Vorbereiten der Bereitstellung von Workspace

Bevor Sie Workspace bereitstellen, müssen Sie Ihre Umgebung vorbereiten. Diese Vorbereitung umfasst das Herunterladen der Workspace-OVF-Datei sowie das Erstellen von DNS-Datensätzen und IP-Adressen.

Voraussetzungen

Führen Sie die Vorbereitungsaufgaben aus, bevor Sie mit der Installation von Workspace beginnen.

- Mindestens ein ESX-Server zum Bereitstellen der Workspace-VA.

  Hinweis Informationen zu unterstützten vSphere- und ESX-Serverversionen finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter „http://www.vmware.com/resources/compatibility/sim/interop_matrix.php“.

- Der VMware vSphere Client oder vSphere Web Client wird für die Bereitstellung der OVF-Datei und den Remotezugriff auf die bereitgestellte virtuelle Appliance zum Konfigurieren des Netzwerks benötigt.
- Von der VMware-Website heruntergeladene Workspace-OFV-Datei.
- Erstellen von DNS-Datensätzen und IP-Adressen auf Seite 11

  Für die Workspace-Appliance müssen ein DNS-Eintrag und eine statische IP-Adresse verfügbar sein. Da jedes Unternehmen seine IP-Adressen und DNS-Datensätze anders verwaltet, sollten Sie vor Beginn der Installation den DNS-Datensatz und die IP-Adressen anfordern, die verwendet werden sollen.

- Datenbankoptionen für Workspace auf Seite 11

  Workspace kann mit einer internen oder mit einer externen Datenbank eingerichtet werden. Eine vPostgres-Datenbank ist in die Workspace-Appliance eingebettet. Die interne Datenbank ist der Standardwert. Beim Konfigurieren des Workspace-Setup-Assistenten können Sie festlegen, dass eine Verbindung zu einer externen Datenbank hergestellt wird.

- Herstellen der Verbindung mit Active Directory auf Seite 12

  Workspace verwendet für Benutzerauthentifizierung und -verwaltung die vorhandene Active Directory-Infrastruktur. Für die Synchronisierung von Benutzern und Gruppen muss die Workspace-VA eine Verbindung mit Active Directory herstellen.

- Checklisten zur Bereitstellung auf Seite 12

  Anhand der Checklisten zur Bereitstellung von Workspace können Sie die erforderlichen Informationen für die Installation von Workspace zusammentragen.

Erstellen von DNS-Datensätzen und IP-Adressen

Für die Workspace-Appliance müssen ein DNS-Eintrag und eine statische IP-Adresse verfügbar sein. Da jedes Unternehmen seine IP-Adressen und DNS-Datensätze anders verwaltet, sollten Sie vor Beginn der Installation den DNS-Datensatz und die IP-Adressen anfordern, die verwendet werden sollen.

(Optional) Reverse-Lookup und IP-Adressen

Das Konfigurieren von Reverse-Lookup ist in Workspace optional. Wenn Sie Reverse-Lookup implementieren, müssen Sie einen PTR-Datensatz auf dem DNS-Server definieren, damit jede virtuelle Appliance die korrekte Netzwerkkonfiguration verwendet.

Verwenden Sie beim Gespräch mit Ihrem Netzwerkadministrator die folgende Beispielliste von DNS-Datensätzen. Ersetzen Sie die Beispielinformationen durch entsprechende Informationen aus Ihrer Umgebung. Dieses Beispiel verdeutlicht Forward-DNS-Datensätze und IP-Adressen.

Tabelle 2-5. Beispiele für Forward-DNS-Datensätze und IP-Adressen

Domänenname	Ressourcentyp	IP-Adresse
my-Workspace-VA.company.com	A	10.28.128.3

Dieses Beispiel verdeutlicht Reverse-DNS-Datensätze und IP-Adressen.

Tabelle 2-6. Beispiele für Reverse-DNS-Datensätze und IP-Adressen

IP-Adresse	Ressourcentyp	Domänenname
128.28.10.in-addr.arpa.	IN	PTR my-Workspace-VA.company.com

Nachdem Sie die DNS-Konfiguration abgeschlossen haben, vergewissern Sie sich, dass das Reverse-DNS-Lookup korrekt konfiguriert ist. Der Befehl *Host-IP-Adresse* der virtuellen Appliance muss z. B. in das DNS-Namen-Lookup aufgelöst werden.

Verwenden eines Unix/Linux-basierten DNS-Servers

Wenn Sie einen Unix/Linux-basierten DNS-Server verwenden und planen, mit Workspace der Active Directory-Domäne beizutreten, stellen Sie sicher, dass für jeden Active Directory-Domänencontroller die geeigneten Service-Ressourcendatensätze (SRV) erstellt werden.

Datenbankoptionen für Workspace

Workspace kann mit einer internen oder mit einer externen Datenbank eingerichtet werden. Eine vPostgres-Datenbank ist in die Workspace-Appliance eingebettet. Die interne Datenbank ist der Standardwert. Beim Konfigurieren des Workspace-Setup-Assistenten können Sie festlegen, dass eine Verbindung zu einer externen Datenbank hergestellt wird.

Die Verwendung der Konfiguration mit einer eingebetteten vPostgres-Datenbank eignet sich für kleine Bereitstellungen und kann standardmäßig verwendet werden. Die interne Datenbank erfordert keine zusätzliche Konfiguration außerhalb von Workspace, es empfiehlt sich jedoch, Ihre interne Datenbank für hohe Verfügbarkeit zu konfigurieren. Siehe KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1 (Verwenden einer eingebetteten vPostgres-Datenbank für VMware Workspace Portal 2.1).

Wenn Sie eine externe Datenbank verwenden möchten, muss Ihr Datenbankadministrator eine leere externe Datenbank und das entsprechende Schema vorbereiten, bevor die Verbindung mit der Datenbank hergestellt wird. Lizenzierte Benutzer können eine externe Datenbank der virtuellen vPostgres-Appliance oder eine Oracle-Datenbank verwenden, um eine High Availability-Umgebung mit einer externen Datenbank einzurichten. Siehe „Herstellen der Verbindung zu einer externen Datenbank“, auf Seite 24.

Herstellen der Verbindung mit Active Directory

Workspace verwendet für Benutzerauthentifizierung und -verwaltung die vorhandene Active Directory-Infrastruktur. Für die Synchronisierung von Benutzern und Gruppen muss die Workspace-VA eine Verbindung mit Active Directory herstellen.

Active Directory muss in demselben LAN wie die Workspace-VA verfügbar sein. Weitere Informationen hierzu finden Sie unter „Herstellen einer Verbindung zu Active Directory“, auf Seite 36

Checklisten zur Bereitstellung

Anhand der Checklisten zur Bereitstellung von Workspace können Sie die erforderlichen Informationen für die Installation von Workspace zusammentragen.

Wenn Sie die statischen IP-Adressen im DNS vor der Installation und während einer Workspace-Installation erstellen, benötigen Sie je nach der Art Ihrer Bereitstellung möglicherweise nur einen Teil der Netzwerkinformationen für Ihre virtuellen Appliances.

Informationen zum vollqualifizierten Domänennamen

Weitere Informationen finden Sie unter „Aktivieren des externen Zugriffs auf Workspace mithilfe eines Lastausgleichsdienstes“, auf Seite 43.

Tabelle 2-7. Informationen zum vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) von Workspace - Checkliste

Zu erfassende Informationen	Liste der Informationen
Workspace FQDN	

Netzwerkinformationen zur Workspace -VA

Tabelle 2-8. Netzwerkinformationen zu Workspace - Checkliste

Zu erfassende Informationen	Liste der Informationen
IP-Adresse	
DNS-Name für diese virtuelle Appliance	
Standard-Gateway-Adresse	
Netzmaske oder Präfix	

Active Directory-Domänencontroller

Tabelle 2-9. Informationen zum Active Directory-Domänencontroller

Zu erfassende Informationen	Liste der Informationen
Active Directory-Servername	
Active Directory-Domänenname	
DN-Benutzername und Kennwort binden	

Tabelle 2-9. Informationen zum Active Directory-Domänencontroller (Fortsetzung)

Zu erfassende Informationen	Liste der Informationen
Basis-DN	
Active Directory-Benutzername und Kennwort (müssen über Berechtigungen für den Beitritt von Computern zur Domäne verfügen.)	

SSL-Zertifikat (optional)

Tabelle 2-10. Informationen zum SSL-Zertifikat - Checkliste

Zu erfassende Informationen	Liste der Informationen
SSL-Zertifikat	
Privater Schlüssel	

HINWEIS Das SSL-Zertifikat ist optional. Sie können ein SSL-Zertifikat hinzufügen, nachdem Sie Workspace bereitgestellt haben.

Workspace-Lizenzschlüssel

Tabelle 2-11. Informationen zum Workspace Lizenzschlüssel - Checkliste

Zu erfassende Informationen	Liste der Informationen
Lizenzschlüssel	

HINWEIS Die Lizenzschlüssel-Informationen werden nach Abschluss der Installation in der Workspace-Verwaltungskonsole auf der Registerkarte Einstellungen > Globale Einstellungen eingegeben.

Externe Datenbank

Tabelle 2-12. Informationen zur externen Datenbank - Checkliste

Zu erfassende Informationen	Liste der Informationen
Hostname der Datenbank	
Port	
Nutzername	
Kennwort	

Workspace-Kennwörter

Tabelle 2-13. In Workspace verwendetes Administratorkennwort

Zu erfassende Informationen	Liste der Informationen
Kennwort für das Workspace-Administratorkonto	
Kennwort für das VA-Root-Konto	
Kennwort des sshuser-Kontos für die Remoteanmeldung	

Bereitstellen von Workspace 3

Das Bereitstellen und Einrichten von Workspace mit dem vSphere Client oder vSphere Web Client umfasst das Bereitstellen der OVF-Vorlage, das Starten der virtuellen Workspace-Appliance und das Einrichten von Workspace.

Nachdem die virtuelle Workspace-Appliance bereitgestellt wurde, richten Sie die Workspace-Umgebung mithilfe des Workspace Setup-Assistenten ein.

Nutzen Sie die Informationen in den Checklisten zur Bereitstellung, um die Installation abzuschließen. Siehe „Checklisten zur Bereitstellung“, auf Seite 12.

Dieses Kapitel behandelt die folgenden Themen:

Installieren der Workspace -OVF-Datei

Zum Starten der Installation von Workspace müssen Sie die OVF-Datei mit dem VMware vSphere Client oder dem vSphere Web Client bereitstellen. Sie können die OVF-Datei als lokale Datei, auf die über den vSphere Client oder eine Web-URL zugegriffen werden kann, herunterladen und bereitstellen.

Voraussetzungen

- Verwenden Sie für den vSphere Web Client Firefox oder Chrome. Verwenden Sie zum Bereitstellen der OVF-Datei nicht Internet Explorer.
- Laden Sie die Workspace-OVF-Datei herunter.

Vorgehensweise

1 Wählen Sie im vSphere Client oder vSphere Web Client **OVF-Vorlage bereitstellen** aus, um die Workspace-OVF-Datei bereitzustellen.

2 Geben Sie auf den Seiten von „OVF-Vorlage bereitstellen“ die speziellen Daten für Ihre Workspace-Bereitstellung ein.

Seite	Beschreibung
Quelle	Navigieren Sie zum Speicherort des OVF-Pakets oder geben Sie eine URL ein.
Einzelheiten zur OVF-Vorlage	Überprüfen Sie, ob Sie die richtige Version von Workspace ausgewählt haben.
Lizenz	Lesen Sie die Endbenutzer-Lizenzvereinbarung und klicken Sie auf **Akzeptieren**.
Name und Speicherort	Geben Sie den Namen für diese Workspace-VA ein. Der Name muss innerhalb des VM-Ordners eindeutig sein. Bei Namen wird die Groß-/Kleinschreibung beachtet.
Host/Cluster	Wählen Sie den Host oder Cluster zum Ausführen der bereitgestellten Vorlage aus.
Ressourcenpool	Wählen Sie den Ressourcenpool aus.
Speicher	Wählen Sie den Speicherort aus, an dem die Dateien der virtuellen Maschine gespeichert werden sollen.
Festplattenformat	Wählen Sie das Festplattenformat zum Speichern der Workspace-Dateien aus. Wählen Sie für Produktionsumgebungen das Format „Thick Provision“ aus. Verwenden Sie für Evaluierungen und Tests das Format „Thin provision“ aus.
Netzwerkzuordnung	Ordnen Sie Netzwerken in Ihrem Bestand die in Workspace verwendeten Netzwerke zu.
Eigenschaften	**Hinweis** Bei der Bereitstellung von Workspace lassen Sie das Kontrollkästchen für den Anwendungsabschnitt deaktiviert. Wählen Sie im Feld „Einstellung der Zeitzone“ die richtige Zeitzone aus. Das Programm zur Verbesserung der Kundenerfahrung ist standardmäßig aktiviert. VMware erfasst anonym Daten zu Ihrer Bereitstellung, damit VMware besser auf die Benutzeranforderungen reagieren kann. Geben Sie im Feld „Hostname“ den zu verwendenden Hostnamen ein. Wenn dieses Feld leer ist, wird zum Suchen des Hostnamens Reverse-DNS verwendet. Um die statische IP-Adresse für Workspace zu konfigurieren, geben Sie die Adresse für jedes der folgenden Felder ein: „Standard-Gateway“, „DNS“, „IP-Adresse“ und „Netzmaske“. **Wichtig** Wenn eines dieser vier Felder oder das Feld „Hostname“ leer ist, wird DHCP verwendet. Um DHCP zu verwenden, lassen Sie die Adressfelder leer. (Optional) Nach dem Installieren von Workspace können Sie IP-Pools konfigurieren. Siehe „(Optional) Hinzufügen von IP-Pools in Workspace“, auf Seite 17.
Bereit zum Abschließen	Überprüfen Sie die ausgewählten Optionen. Wenn die Informationen richtig sind, klicken Sie auf **Fertig stellen**.

Eine Fortschrittsanzeige wird geöffnet. Je nach der Geschwindigkeit Ihres Netzwerks kann diese Bereitstellung mehrere Minuten dauern.

3 Wenn die Bereitstellung abgeschlossen ist, klicken Sie in der Fortschrittsanzeige auf **Schließen**.

4 Wählen Sie die virtuelle Workspace-Appliance aus, die Sie gerade bereitgestellt haben, und klicken Sie auf **Virtuelle Maschine einschalten**.

Die virtuelle Workspace-Appliance wird initialisiert. Sie können die Registerkarte „Konsole“ öffnen, um die Details anzuzeigen. Wenn die Initialisierung der virtuellen Appliance abgeschlossen ist, werden auf dem Bildschirm „Konsole“ die Workspace-Version und URLs zum Anmelden bei der Workspace-Webschnittstelle und zum Abschließen des Setups von Workspace angezeigt.

Weiter

Konfigurieren Sie die Workspace-Einstellungen. Dies schließt auch die Herstellung der Verbindung mit Active Directory und die Auswahl von Benutzern und Gruppen ein, die mit Workspace synchronisiert werden sollen.

(Optional) Hinzufügen von IP-Pools in Workspace

Die Netzwerkkonfiguration mit IP-Pool ist in Workspace optional. Sie können Workspace manuell IP-Pools hinzufügen, nachdem Workspace installiert wurde. Sie bearbeiten die Netzwerkeigenschaften der workspace-va-VA, um die Eigenschaften in dynamische Eigenschaften zu ändern und die Einstellungen für Netzmaske, Gateway und DNS zu konfigurieren.

IP-Pools verhalten sich wie DHCP (Dynamic Host Configuration Protocol)-Server, um der workspace-va-VA IP-Adressen aus dem Pool zuzuweisen. Damit die Workspace-Appliance IP-Pools verwenden kann, müssen Sie Appliance-OVF-Eigenschaften bearbeiten.

Voraussetzungen

Zum Hinzufügen von IP-Pool-Einstellungen muss die workspace-va-VA ausgeschaltet sein.

Vorgehensweise

1 Klicken Sie im vSphere Client oder vSphere Web Client mit der rechten Maustaste auf die virtuelle Appliance, die für IP-Pools konfiguriert werden soll, und wählen Sie **Einstellungen bearbeiten** aus.

2 Klicken Sie im Abschnitt „Eigenschaften“ der Seite auf **Eigenschaften**.

3 Konfigurieren Sie auf der Seite „Erweiterte Eigenschaftskonfiguration“ die folgenden Schlüsselbezeichnungen: „vami.DNS.WorkspacePortal“, „vami.netmask0.WorkspacePortal“ und „vami.gateway.WorkspacePortal“.

   a Wählen Sie auf der Seite „Erweiterte Eigenschaftskonfiguration“ eine der Schlüsselbezeichnungen aus und klicken Sie auf **Bearbeiten**.

   b Klicken Sie auf der Seite „Eigenschaftseinstellungen bearbeiten“ neben dem Feld „Typ“ auf **Bearbeiten**.

   c Wählen Sie auf der Seite „Eigenschaftstyp bearbeiten“ die Option **Dynamische Eigenschaft** und den jeweils entsprechenden Wert aus dem Drop-down-Menü für Netzmaske, Gateway und DNS-Server aus.

   d Klicken Sie auf **OK**, bis alle Seiten geschlossen sind.

4 Schalten Sie die virtuelle Appliance ein.

Die Eigenschaften sind zum Auswählen aus IP-Pools konfiguriert.

Konfigurieren von Workspace -Einstellungen

Nachdem das Workspace-OVF-Paket bereitgestellt und installiert wurde, führen Sie den Workspace-Setup-Assistenten aus, um die Informationen zum Herstellen der Verbindung mit Active Directory zu konfigurieren. Erstellen Sie eine interne Datenbank oder wählen Sie ggf. eine externe Datenbank aus. Wählen Sie dann Benutzer und Gruppen aus, die mit Workspace synchronisiert werden sollen.

Voraussetzungen

- Eingeschaltete virtuelle Appliance von Workspace.
- Die Liste der Kennwörter für den Workspace-Administrator, das Workspace-Root-Konto und das Workspace-Sshuser-Konto.

- Wenn Sie eine externe Datenbank verwenden, muss diese eingerichtet sein und die Verbindungsinformationen für die externe Datenbank müssen verfügbar sein.
- Active Directory-Verbindungsinformationen.
- Wenn eine Active Directory-Umgebung in mehreren Strukturen konfiguriert wurde und die lokale Domänengruppe Mitglieder aus Domänen in verschiedenen Strukturen enthält, muss der auf der Workspace-Verzeichnisseite verwendete Bind-DN-Benutzer zur Administratorgruppe der Domäne hinzugefügt werden, in der sich die lokale Domänengruppe befindet. Wird dies versäumt, fehlen diese Benutzer in der lokalen Domänengruppe.
- Liste der Active Directory-Benutzerattribute, die Sie als Filter verwenden möchten, und eine Liste der Gruppen, die Sie Workspace hinzufügen möchten.

Vorgehensweise

1 Um Workspace nach der Bereitstellung des OVF-Pakets zu konfigurieren, rufen Sie die Workspace-URL `https://workspacehostname.com` auf.

Klicken Sie im Begrüßungsbildschirm auf **Fortfahren**.

2 Erstellen Sie auf der Seite „Kennwörter festlegen“ Kennwörter für die folgenden Administratorkonten.

- Appliance-Administratorkonto. Erstellen Sie das Kennwort für den Workspace-Administrator. Der Benutzername lautet „admin“ und kann nicht geändert werden. Dieses Konto wurde während der Erstinstallation von Workspace erstellt.
- Root-Konto. Zum Einrichten von Workspace wurde ein standardmäßiges VMware-Root-Kennwort verwendet. Erstellen Sie ein neues Root-Kennwort.
- sshuser-Konto. Erstellen Sie das Kennwort für den Remotezugriff auf die workspace-va-VA.

Klicken Sie auf **Fortfahren**.

3 Wählen Sie die zu verwendende Datenbank aus.

- Wenn Sie eine interne Datenbank verwenden, klicken Sie auf **Fortfahren**.
- Wenn Sie eine externe Datenbank verwenden, wählen Sie **Externe Datenbank** aus und geben Sie die Verbindungsinformationen für die externe Datenbank sowie den Benutzernamen und das Kennwort für den Datenbankserver ein, den Sie zuvor eingerichtet haben. Um zu überprüfen, ob Workspace eine Verbindung mit der Datenbank herstellen kann, klicken Sie auf **Verbindung testen**.

Klicken Sie auf **Fortfahren**.

Die Verbindung mit der Datenbank ist konfiguriert und die Datenbank ist initialisiert.

4 Geben Sie auf der Seite „Verzeichnis“ die Active Directory-Informationen ein und klicken Sie auf **Überprüfen**.

Informationstyp	Beschreibung
Verzeichnistyp	Übernehmen Sie den Verzeichnistyp „Active Directory“.
SSL verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn Sie für die Verzeichnisverbindung SSL verwenden möchten.
DNS-Dienstspeicherort verwenden	Aktivieren Sie dieses Kontrollkästchen, wenn für die Verzeichnisverbindung der DNS-Dienstspeicherort verwendet wird.
Server-Host	Geben Sie die Active Directory-Hostadresse ein. Verwenden Sie beim Eingeben des Hostnamens ausschließlich ASCII-Zeichen.
Server-Port	Geben Sie die Portnummer für den Active Directory-Host ein. Für Active Directory mit einer einzelnen Domäne lautet der Standardport 389. Wenn SSL ausgewählt ist, lautet der Standardport 636.

Informationstyp	Beschreibung
Suchattribut	Geben Sie das Active Directory-Kontoattribut ein, das den Benutzernamen enthält. Für die meisten Bereitstellungen sollte **sAMAccountName** ausgewählt werden.
Basis-DN	Geben Sie den DN ein, der der Startpunkt für Verzeichnisserver-Suchvorgänge ist. Beispiel: OU-myunit,DC=mycompany,DC=com.
Bind-DN	Geben Sie den Bind-DN, einschließlich des allgemeinen Namens (Common Name, CN), eines Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern ein. Dieser Benutzer wird Administrator für die Workspace-Bereitstellung.
Bind-Kennwort	Geben Sie das Active Directory-Kennwort für das Bind-DN-Konto ein.

Die Bind-DN-Informationen werden bestätigt und das Administratorkonto wird als Benutzer in Workspace hinzugefügt.

Klicken Sie auf **Fortfahren**.

5 Wählen Sie auf der Seite „Benutzerattribute zuordnen“ die in Active Directory verwendeten Attribute aus, die den Workspace-Verzeichnisattributen zugeordnet werden.

Wenn Sie eine Integration in View planen, aktivieren Sie **Erforderlich** neben dem Attribut „userPrincipal Name“. Wenn Sie eine Integration in Horizon DaaS planen, aktivieren Sie **Erforderlich** neben dem Attribut „distinguishedName“. Sie können dies auch später auf den Connector Services-Administrator-Seiten ausführen.

6 Wählen Sie auf der Seite „Benutzer auswählen“ Benutzerattribute aus dem Drop-down-Menü aus, um Filter zum Beschränken der Typen von Benutzer zu erstellen, die mit Workspace synchronisiert werden. Klicken Sie auf **Fortfahren**.

7 Gruppen in Active Directory werden nicht automatisch mit Workspace synchronisiert. Klicken Sie auf der Seite „Ausgewählte Gruppen“ neben der DN-Beschreibung der Gruppe auf **Hinzufügen**, um die Gruppe hinzuzufügen. Klicken Sie auf **Fortfahren**.

Auf der Seite „An Workspace weitergeben“ werden Informationen über die Anzahl der Benutzer und Gruppen angezeigt, die mit Workspace synchronisiert werden.

Klicken Sie zum Starten der Synchronisierung auf **An Workspace weitergeben**.

8 Wenn die Seite „Setup ist abgeschlossen“ angezeigt wird, klicken Sie auf **Bei Workspace anmelden**, um sich bei der Verwaltungskonsole anzumelden.

Der Anmeldebildschirm von Workspace wird angezeigt. Geben Sie den Benutzernamen und das Kennwort für den Bind-DN ein, die Sie beim Einrichten der Verbindung mit Active Directory eingegeben haben. In der Workspace-Verwaltungskonsole können Sie Ressourcen für die Verwendung von Workspace einrichten und diesen Ressourcen Benutzer zuweisen.

Hinweis Wenn ein Netzwerkfehler auftritt und der Hostname mithilfe von DNS-Reverse-Lookup nicht eindeutig aufgelöst werden kann, wird der Konfigurator-Vorgang beendet. Sie müssen zuerst die Netzwerkprobleme beheben und dann die workspace-va-VA neu starten. Anschließend können Sie mit der Bereitstellung fortfahren. Die neuen Netzwerkeinstellungen stehen erst nach einem Neustart der workspace-va-VA zur Verfügung.

Weiter

Melden Sie sich bei der Workspace-Verwaltungskonsole an, um einen Katalog mit Ressourcen für die Anwendungen Ihrer Organisation anzupassen und den Benutzerzugriff auf diese Ressourcen zu aktivieren.

Richten Sie weitere Ressourcen ein, z. B. View, ThinApp, Horizon DaaS und Citrix-basierte Anwendungen. Siehe *Einrichten von Ressourcen in VMware Workspace Portal*.

Festlegen der Proxy-Server-Einstellungen für Workspace

Über die Workspace-VAs wird auf den Cloud-Anwendungskatalog und andere Webservices im Internet zugegriffen. Wenn Ihre Netzwerkkonfiguration Internetzugriff über einen HTTP-Proxy bereitstellt, müssen Sie Ihre Proxy-Einstellungen in der Workspace-Appliance anpassen.

Aktivieren Sie den Proxy, damit dieser nur den Internetdatenverkehr verarbeitet. Um sicherzustellen, dass der Proxy korrekt eingerichtet ist, setzen Sie den Parameter für internen Datenverkehr innerhalb der Domäne auf `no–proxy`.

Vorgehensweise

1 Melden Sie sich im vSphere Client als Root-Benutzer bei der workspace-va-VA an.

2 Geben Sie **YaST2** ein.

3 Wählen Sie **Netzwerkdienste** und dann **Proxy** aus.

4 Geben Sie die korrekte Proxy-URL in das HTTP-Feld ein.

http://proxy.beispiel.com:3128

5 Geben Sie die korrekte Proxy-URL in das HTTPS-Feld ein.

https://proxy.beispiel.com:3128

6 Führen Sie auf der workspace-va-VM einen Neustart des Tomcat-Servers aus, um die neuen Proxy-Einstellungen anzuwenden.

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

Der Cloud-Anwendungskatalog und andere Webservices sind jetzt in Workspace verfügbar.

Workspace-Verwaltungsdienste

Sie verwalten Benutzer, Gruppen, Ressourcen, Authentifizierung, die Konfiguration der Synchronisierung und die Datenbankverbindung für Workspace über verschiedene Workspace-Verwaltungsdienste.

Dienst	Beschreibung
Workspace-Verwaltungskonsole	Über die Workspace-Verwaltungskonsole richten Sie den Ressourcenkatalog ein und verwalten Benutzer und Gruppen, Berechtigungen und die Berichterstellung. 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“.
Connector Services-Administrator	Auf den Administrator-Seiten für Connector-Dienste konfigurieren Sie das Verzeichnis, richten Authentifizierungsadapter ein und verwalten andere integrierte Unternehmensressourcen wie virtuelle Desktops und Remoteanwendungen. 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 Administrator-Seiten für Connector-Dienste finden Sie unter https://*Workspace_FQDN*.com:8443.
Appliance-Konfigurator	Auf den Appliance-Konfigurator-Seiten können Sie 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 Benutzernamen **`admin`** und das beim Einrichten von Workspace erstellte Administratorkennwort. Einen Link zu den Appliance-Konfigurator-Seiten finden Sie unter https://*Workspace_FQDN*.com:8443. Sie können auch über die Workspace-Verwaltungskonsole-Seite Einstellungen > Systemkonfiguration einer virtuellen Appliance auf die Appliance-Konfigurator-Seiten zugreifen.

Programm zur Verbesserung der Benutzerfreundlichkeit

Beim Installieren von Workspace können Sie sich für die Teilnahme am Programm von VMware zur Verbesserung der Kundenerfahrung entscheiden.

Wenn Sie am Programm teilnehmen, erfasst VMware anonyme Daten zu Ihrer Bereitstellung, damit VMware besser auf die Benutzeranforderungen reagieren kann. Es werden keine Daten erfasst, anhand derer sich Ihre Organisation identifizieren lässt.

VMware anonymisiert vor dem Erfassen der Daten alle Felder, die spezifische Informationen der Organisation enthalten.

Hinweis Wenn der Internetzugriff in Ihren Netzwerkkonfigurationen über einen HTTP-Proxy erfolgt, müssen Sie Ihre Proxy-Einstellungen in der Workspace-Appliance anpassen. Weitere Informationen hierzu finden Sie unter „Festlegen der Proxy-Server-Einstellungen für Workspace“, auf Seite 20

Verwalten der Konfigurationseinstellungen für die Workspace-Appliance

4

Nachdem Sie Workspace konfiguriert haben, können Sie die Seiten des Appliance Configurator aufrufen, um die aktuelle Konfiguration zu aktualisieren und Systeminformationen für die virtuelle Appliance zu überwachen.

Sie können außerdem auf den Appliance-Konfigurator-Seiten Einstellungen für die Datenbank, den FQDN, SSL-Zertifikate usw. aktualisieren oder ändern.

Tabelle 4-1. Appliance-Konfigurator-Einstellungen

Seitenname	Einstellung Beschreibung
Datenbankverbindung	Die Einstellung für die Datenbankverbindung, entweder „Intern“ oder „Extern“, ist aktiviert. Sie können den Datenbanktyp ändern. Wenn Sie „Externe Datenbank“ auswählen, geben Sie die URL, den Benutzernamen und das Kennwort für die externe Datenbank ein. Informationen zum Einrichten einer externen Datenbank finden Sie unter „Herstellen der Verbindung zu einer externen Datenbank“, auf Seite 24.
Zertifikat installieren	Auf dieser Seite installieren Sie ein benutzerdefiniertes oder selbstsigniertes Zertifikat für Workspace. Wenn Workspace mit einem Lastausgleichsdienst konfiguriert ist, können Sie das Root-Zertifikat des Lastausgleichsdienstes installieren. Auf dieser Seite wird auch der Speicherort des Workspace-Root-CA-Zertifikats angezeigt. Siehe „Verwenden von SSL-Zertifikaten in Workspace“, auf Seite 29.
Workspace-FQDN	Auf dieser Seite wird der Workspace-FQDN angezeigt. Sie können diesen ändern. Der Workspace-FQDN ist die URL, die Benutzer für den Zugriff auf Workspace verwenden.
Syslog konfigurieren	Auf dieser Seite können Sie einen externen Syslog-Server aktivieren. Workspace-Protokolle werden an diesen externen Server gesendet. Siehe „Aktivieren des Syslog-Servers“, auf Seite 29.
Kennwort ändern	Auf dieser Seite können Sie das Workspace-Administratorkennwort ändern.
Systemsicherheit	Auf dieser Seite können Sie das Root-Kennwort für die Workspace-Appliance und das Kennwort für die Remoteanmeldung als Administrator ändern.
Speicherorte der Protokolldateien	Auf dieser Seite wird eine Liste der Workspace-Protokolldateien und ihrer Verzeichnispfade angezeigt. Sie können die Protokolldateien in einer tar.zip-Datei bündeln und von dieser Seite herunterladen. Siehe „Protokolldatei-Informationen“, auf Seite 30.

Dieses Kapitel behandelt die folgenden Themen:

Ändern der Konfigurationseinstellungen für die Workspace - Appliance

Nachdem Sie Workspace konfiguriert haben, können Sie die Seiten des Appliance-Konfigurators aufrufen, um die aktuelle Konfiguration zu aktualisieren und Systeminformationen für die virtuelle Appliance zu überwachen.

Vorgehensweise

1 Melden Sie sich für den Zugriff auf die Seiten des Appliance-Konfigurators bei der Workspace-Verwaltungskonsole an.

2 Öffnen Sie die Registerkarte „Einstellungen“ und klicken Sie auf **Systemkonfiguration einer virtuellen Appliance**.

3 Melden Sie sich beim Appliance-Konfigurator mit dem Workspace-Administratorkennwort an.

4 Wählen Sie im linken Navigationsbereich die Seite aus, die Sie anzeigen möchten.

Weiter

Vergewissern Sie sich, dass die vorgenommenen Einstellungen oder Aktualisierungen wirksam sind.

Herstellen der Verbindung zu einer externen Datenbank

In der Workspace-Appliance ist eine interne PostgreSQL-Datenbank eingebettet. Wenn Sie eine externe Datenbank mit Workspace verwenden möchten, muss Ihr Datenbankadministrator eine leere externe Oracle- oder PostgreSQL-Datenbank und das entsprechende Schema vorbereiten, bevor die Verbindung mit der Datenbank in Workspace hergestellt wird.

Sie können die Verbindung zur externen Datenbank herstellen, wenn Sie den Workspace-Setup-Assistenten ausführen. Sie können auch zur Seite Appliance-Konfigurator-Datenbankverbindung navigieren, um die Verbindung zur externen Datenbank zu konfigurieren.

Lizenzierte Benutzer können eine externe Datenbank der virtuellen vPostgres-Appliance oder eine Oracle-Datenbank verwenden, um eine High Availability-Umgebung einzurichten.

Hinweis Um Ihre interne Datenbank für hohe Verfügbarkeit einzurichten, ziehen Sie KB 2094258, Using embedded vPostgres database for VMware Workspace Portal 2.1 (Verwenden einer eingebetteten vPostgres-Datenbank für VMware Workspace Portal 2.1) zurate.

Konfigurieren einer Oracle-Datenbank

Während der Oracle-Installation müssen Sie bestimmte Oracle-Konfigurationen festlegen, um eine optimale Leistung mit Workspace zu erzielen.

Voraussetzungen

In Workspace müssen Oracle-Bezeichner für den Benutzernamen und das Schema in Anführungszeichen angegeben werden. Daher müssen Sie beim Erstellen des `saas`-Benutzernamens und Schemas für Oracle doppelte Anführungszeichen verwenden.

Vorgehensweise

1 Legen Sie beim Erstellen einer Oracle-Datenbank die folgenden Einstellungen fest.

   a Wählen Sie die Konfigurationsoption **General Purpose/Transaction Processing Database** (Allzweck-/Transaktionsverarbeitungsdatenbank) aus.

   b Klicken Sie auf **Unicode > UTF8 verwenden**.

   c Verwenden Sie den nationalen Zeichensatz.

2 Stellen Sie nach Abschluss der Installation eine Verbindung mit der Oracle-Datenbank her.

3 Melden Sie sich bei der Oracle-Datenbank als sys-Benutzer an.

4 Erhöhen Sie die Prozessverbindungen. Jede zusätzliche workspace-va-VM erfordert mindestens 300 Prozessverbindungen, um mit Workspace verwendet werden zu können. Wenn Ihre Umgebung beispielsweise zwei workspace-va-VMs enthält, führen Sie den Befehl `alter` als sys- oder system-Benutzer aus.

   a Erhöhen Sie die Prozessverbindungen mit dem Befehl `alter`.

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

   b Starten Sie die Datenbank neu.

5 Erstellen Sie einen Datenbankauslöser, den alle Benutzer verwenden können.

Beispiel-SQL zum Erstellen eines Datenbankauslösers

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

6 Ausführen der Oracle-Befehle zum Erstellen eines neuen Benutzerschemas.

Beispiel-SQL zum Erstellen eines neuen Benutzers

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

Wenn Sie eine Oracle-Clusterdatenbank verwenden, finden Sie weitere Informationen zur RAC-Einrichtung in der VMware Dokumentation.

Konfigurieren einer PostgreSQL-Datenbank

Während der PostgreSQL-Installation müssen Sie bestimmte PostgreSQL-Konfigurationen festlegen, um eine optimale Leistung mit Workspace zu erzielen.

HINWEIS Workspace unterstützt derzeit kein generisches PostgreSQL.

Voraussetzungen

- Installieren und konfigurieren Sie eine unterstützte Version von VMware vFabric PostgreSQL als externen Datenbankserver aus einem der Installationspakete, z.˚B. OVA, OVF oder RPM, wobei das citext-Modul installiert sein muss. Das citext-Modul unterstützt den CITEXT-Datentyp, einen Textdatentyp, bei dem nicht zwischen Groß- und Kleinschreibung unterschieden wird. Versichern Sie sich, dass die VMware vFabric PostgreSQL-Version, die Sie verwenden, mit Ihrer Version von Workspace kompatibel ist. Informationen über unterstützte VMware vFabric PostgreSQL-Versionen finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter „http://www.vmware.com/resources/compatibility/sim/interop_matrix.php“.
- Installieren und Konfigurieren der Lastausgleichsimplementierung.
- Vergewissern Sie sich, dass Ihre Umgebung die folgenden Anforderungen erfüllt:
  - Der verwendete Datenbankserver ist PostgreSQL.
  - Der Benutzername und das Kennwort des Datenbankadministrators sind verfügbar.
  - Sie müssen einen Benutzernamen und ein Kennwort eingeben, um einen Benutzer mit der Autorisierung für das `saas`-Schema zu erstellen. Dieser Benutzer wird benötigt, wenn Sie eine Verbindung zwischen der Workspace-VA-VM-Instanz und der Datenbank herstellen.

    HINWEIS Die Workspace-VA-VM verwendet den Datenbanknamen `saas`. Während des Initialisierungsvorgangs werden alle vorhandenen Datenbanken mit dem Namen `saas` gelöscht und neu erstellt.

Vorgehensweise

1 Melden Sie sich als Root-Benutzer an.

2 Bearbeiten Sie die Datei `postgresql.conf`.

Die VMware vFabric PostgreSQL-Datenbank befindet sich beispielsweise unter `/var/vmware/vpostgres/current/pgdata/`

3 Erhöhen Sie den Parameter `max_connections`. Jede zusätzliche Workspace-VA-VM erfordert mindestens `300` Verbindungen, um korrekt mit Workspace zu arbeiten.

4 Legen Sie den Wert des Parameters `max_connections` für die zwei Workspace-VA-VMs auf **`600`** fest.

5 Starten Sie die Datenbank neu.

6 Fügen Sie eine neue Zeile zur Datei `postgresql.conf.auto` hinzu, die den folgenden `search_path='saas'`-Parameter enthält.

7 Ausführen der PostgresSQL-Befehle zum Erstellen eines neuen PostgresSQL-Datenbankschemas.

Tabelle 4-2. Erstellen einer SQL für ein neues Datenbankschema

Beispiel-SQL zum Erstellen eines neuen Datenbankschemas
CREATE ROLE horizon LOGIN PASSWORD `yourpassword` NOSUPERUSER INHERIT NOCREATEDB NOCREATEROLE NOREPLICATION; ALTER ROLE horizon SET search_path = saas; CREATE DATABASE saas WITH OWNER = postgres ENCODING = 'UTF8' TABLESPACE = pg_default CONNECTION LIMIT = -1; GRANT CONNECT, TEMPORARY ON DATABASE saas TO public; GRANT ALL ON DATABASE saas TO postgres; GRANT ALL ON DATABASE saas TO horizon; \connect saas; CREATE SCHEMA saas AUTHORIZATION horizon; CREATE EXTENSION citext SCHEMA saas;

Übertragen von Daten aus der internen Datenbank

Wenn Ihre Bereitstellung eine interne Datenbank verwendet und Sie planen, zu einer externen Datenbank zu wechseln, können Sie die vorhandenen Daten aus der Datenbank extrahieren und zu einer neuen externen Datenbank hinzufügen.

Voraussetzungen

Bereiten Sie den externen Datenbankserver vor. Siehe „Konfigurieren einer PostgreSQL-Datenbank“, auf Seite 26.

Vorgehensweise

1 Melden Sie sich als Root-Benutzer an.

2 Wechseln Sie in das Verzeichnis `/opt/vmware/vpostgres/current/bin`.

3 Führen Sie den Befehl `./pg_dump –U postgres –w ––clean –f /tmp/db_dump.data saas` aus.

4 Kopieren Sie die Datei `db_dump.data` auf den neuen, vorbereiteten externen Datenbankserver.

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

5 Melden Sie sich als Root-Benutzer beim externen Datenbankserver an.

6 Wechseln Sie in das Verzeichnis `/opt/vmware/vpostgres/current/bin`.

7 Führen Sie den Befehl `db_dump.data` aus.

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

Möglicherweise werden während der Ausführung des Befehls `db_dump.data` die Befehle `DROP` und `ALTER` angezeigt.

Hinzufügen einer externen Datenbank zur Workspace -Appliance

Nachdem Sie den Setup-Assistenten für Workspace ausgeführt haben, können Sie Workspace zur Verwendung einer anderen Datenbank konfigurieren.

Sie müssen Workspace auf eine initialisierte, gefüllte Datenbank verweisen. Sie können z.°B. eine Datenbank, die während einer erfolgreichen Ausführung des Workspace Setup-Assistenten konfiguriert wurde, eine Datenbank aus einer Sicherung oder eine vorhandene Datenbank aus einem wiederhergestellten Snapshot verwenden.

Voraussetzungen

- Installieren und konfigurieren Sie VMware vFabric PostgreSQL oder Oracle als externen Datenbankserver. Informationen zum Konfigurieren einer PostgreSQL-Datenbank für Workspace finden Sie unter „Konfigurieren einer PostgreSQL-Datenbank“, auf Seite 26. Informationen über bestimmte Oracle-Versionen, die von Workspace unterstützt werden, finden Sie in der VMware-Produkt-Interoperabilitätsmatrix unter „http://www.vmware.com/resources/compatibility/sim/interop_matrix.php“.
- Übertragen Sie Daten von der internen Datenbank, sofern Sie eine interne Datenbank verwendet haben.

Vorgehensweise

1 Klicken Sie in der Workspace-Verwaltungskonsole auf **Einstellungen** und wählen Sie **VA-Konfiguration** aus.

2 Klicken Sie auf **Manuelle Konfiguration**.

3 Melden Sie sich beim Appliance-Konfigurator mit dem Workspace-Administratorkennwort an.

4 Wählen Sie auf der Seite „Einrichtung der Datenbankverbindung“ als Datenbanktyp **Externe Datenbank** aus.

5 Geben Sie Informationen zur Datenbankverbindung ein.

a Geben Sie die JDBC-URL des Datenbankservers ein.

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

b Geben Sie den Namen des Benutzers mit Lese- und Schreibberechtigungen für die Datenbank ein.

PostgreSQL	`horizon`
Oracle	`“saas”`

c Geben Sie das Kennwort für den Benutzer ein, den Sie beim Konfigurieren Ihrer Oracle- oder PostgreSQL-Datenbank erstellt haben.

6 Klicken Sie auf **Verbindung testen**, um die Informationen zu überprüfen und zu speichern.

Aktivieren des Syslog-Servers

Workspace exportiert Ereignisse auf Anwendungsebene auf den externen Syslog-Server. Betriebssystemereignisse werden nicht exportiert.

Da die meisten Unternehmen nicht über unbegrenzten Festplattenspeicher verfügen, wird von Workspace nicht der komplette Protokollverlauf für jede virtuelle Maschine gespeichert. Wenn Sie mehr Verlaufsdaten speichern oder einen zentralen Speicherort für Ihren Protokollverlauf erstellen möchten, können Sie einen externen Syslog-Server einrichten.

Wenn Sie während der Erstkonfiguration keinen Syslog-Server konfigurieren, können Sie ihn später über die Seite „Syslog-Konfiguration“ im Appliance-Konfigurator konfigurieren.

Voraussetzungen

Richten Sie einen externen Syslog-Server ein. Sie können jeden der verfügbaren Syslog-Standardserver verwenden. Verschiedene Syslog-Server bieten erweiterte Suchfunktionen.

Vorgehensweise

1 Klicken Sie in der Workspace-Verwaltungskonsole auf **Einstellungen** und wählen Sie **VA-Konfiguration** aus.

2 Klicken Sie auf **Manuelle Konfiguration**.

3 Melden Sie sich bei Appliance-Konfigurator an.

4 Klicken Sie im linken Navigationsbereich auf **Syslog konfigurieren**.

5 Klicken Sie auf **Aktivieren**.

6 Geben Sie die IP-Adresse oder den FQDN des Servers ein, auf dem die Protokolle gespeichert werden sollen.

7 Klicken Sie auf **Speichern**.

Workspace sendet eine Kopie Ihrer Protokolle an den Syslog-Server.

Verwenden von SSL-Zertifikaten in Workspace

Wenn die Workspace-Appliance installiert ist, wird automatisch ein standardmäßiges SSL-Serverzertifikat generiert. Sie können dieses selbstsignierte Zertifikat zum Testen von Workspace verwenden. Es wird dringend empfohlen, gewerbliche SSL-Zertifikate zu generieren und installieren, wenn Workspace in einer Produktionsumgebung verwendet wird.

Eine Zertifizierungsstelle (Certificate Authority, CA) ist eine vertrauenswürdige Instanz, die die Identität des Zertifikats und seines Erstellers gewährleistet. Wenn ein Zertifikat von einer vertrauenswürdigen Zertifizierungsstelle zertifiziert ist, empfangen die Benutzer keine Nachrichten mehr, in denen sie zum Überprüfen des Zertifikats aufgefordert werden.

Wenn Sie Workspace mit dem selbstgenerierten SSL-Zertifikat bereitstellen, muss das Workspace-Root-CA-Zertifikat als vertrauenswürdige Zertifizierungsstelle für alle Clients, die auf Workspace zugreifen, verfügbar sein. Clients können Computer von Endbenutzern, Lastausgleichsdienst, Proxys usw. sein. Sie können die Workspace-Root-CA von *https://Workspace-Hostname.com/horizon_workspace_rootca.pem* herunterladen.

Sie können das Workspace-Zertifikat der Zertifizierungsstelle über die Seite Appliance-Konfigurator > Zertifikat installieren installieren. Auf dieser Seite können Sie auch das Root-CA-Zertifikat des Lastausgleichsdienstes hinzufügen. Siehe „Anwenden des Workspace-Root-Zertifikats auf den Lastausgleichsdienst“, auf Seite 45.

Anwenden einer öffentlichen Zertifizierungsstelle auf Workspace

Einige Unternehmen verwenden selbst generierte oder von anderen Zertifizierungsstellen (CAs) herausgegebene Zertifikate. Diese Zertifikate sind nicht in der Liste der vertrauenswürdigen Zertifizierungsstellen enthalten.

Sie können Workspace neue Zertifikate hinzufügen.

HINWEIS Wenn der Workspace-FQDN auf einen Lastausgleichsdienst verweist, wird das SSL-Zertifikat auf den Lastausgleichsdienst angewendet.

Voraussetzungen

Generieren Sie eine Zertifikatssignieranforderung (CSR, Certificate Signing Request) und Sie erhalten ein gültiges, signiertes Zertifikat von einer Zertifizierungsstelle. Wenn Ihre Organisation von einer Zertifizierungsstelle signierte SSL-Zertifikate bereitstellt, können Sie diese verwenden.

Vorgehensweise

1 Um das Zertifikat auf Workspace anzuwenden, klicken Sie in der Workspace-Verwaltungskonsole auf **Einstellungen** und wählen Sie **VA-Konfiguration** aus.

2 Klicken Sie auf **Manuelle Konfiguration**.

3 Melden Sie sich mit dem Workspace-Administratorkennwort beim Appliance-Konfigurator an.

4 Wählen Sie **Zertifikat installieren** aus.

5 Fügen Sie auf der Registerkarte „SSL beenden“ der Workspace-Appliance die vollständige Zertifikatkette und den privaten Schlüssel ein. Stellen Sie sicher, dass das Zertifikat den Workspace-FQDN-Hostnamen enthält.

6 Speichern Sie das SSL-Zertifikat.

Weiter

Vergewissern Sie sich, dass Benutzer sich erfolgreich anmelden können.

Protokolldatei-Informationen

Workspace-Protokolldateien können für Debugging und Fehlerbehebung hilfreich sein. Die unten aufgeführten Protokolldateien sind ein häufiger Ansatzpunkt. Weitere Protokolle finden Sie im Verzeichnis `/opt/vmware/horizon/workspace/logs`.

Tabelle 4-3. Protokolldatei-Informationen

Komponente	Speicherort der Protokolldatei	Beschreibung
Workspace-Dienstprotokolle	`/opt/vmware/horizon/workspace/logs/horizon.log`	Informationen zu Aktivitäten in der Workspace-Anwendung, z.°B. Berechtigungen, Benutzer und Gruppen.
Konfigurator-Protokolle	`/opt/vmware/horizon/workspace/logs/configurator.log`	Anforderungen, die der Konfigurator vom REST-Client und der Web-Benutzeroberfläche empfängt
Connector Protokolle	`/opt/vmware/horizon/workspace/logs/connector.log`	Ein Datensatz für jede von der Webschnittstelle empfangene Anforderung. Jeder Protokolleintrag enthält zudem die Anforderungs-URL, den Zeitstempel und Ausnahmen. Synchronisierungsaktionen werden nicht erfasst.

Tabelle 4-3. Protokolldatei-Informationen (Fortsetzung)

Komponente	Speicherort der Protokolldatei	Beschreibung
Aktualisierungs-protokolle	`/opt/vmware/var/log/update.log` `/opt/vmware/var/log/vami`	Ein Datensatz mit Ausgabemeldungen, die sich auf Aktualisierungsanforderungen während eines Upgrades von Workspace beziehen. Die Dateien im Verzeichnis `/opt/vmware/var/log/vami` sind für die Fehlerbehebung nützlich. Nach einem Upgrade können Sie diese Dateien auf allen VMs finden..
Apache Tomcat-Protokolle	`/opt/vmware/horizon/workspace/logs/catalina.log`	Apache Tomcat zeichnet Meldungen auf, die in den anderen Protokolldateien nicht aufgezeichnet werden.

Erfassen von Protokollinformationen

Bei Tests und während der Fehlerbehebung können die Protokolle Feedback über Aktivität und Leistung der virtuellen Appliance sowie Informationen über auftretende Probleme liefern.

Sie erfassen die Protokolle von jeder workspace-va-Appliance in Ihrer Umgebung.

Vorgehensweise

1 Melden Sie sich beim Appliance-Konfigurator an.

2 Öffnen Sie die Seite „Speicherorte der Protokolldateien“ und klicken Sie auf **Protokollpaket vorbereiten**.

Die Informationen werden in einer tar.gz-Datei erfasst, die heruntergeladen werden kann.

3 Laden Sie das erstellte Paket herunter.

Weiter

Wenn Sie alle Protokolle erfassen möchten, führen Sie diese Schritte für jede workspace-va-Appliance aus.

Aktualisieren von Workspace - Einstellungen über Seiten der Connector Services-Administrator

5

Nach dem Konfigurieren von Workspace können Sie auf den Seiten der Connector Services-Administrator das Workspace-Verzeichnis verwalten, Authentifizierungsadapter aktivieren oder deaktivieren, Active Directory-Benutzerattribute ändern, Active Directory-Gruppen verwalten, das Verzeichnis manuell synchronisieren und in Workspace verwendete Ressourcen, einschließlich View-Pools, Citrix-basierter Ressourcen und ThinApp-Paketen, einrichten.

Tabelle 5-1. Auf den Seiten der Connector Services-Administrator verwaltete Einstellungen

Seitenname	Einstellung
Info	Auf der Seite „Info“ werden allgemeine Informationen zu Workspace, einschließlich der Versionsnummer, angezeigt.
Konfiguration	Die Seite „Konfiguration“ ist derzeit nicht für die Workspace-Appliance verfügbar.
Domäne beitreten	Aktivieren Sie „Domäne beitreten“ und geben Sie die Informationen auf dieser Seite ein, um in Workspace View- oder ThinApp-Ressourcen zu verwenden und mithilfe von Kerberos-Windows-Authentifizierung Single Sign-on für die Webschnittstelle bereitzustellen. Sie müssen der von der Ressource verwendeten Active Directory-Domäne beitreten. Auf dieser Seite geben Sie die Active Directory-Informationen für den Benutzer ein, der über die Berechtigung für den Beitritt von Maschinen zur Active Directory-Domäne verfügt. Informationen zum Konfigurieren dieser Ressourcen finden Sie in den entsprechenden Kapiteln im *Einrichten von Ressourcen in VMware Workspace Portal*.
Methode für Verzeichnisauthentifizierung	Aktivieren Sie die Windows-Authentifizierung, um eine Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen in Workspace konfigurieren zu können. Siehe „Konfigurieren der Windows-Authentifizierung für mehrere Domänen oder Active Directory-Umgebungen in mehreren vertrauenswürdigen Strukturen“, auf Seite 38.
Identitätsanbieter	Auf der Seite „Identitätsanbieter“ wird die Identitätsanbieter-Instanz angezeigt, mit der Sie Benutzer innerhalb des Unternehmensnetzwerks bei Active Directory authentifizieren.
Authentifizierungsadapter	Auf der Seite „Authentifizierungsadapter“ werden die in Workspace verfügbaren Authentifizierungsmethoden, einschließlich Kennwortauthentifizierung, Kerberos-Authentifizierung und SecurID, angezeigt. Sie können die Authentifizierungsinformationen aktivieren und konfigurieren. Siehe Kapitel 8, „Einrichten der Benutzerauthentifizierung“, auf Seite 49.
Verzeichnis	Auf dieser Seite können Sie die Active Directory-Verbindungsinformationen anzeigen und verwalten. Siehe „Herstellen einer Verbindung zu Active Directory“, auf Seite 36.
Benutzerattribute zuordnen	Auf dieser Seite wird die Zuordnung von Active Directory-Attributen zu Workspace-Verzeichnisattributen angezeigt. Wenn Sie View-Ressourcen konfigurieren, muss auf dieser Seite das Attribut „userPrincipalName“ aktiviert sein.

Tabelle 5-1. Auf den Seiten der Connector Services-Administrator verwaltete Einstellungen (Fortsetzung)

Seitenname	Einstellung
Verzeichnissynchronisierung	Hier können Sie die Synchronisierungsplanung ändern. Beim Installieren von Workspace wurde als Standardzeitplan das Synchronisieren der Verzeichnisse einmal täglich um 23:55 Uhr festgelegt. Sie können auch die Regeln für die Verzeichnissynchronisierung zum Auswählen von Benutzern und Gruppen aus Active Directory bearbeiten.
Sicherheitsmaßnahmen für die Synchronisierung	Legen Sie Sicherheitsmaßnahmen fest, um unbeabsichtigte Änderungen an Benutzern und Gruppen zu verhindern, die infolge einer Verzeichnissynchronisierung zu Workspace hinzugefügt werden. Sie können z. B. den maximalen Prozentsatz der Benutzer festlegen, die sich gleichzeitig löschen lassen. Wenn eine Ihrer Auslöserbedingungen erfüllt wird, findet die Verzeichnissynchronisierung nicht statt, und es ist ein manueller Eingriff erforderlich. Es werden die Standardbedingungen aktiviert, deren Schutzgrad sich anpassen lässt. Auf der Registerkarte „Fehlerbehebung“ werden die Schutzwarnungen angezeigt.
Horizon DaaS-Ressourcen	Sie können Horizon DaaS als Ressource aktivieren und konfigurieren. Sie müssen auf der Seite „Benutzerattribute zuordnen“ das Attribut „distinguishedName“ aktivieren.
View-Pools	Sie können View-Pools in Workspace als Ressource aktivieren und konfigurieren. Zunächst müssen Sie auf der Seite „Domäne beitreten“ die Domänenverbindung konfigurieren und auf der Seite „Benutzerattribute zuordnen“ das Attribut „userPrincipalName“ aktivieren. Informationen zum Konfigurieren dieser Ressource finden Sie in den entsprechenden Kapiteln im *Einrichten von Ressourcen in VMware Workspace Portal*.
Veröffentlichte Apps - Citrix	Sie können Citrix-basierte Anwendungen in Workspace als Ressource aktivieren und konfigurieren. Informationen zum Konfigurieren dieser Ressource finden Sie in den entsprechenden Kapiteln im *Einrichten von Ressourcen in VMware Workspace Portal*.
App-Pakete - ThinApp	Sie können ThinApp-Pakete in Workspace als Ressource aktivieren und konfigurieren. Sie müssen zunächst auf der Seite „Domäne beitreten“ die Domäne konfigurieren. Informationen zum Konfigurieren dieser Ressource finden Sie in den entsprechenden Kapiteln im *Einrichten von Ressourcen in VMware Workspace Portal*.

Vorgehensweise

1 Rufen Sie https://*Workspace_FQDN*.com:8443 auf.

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

3 Wählen Sie im linken Navigationsbereich die Seite aus, die Sie anzeigen möchten.

Weiter

Stellen Sie sicher, dass die neuen Einstellungen oder Aktualisierungen verfügbar sind.

Verwalten der Active Directory-Verbindung mit Workspace

6

Die Active Directory-Umgebung kann aus einer einzelnen Active Directory-Domäne, mehreren Domänen in einer einzelnen Active Directory-Struktur oder mehreren Domänen in mehreren Active Directory-Strukturen bestehen. Nachdem Sie Active Directory angepasst haben, aktualisieren Sie die Konfigurationsinformationen in Workspace.

- Integration von Workspace mit Active Directory auf Seite 35

  Sie können Workspace in eine Active Directory-Umgebung integrieren, die aus einer einzelnen Active Directory-Domäne, mehreren Domänen in einer einzelnen Active Directory-Struktur oder mehreren Domänen in mehreren Active Directory-Strukturen besteht.

- Herstellen einer Verbindung zu Active Directory auf Seite 36

  Workspace verwendet für die Benutzerauthentifizierung und -verwaltung die vorhandene Active Directory-Infrastruktur. Die Active Directory-Informationen konfigurieren Sie bei der Installation und Einrichtung von Workspace.

- Einrichten einer Verbindung mit mehreren Domänen oder Domänen in mehreren vertrauenswürdigen Strukturen von Active Directory auf Seite 38

  Nach der Installation von Workspace wird eine einzelne Active Directory-Domäne konfiguriert und mit Workspace synchronisiert. Sie müssen die Windows-Authentifizierung aktivieren, um eine Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen in Workspace konfigurieren zu können.

Integration von Workspace mit Active Directory

Sie können Workspace in eine Active Directory-Umgebung integrieren, die aus einer einzelnen Active Directory-Domäne, mehreren Domänen in einer einzelnen Active Directory-Struktur oder mehreren Domänen in mehreren Active Directory-Strukturen besteht.

Wenn Sie Workspace installieren, verbinden Sie Workspace mit einer einzelnen Active Directory-Domäne. Bei mehreren Domänen können Sie Workspace nach der Installation auf den Connector Services-Administrator-Seiten in die bestehende Active Directory-Umgebung integrieren.

Active Directory-Umgebung mit einer einzelnen Domäne

Eine einzelne Active Directory-Bereitstellung ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus einer einzelnen Active Directory-Domäne heraus. Informationen zur Installation von Workspace in einer einzelnen Active Directory-Domäne finden Sie unter „Herstellen einer Verbindung zu Active Directory“, auf Seite 36.

Active Directory-Umgebung mit mehreren Domänen in einer einzelnen Struktur

Die Active Directory-Bereitstellung mit mehreren Domänen in einer einzelnen Struktur ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in einer einzelnen Struktur heraus.

Sie aktivieren die Windows-Authentifizierung als Methode für die Verzeichnisauthentifizierung, um für Workspace eine Active Directory-Umgebung mit mehreren Domänen in einer einzelnen Struktur konfigurieren zu können.

Informationen zur Installation von Workspace in einer Active Directory-Umgebung mit mehreren Domänen in einer einzelnen Struktur finden Sie unter „Konfigurieren der Windows-Authentifizierung für mehrere Domänen oder Active Directory-Umgebungen in mehreren vertrauenswürdigen Strukturen“, auf Seite 38.

Active Directory-Umgebung mit mehreren Strukturen und Vertrauensbeziehungen

Eine Active Directory-Bereitstellung mit mehreren Strukturen und Vertrauensbeziehungen ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in Strukturen heraus, bei denen zwischen den Domänen gegenseitige Vertrauensbeziehungen bestehen.

Sie aktivieren die Windows-Authentifizierung als Methode für die Verzeichnisauthentifizierung, um für Workspace eine Active Directory-Umgebung mit mehreren Strukturen konfigurieren zu können.

Informationen zur Installation von Workspace in einer Active Directory-Umgebung mit mehreren Strukturen in einer Vertrauensbeziehung finden Sie unter „Konfigurieren der Windows-Authentifizierung für mehrere Domänen oder Active Directory-Umgebungen in mehreren vertrauenswürdigen Strukturen“, auf Seite 38.

Active Directory-Umgebung mit mehreren Strukturen, aber ohne Vertrauensbeziehungen

Eine Active Directory-Bereitstellung mit mehreren Strukturen, aber ohne Vertrauensbeziehungen ermöglicht Ihnen die Synchronisierung von Benutzern und Gruppen aus mehreren Active Directory-Domänen in mehreren Strukturen heraus, bei denen zwischen den Domänen keine gegenseitigen Vertrauensbeziehungen bestehen. Bei dieser Bereitstellung muss die Benutzerspeicher-Technologie von Workspace verwendet werden.

Wenden Sie sich an VMware Professional Services, um mehr über die Active Directory-Umgebung mit mehreren Strukturen, aber ohne Vertrauensbeziehungen zu erfahren.

Herstellen einer Verbindung zu Active Directory

Workspace verwendet für die Benutzerauthentifizierung und -verwaltung die vorhandene Active Directory-Infrastruktur. Die Active Directory-Informationen konfigurieren Sie bei der Installation und Einrichtung von Workspace.

Erforderliche Active Directory-Informationen

Workspace verwendet die folgenden Active Directory-Informationen, um die Anmeldedaten der Endbenutzer bei der Anmeldung zu überprüfen. Sie konfigurieren diese Informationen bei der Installation von Workspace.

Server-Host	Active Directory-Hostadresse.
SSL verwenden	Wenn Sie für die Verbindung mit Active Directory SSL verwenden, konfigurieren Sie diese Einstellung und fügen das Zertifikat im Zertifikatfeld hinzu.

DNS-Dienstspeicherort verwenden	Wenn Sie den Hostnamen und die Portnummer des Servers nicht kennen, aktivieren Sie „DNS-Dienstspeicherort verwenden“. Workspace verwendet Datensätze für den DNS-Dienstspeicherort, um die Active Directory-Domäne zu finden.
Server-Port	Die Portnummer für den Active Directory-Host. Der Standardport für LDAP ist 389. Der Standardport für LDAP over SSL ist 636.
Suchattribut	Das Active Directory-Kontoattribut, das den Benutzernamen enthält. Die meisten Bereitstellungen von Active Directory-Domänendiensten verwenden **`sAMAccountName`**.
Basis-DN	Der Basis-DN, der als Startpunkt für Verzeichnisserver-Suchvorgänge verwendet wird. Beispiel: DC=mycompany, DC=com. Der Connector startet von diesem DN aus mit der Erstellung von Master-Listen, aus denen Sie später einzelne Benutzer herausfiltern und zu denen Sie Gruppen hinzufügen können.
Bind-DN	Der Bind-DN des Active Directory-Benutzerkontos mit Berechtigungen zum Suchen von Benutzern. Der Benutzerdatensatz des Bind-DN-Kontos in Active Directory muss einen Benutzernamen, den Vornamen, den Nachnamen, die E-Mail-Adresse, alle erforderlichen erweiterten Attribute und ein in Active Directory definiertes DN-Attribut umfassen. Dieser Benutzer wird der Administrator für die Workspace-Bereitstellung. Sie können über Workspace-Verwaltungskonsole andere Active Directory-Benutzer auf die Administratorrolle heraufstufen. **Hinweis** Wenn eine Active Directory-Umgebung in mehreren Strukturen konfiguriert wurde und die lokale Domänengruppe Mitglieder aus Domänen in verschiedenen Strukturen enthält, muss der auf der Workspace-Verzeichnisseite verwendete Bind-DN-Benutzer zur Administratorgruppe der Domäne hinzugefügt werden, in der sich die lokale Domänengruppe befindet. Wird dies versäumt, fehlen diese Benutzer in der lokalen Domänengruppe. Die folgenden Beispiele verdeutlichen bewährte Vorgehensweisen für die Auswahl von Basis-DN und Bind-DN: ■ Basis-DN: dc=example, dc=com. Verwenden Sie die oberste Ebene für den Basis-DN, damit alle Benutzer und Gruppen eingeschlossen sind. ■ Bind-DN: cn=admin user, ou=users, dc=example, dc=com. Stellen Sie sicher, dass der Bind-DN im ausgewählten Basis-DN enthalten ist.
Bind-Kennwort	Das Active Directory-Kennwort für das Bind-DN-Konto.

Auswählen von Active Directory-Benutzern und -Gruppen zum Synchronisieren mit Workspace

Wenn Sie die Active Directory-Verbindung in Workspace konfigurieren, richten Sie einen Basis-DN als Punkt ein, von dem aus nach Benutzern gesucht wird. Diese Seite umfasst alle Benutzer. Wenn Sie die Anzahl der Benutzer einschränken möchten, die mit Workspace synchronisiert werden, können Sie auf Benutzerattributen basierende Suchfilter erstellen, um bestimmte Benutzertypen auszuschließen.

Zum Suchen von Benutzern wird der von Ihnen eingerichtete Basis-DN verwendet. Wenn Sie Gruppen in die Suche einbeziehen möchten, können Sie Filter erstellen, um dem Workspace-Verzeichnis bestimmte Typen von Gruppen hinzuzufügen.

Bevor Sie in Workspace Filter erstellen und Gruppen hinzufügen, lassen Sie sich vom Active Directory-Administrator die Struktur Ihres Active Directory erläutern, um die richtigen Benutzer und Gruppen zum Synchronisieren auszuwählen.

Verwenden von Filtern zum Hinzufügen von Benutzern und Gruppen

Wählen Sie die Benutzer und Gruppen aus, die Sie mit Workspacesynchronisieren möchten. Die erste Synchronisierung findet während der Ersteinrichtung von Workspace statt. Auf den Connector Services-Administrator-Seiten können Sie jederzeit Änderungen vornehmen.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator an.

2 Wählen Sie die Seite „Verzeichnissynchronisierung“ aus und klicken Sie auf **Regeln für die Verzeichnissynchronisierung bearbeiten**.

3 Auf der Seite „Benutzer auswählen“ wird im Textfeld „Basis-DN für Benutzer“ der vorhandene Basis-DN angegeben. Um einen weiteren Basis-DN hinzuzufügen, klicken Sie auf **Weitere hinzufügen**.

4 Zum Ausschließen bestimmter Benutzertypen wählen Sie im Dropdown-Menü **Filter zum Ausschluss von Benutzern anwenden** das Benutzerattribut, nach dem gefiltert werden soll, und die Abfrageregel aus und fügen Sie den Wert hinzu.

5 Klicken Sie auf **Weitere hinzufügen**, um weitere Filter hinzuzufügen.

6 Klicken Sie auf **Weiter**, um Gruppen hinzuzufügen.

7 Um in der Liste „Ausgewählte Gruppen“ bestimmte Gruppen zu finden, geben Sie in das Textfeld **Gruppennamenfilter** den hinzuzufügenden Gruppennamen ein.

8 Klicken Sie auf **Hinzufügen** und wählen Sie die einzubeziehenden Gruppennamen aus.

9 Klicken Sie auf **Weiter**.

Auf der Seite „An Workspace weitergeben“ wird die Anzahl der Benutzer und Gruppen angezeigt, die Sie zum Hinzufügen zu Workspace ausgewählt haben.

10 Klicken Sie auf **Speichern und fortsetzen**.

Active Directory wird mit Workspace synchronisiert.

Einrichten einer Verbindung mit mehreren Domänen oder Domänen in mehreren vertrauenswürdigen Strukturen von Active Directory

Nach der Installation von Workspace wird eine einzelne Active Directory-Domäne konfiguriert und mit Workspace synchronisiert. Sie müssen die Windows-Authentifizierung aktivieren, um eine Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen in Workspace konfigurieren zu können.

Hinweis Wenn Sie Windows-Authentifizierung aktivieren, wird die Verzeichniskonfiguration so geändert, dass das Feld „DNS-Dienstspeicherort“ aktiviert wird. Wenn Sie die integrierte SRV-Suche außer Kraft setzen möchten, ziehen Sie „Erstellen einer Domänenhost-Suchdatei, um DNS-Dienstspeicherort-Suchvorgänge (SRV) außer Kraft zu setzen“, auf Seite 42 zurate.

Um Workspace für die Bereitstellung einer interaktiven Windows-Benutzerauthentifizierung zu konfigurieren, müssen Sie Workspace der Active Directory-Domäne hinzufügen, die Windows-Authentifizierung in Workspace aktivieren und Benutzer und Gruppen mit Workspace synchronisieren.

Konfigurieren der Windows-Authentifizierung für mehrere Domänen oder Active Directory-Umgebungen in mehreren vertrauenswürdigen Strukturen

Um Workspace für die Bereitstellung einer interaktiven Windows-Authentifizierung für mehrere Domänen oder Active Directory-Umgebungen in mehreren vertrauenswürdigen Strukturen zu konfigurieren, müssen Sie Workspace der Active Directory-Domäne hinzufügen, die Windows-Authentifizierung aktivieren und Benutzer und Gruppen mit Workspace synchronisieren.

Vorgehensweise

1 Hinzufügen von Workspace zu Active Directory-Umgebungen mit mehreren Domänen oder Domänen in mehreren vertrauenswürdigen Strukturen auf Seite 39

Wenn Sie eine Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen mit der interaktiven Windows-Authentifizierungsmethode konfigurieren möchten, müssen Sie die Workspace-Appliance der Active Directory-Domäne hinzufügen.

2 Aktivieren des Zugriffs auf die Windows-Authentifizierung für eine vertrauenswürdige Active Directory-Domäne in mehreren Strukturen auf Seite 40

   Um Workspace für die Bereitstellung der interaktiven Windows-Authentifizierung zu konfigurieren, müssen Sie zunächst Workspace der Active Directory-Umgebung mit mehreren vertrauenswürdigen Strukturen hinzufügen und dann die Windows-Authentifizierung in Workspace aktivieren.

3 Auswählen von Benutzern und Gruppen zum Synchronisieren mit Workspace auf Seite 40

   Bevor Sie Benutzer und Gruppen aus Active Directory-Domänen mit Workspace synchronisieren, schränken Sie den Typ von Benutzern ein, die Workspace hinzugefügt werden können, und wählen Sie die Gruppen aus, die aus den verschiedenen Domänen hinzugefügt werden sollen.

4 Hinzufügen mehrerer Domänennamen zur Anmeldeseite auf Seite 41

   Nach der Konfiguration der Windows-Authentifizierung für mehrere Active Directory-Domänen aktivieren Sie den Kennwortadapter, um die Domänen der Benutzeranmeldeseite hinzuzufügen. Die Benutzer können bei der Anmeldung bei Workspace ihre Domäne aus der Dropdown-Liste auswählen.

5 Erstellen einer Domänenhost-Suchdatei, um DNS-Dienstspeicherort-Suchvorgänge (SRV) außer Kraft zu setzen auf Seite 42

   Wenn Sie Windows-Authentifizierung aktivieren, wird die Verzeichniskonfiguration so geändert, dass das Feld „DNS-Dienstspeicherort“ aktiviert wird. Um die integrierte SRV-Suche außer Kraft zu setzen, können Sie eine Datei namens `domain_krb.properties` erstellen und die Domäne zu Hostwerten hinzufügen, die Vorrang vor der SRV-Suche haben.

Hinzufügen von Workspace zu Active Directory-Umgebungen mit mehreren Domänen oder Domänen in mehreren vertrauenswürdigen Strukturen

Wenn Sie eine Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen mit der interaktiven Windows-Authentifizierungsmethode konfigurieren möchten, müssen Sie die Workspace-Appliance der Active Directory-Domäne hinzufügen.

Voraussetzungen

- Stellen Sie sicher, dass Sie über einen Active Directory-Domänennamen sowie den Benutzernamen und das Kennwort eines Kontos in diesem Active Directory verfügen, das die erforderlichen Rechte besitzt, um der Domäne beizutreten.

Vorgehensweise

1 Melden Sie sich als Administrator für Connector-Dienste an.

2 Wählen Sie die Seite **Domäne beitreten** aus.

3 Geben Sie im Textfeld **AD-Domäne** den vollqualifizierten Namen der Active Directory-Domäne ein.

4 Geben Sie im Textfeld **AD-Benutzername** den Benutzernamen eines Kontos in Active Directory ein, das über die erforderlichen Berechtigungen verfügt, um mit Systemen einer Active Directory-Domäne beizutreten.

5 Geben Sie im Textfeld **AD-Kennwort** das Kennwort für den AD-Benutzernamen ein. Dieses Kennwort wird von Workspace nicht gespeichert.

6 Klicken Sie auf **Domäne beitreten**.

Die Seite „Domäne beitreten“ wird aktualisiert und es wird eine Meldung angezeigt, dass Sie der Domäne beigetreten sind.

Weiter

Aktivieren Sie die Windows-Authentifizierung, um auf die Active Directory-Umgebung mit mehreren Domänen, einzelner Struktur oder mehreren vertrauenswürdigen Strukturen zugreifen zu können.

Aktivieren des Zugriffs auf die Windows-Authentifizierung für eine vertrauenswürdige Active Directory-Domäne in mehreren Strukturen

Um Workspace für die Bereitstellung der interaktiven Windows-Authentifizierung zu konfigurieren, müssen Sie zunächst Workspace der Active Directory-Umgebung mit mehreren vertrauenswürdigen Strukturen hinzufügen und dann die Windows-Authentifizierung in Workspace aktivieren.

Voraussetzungen

Stellen Sie sicher, dass Sie Workspace der Active Directory-Domäne hinzugefügt haben.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator an.

2 Wählen Sie die Seite **Methode für Verzeichnisauthentifizierung** aus.

3 Klicken Sie auf **Windows-Authentifizierung aktivieren**.

4 Klicken Sie auf **Speichern**.

Die Windows-Authentifizierung wird aktiviert. Workspace aktualisiert die Verzeichnisseite und die Seite „PasswordIdpAdapter“ für Authentifizierungsadapter, indem dem Feld „DNS-Dienstspeicherort verwenden“ ein Häkchen hinzugefügt und das Bind-DN-Kontoformat in „sAMAccountName“ geändert wird.

Wenn Active Directory die Domänen mit Workspace synchronisiert hat, wird der Seite „Methode für Verzeichnisauthentifizierung“ eine Liste von Domänen hinzugefügt. Wenn die Authentifizierung per Kennwortadapter auf der Seite „PasswordldpAdapter“ für Authentifizierungsadapter aktiviert wurde, werden die Domänennamen der Benutzeranmeldeseite hinzugefügt.

Weiter

Wenn eine Active Directory-Umgebung in mehreren Strukturen konfiguriert wurde und die lokale Domänengruppe Mitglieder aus Domänen in verschiedenen Strukturen enthält, muss der auf der Workspace-Verzeichnisseite verwendete Bind-DN-Benutzer zur Administratorgruppe der Domäne hinzugefügt werden, in der sich die lokale Domänengruppe befindet. Wird dies versäumt, fehlen diese Benutzer in der lokalen Domänengruppe.

Wählen Sie Benutzer und Gruppen aus den Active Directory-Domänen aus und synchronisieren Sie Active Directory mit Workspace.

Auswählen von Benutzern und Gruppen zum Synchronisieren mit Workspace

Bevor Sie Benutzer und Gruppen aus Active Directory-Domänen mit Workspace synchronisieren, schränken Sie den Typ von Benutzern ein, die Workspace hinzugefügt werden können, und wählen Sie die Gruppen aus, die aus den verschiedenen Domänen hinzugefügt werden sollen.

Voraussetzungen

Erstellen Sie eine Liste der Active Directory-Benutzerattribute, die Sie als Filter verwenden möchten, und eine Liste von Gruppen, die Sie Workspace hinzufügen möchten.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator an.

2 Wählen Sie die Seite „Verzeichnissynchronisierung“ aus. Klicken Sie auf **Regeln für die Verzeichnissynchronisierung bearbeiten**.

3 Auf der Seite „Benutzer auswählen“ wird in den Textfeldern „Basis-DN für Benutzer“ die vorhandene Basis-DN-Konfiguration angegeben. Um einen weiteren Basis-DN hinzuzufügen, klicken Sie auf **Weitere hinzufügen**.

4 Zum Ausschließen bestimmter Benutzertypen wählen Sie im Dropdown-Menü **Filter zum Ausschluss von Benutzern anwenden** das Benutzerattribut, nach dem gefiltert werden soll, und die Abfrageregel aus und fügen Sie den Wert hinzu.

5 Klicken Sie auf **Weitere hinzufügen**, um weitere Filter hinzuzufügen.

6 Klicken Sie auf **Weiter**, um Gruppen hinzuzufügen.

7 Gruppen, die in Active Directory erstellt wurden, werden auf der Seite „Ausgewählte Gruppen“ aufgelistet. Um bestimmte Gruppen zu finden, geben Sie in das Textfeld **Gruppennamenfilter** den hinzuzufügenden Gruppennamen ein.

8 Klicken Sie auf **Hinzufügen** und wählen Sie die einzubeziehenden Gruppennamen aus.

9 Klicken Sie auf **Weiter**.

Auf der Seite „An Workspace weitergeben“ wird die Anzahl der Benutzer und Gruppen angezeigt, die Sie zum Hinzufügen zu Workspace ausgewählt haben.

10 Klicken Sie auf **Speichern und fortsetzen**.

Die Benutzer und Gruppen in den Active Directory-Domänen werden mit Workspace synchronisiert. Die Domänennamen werden beim Synchronisieren mit Workspace der Seite „Methode für Verzeichnisauthentifizierung“ hinzugefügt.

Weiter

Aktivieren Sie die Kennwortadapter-Funktion, damit die Active Directory-Domänennamen der Benutzeranmeldeseite hinzugefügt werden. Die Benutzer wählen bei der Anmeldung ihre Domäne aus.

Hinzufügen mehrerer Domänennamen zur Anmeldeseite

Nach der Konfiguration der Windows-Authentifizierung für mehrere Active Directory-Domänen aktivieren Sie den Kennwortadapter, um die Domänen der Benutzeranmeldeseite hinzuzufügen. Die Benutzer können bei der Anmeldung bei Workspace ihre Domäne aus der Dropdown-Liste auswählen.

Voraussetzungen

Um die Verbindung mit mehreren Domänen oder vertrauenswürdigen Domänen in mehreren Strukturen herstellen zu können, muss in Workspace die Windows-Authentifizierungsmethode aktiviert werden.

Die Active Directory-Domänen werden mit Workspace synchronisiert.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator an.

2 Öffnen Sie die Seite „Authentifizierungsadapter“ und klicken Sie in der Zeile „PasswordldpAdapter“ auf **Bearbeiten**.

3 Wählen Sie **Kennwortadapter aktivieren**.

4 Klicken Sie auf **Speichern**.

Die Domänennamen werden einer Dropdown-Liste auf der Benutzeranmeldeseite hinzugefügt.

Erstellen einer Domänenhost-Suchdatei, um DNS-Dienstspeicherort-Suchvorgänge (SRV) außer Kraft zu setzen

Wenn Sie Windows-Authentifizierung aktivieren, wird die Verzeichniskonfiguration so geändert, dass das Feld „DNS-Dienstspeicherort“ aktiviert wird. Um die integrierte SRV-Suche außer Kraft zu setzen, können Sie eine Datei namens `domain_krb.properties` erstellen und die Domäne zu Hostwerten hinzufügen, die Vorrang vor der SRV-Suche haben.

Vorgehensweise

1 Melden Sie sich an der workspace-va-Befehlszeile als Benutzer mit Root-Berechtigungen an.

2 Ändern Sie die Verzeichnisse in `/usr/local/horizon/conf` und erstellen Sie eine Datei mit dem Namen `domain_krb.properties`.

3 Bearbeiten Sie die Datei „domain_krb.properties“ und fügen Sie die Liste der Domänen zu den Hostwerten hinzu. Fügen Sie die Informationen als `<AD Domain>=<host:port>, <host2:port2>, <host2:port2>` hinzu.

   Geben Sie die Liste z. B. als `example.com=examplehost.com:636, examplehost2.example.com:389` ein.

4 Ändern Sie den Besitzer der Datei „domain_krb.properties“ in „horizon“ und gruppieren Sie unter „www“. Geben Sie **`chown horizon:www /usr/local/horizon/conf/domain_krb.properties`** ein.

5 Starten Sie Workspace neu. Geben Sie **`service horizon-workspace restart`** ein.

Erweiterte Konfiguration für die VMware Workspace Portal -Appliance

7

Nachdem Sie die Basisinstallation von Workspace abgeschlossen haben, müssen Sie möglicherweise weitere Konfigurationsaufgaben ausführen, z. B. das Aktivieren des externen Zugriffs auf Workspace oder das Klonen von virtuellen Maschinen.

Das Diagramm der Workspace-Architektur verdeutlicht, was Sie in der Workspace-Umgebung erstellen können. Unter Kapitel 2, „Vorbereiten der Installation von VMware Workspace Portal“, auf Seite 7 finden Sie eine typische Bereitstellung.

- Aktivieren des externen Zugriffs auf Workspace mithilfe eines Lastausgleichsdienstes auf Seite 43

  Workspace wird während der Bereitstellung im internen Netzwerk eingerichtet. Wenn Sie Benutzern außerhalb des Netzwerks Zugriff auf Workspace bereitstellen möchten, müssen Sie einen Lastausgleichsdienst, z. B. Apache, nginx, F5 usw., in der DMZ installieren.

- Konfigurieren von Redundanz/Failover für Workspace-VAs auf Seite 45

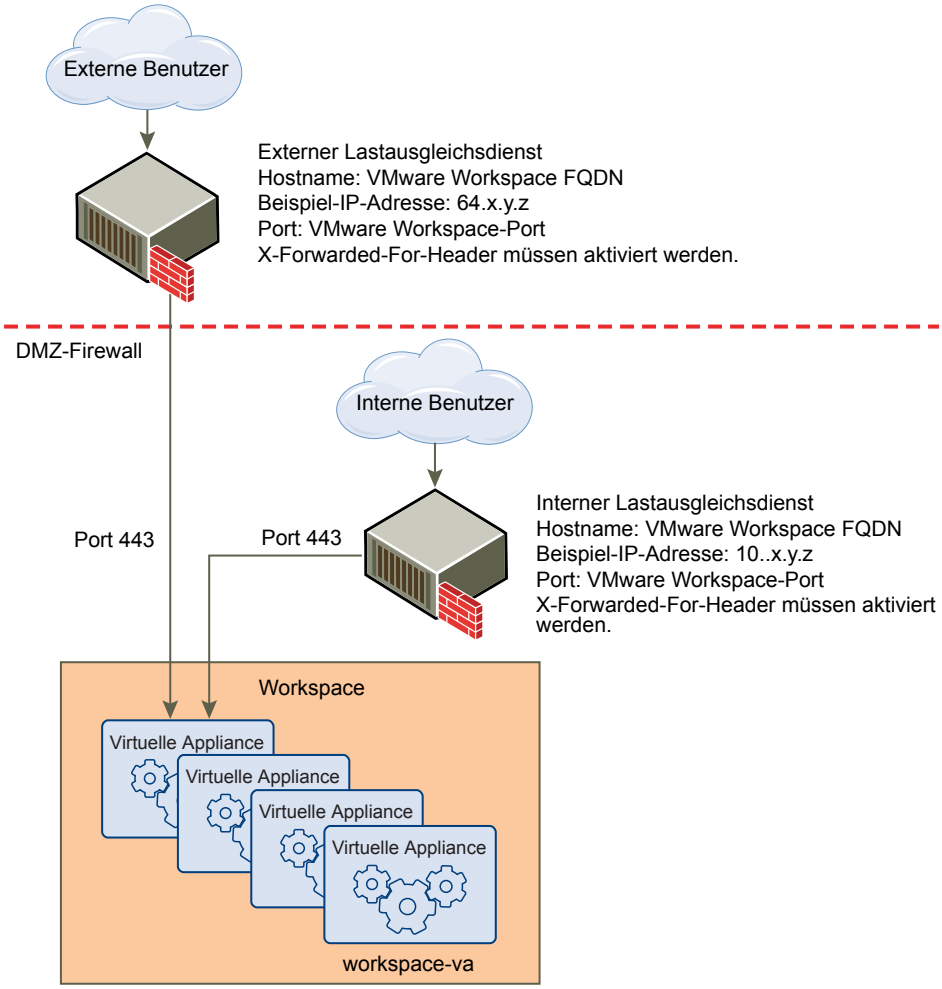
  Mit Workspace erreichen Unternehmen Failover und Redundanz, indem sie mehrere workspace-va-VAs zum Workspace-Cluster hinzufügen. Wenn eine der virtuellen Appliances ausfällt, ist Workspace weiterhin verfügbar.

Aktivieren des externen Zugriffs auf Workspace mithilfe eines Lastausgleichsdienstes

Workspace wird während der Bereitstellung im internen Netzwerk eingerichtet. Wenn Sie Benutzern außerhalb des Netzwerks Zugriff auf Workspace bereitstellen möchten, müssen Sie einen Lastausgleichsdienst, z. B. Apache, nginx, F5 usw., in der DMZ installieren.

Wenn Sie keinen Lastausgleichsdienst verwenden, können Sie die Anzahl der Workspace-VMs zukünftig nicht erweitern. Möglicherweise müssen Sie weitere Workspace-VMs hinzufügen, um Redundanz und Lastausgleich zu ermöglichen. Im folgenden Diagramm ist die Basis-Bereitstellungsarchitektur dargestellt, die Sie verwenden können, um den externen Zugriff zuzulassen.

Abbildung 7-1. Externer Lastausgleichsdienst-Proxy mit VM



Festlegen des Workspace -FQDN während der Bereitstellung

Während der Bereitstellung müssen Sie für die Workspace-VM den Workspace-FQDN und die Workspace-Portnummer eingeben. Diese Werte müssen auf den Hostnamen verweisen, auf den Endbenutzer zugreifen sollen.

Die Workspace-VM wird immer über Port 443 ausgeführt. Sie können für den Lastausgleichsdienst eine andere Portnummer verwenden. Wenn Sie eine andere Portnummer verwenden, müssen Sie diese während der Bereitstellung angeben.

Einstellungen im Lastausgleichsdienst zum Konfigurieren für Workspace

Die Einstellungen des Lastausgleichsdienstes zum Konfigurieren für Workspace umfassen das Aktivieren von „X-Forwarded-For“-Kopfzeilen, das richtige Festlegen der Lastausgleichsdienst-Zeitüberschreitung und das Aktivieren von Sticky-Sitzungen. Außerdem muss ein SSL-Vertrauensverhältnis zwischen Workspace und dem Lastausgleichsdienst konfiguriert werden.

- „X-Forwarded-For“-Kopfzeilen. Sie müssen "X-Forwarded-For"-Kopfzeilen auf dem Lastausgleichsdienst aktivieren. Dadurch wird zudem die Authentifizierungsmethode bestimmt. Weitere Informationen finden Sie in der vom Anbieter des Lastausgleichsdienstes bereitgestellten Dokumentation.

- Lastausgleichsdienst-Zeitüberschreitung. Damit Workspace ordnungsgemäß funktioniert, müssen Sie möglicherweise den Zeitüberschreitungswert für die Anforderungen des Lastausgleichsdienstes erhöhen. Der Wert wird in Minuten angegeben. Wenn der eingestellte Wert für die Zeitüberschreitung zu niedrig ist, wird möglicherweise folgender Fehler angezeigt: "Fehler 502: Der Dienst ist derzeit nicht verfügbar".
- Aktivieren einer „Sticky-Sitzung“ auf dem Lastausgleichsdienst für Workspace. Stellen Sie sicher, dass Sie "Sticky-Sitzung" im Lastausgleichsdienst für die workspace-va-Server aktivieren, wenn Ihre Bereitstellung mehrere Workspace-Server umfasst. "Sticky-Sitzung" verbessert die Leistung der Webschnittstelle. Wenn "Sticky-Sitzung" nicht aktiviert ist, schlagen möglicherweise einzelne Funktionen fehl.

Anwenden des Workspace -Root-Zertifikats auf den Lastausgleichsdienst

Wenn Workspace mit einem Lastausgleichsdienst konfiguriert ist, müssen Sie ein SSL-Vertrauensverhältnis zwischen dem Lastausgleichsdienst und Workspace einrichten. Das Workspace-Root-Zertifikat muss in den Lastausgleichsdienst kopiert werden. Das Zertifikat kann von der Seite „Appliance-Konfigurator“ unter „Zertifikat installieren“ heruntergeladen werden.

Wenn der Workspace-FQDN auf einen Lastausgleichsdienst verweist, kann das SSL-Zertifikat nur auf den Lastausgleichsdienst angewendet werden. Da der Lastausgleichsdienst mit der Workspace-VM kommuniziert, müssen Sie das Workspace-Stamm-CA-Zertifikat als vertrauenswürdiges Stammzertifikat auf den Lastausgleichsdienst kopieren.

Vorgehensweise

1 Klicken Sie in der Workspace-Verwaltungskonsole auf **Einstellungen** und wählen Sie **VA-Konfiguration** aus.

2 Klicken Sie auf **Manuelle Konfiguration**.

3 Melden Sie sich beim Appliance-Konfigurator mit dem Workspace-Administratorkennwort an.

4 Wählen Sie **Zertifikat installieren** aus.

5 Wählen Sie die Registerkarte „SSL auf einem Lastausgleichsdienst beenden“ aus und klicken Sie im Feld „Root-CA-Zertifikat der Appliance“ auf den Link `https://workspacehostname/horizon_workspace_rootca.pem`.

   Das Workspace-Root-Zertifikat wird angezeigt.

6 Kopieren Sie das Root-Zertifikat und fügen Sie es in das richtige Verzeichnis in den einzelnen Lastausgleichsdiensten ein. Weitere Informationen finden Sie in der vom Anbieter des Lastausgleichsdienstes bereitgestellten Dokumentation.

Weiter

Kopieren Sie das Lastausgleichsdienst-Root-Zertifikat und fügen Sie es in die Workspace Appliance-Konfigurator-Seite „Zertifikat installieren“ > „SSL auf einem Lastausgleichsdienst beenden“ ein.

Konfigurieren von Redundanz/Failover für Workspace -VAs

Mit Workspace erreichen Unternehmen Failover und Redundanz, indem sie mehrere workspace-va-VAs zum Workspace-Cluster hinzufügen. Wenn eine der virtuellen Appliances ausfällt, ist Workspace weiterhin verfügbar.

Zum Einrichten von Failover in Workspace klonen Sie die workspace-va-VA. Durch Klonen der virtuellen Appliance wird ein Duplikat der virtuellen Appliance erstellt, die die gleiche Konfiguration wie das Original aufweist. Sie können die geklonte virtuelle Appliance anpassen, um ihren Namen, Netzwerkeinstellungen und andere Eigenschaften nach Bedarf zu ändern.

Die IP-Adresse der geklonten virtuellen Appliance muss dieselben Richtlinien erfüllen wie die IP-Adresse der Original-VA. Die IP-Adresse muss über Forward- und Reverse-DNS in einen gültigen Hostnamen aufgelöst werden.

Alle Knoten im Cluster sind identische und nahezu statusfreie Kopien. In den geklonten virtuellen Appliances ist das Synchronisieren mit Active Directory und mit allen in Workspace konfigurierten Ressourcen, z. B. View oder ThinApp, deaktiviert.

Erstellen mehrerer Workspace-VAs

Um Failover-Funktionen bereitzustellen, können Unternehmen die Workspace-VA-VA klonen, um mehrere virtuelle Appliances desselben Typs zu erstellen und damit den Datenverkehr zu verteilen und potenzielle Ausfallzeiten zu verkürzen.

Durch Verwendung mehrerer Workspace-VA-VAs verbessern Sie die Verfügbarkeit, erreichen einen Lastausgleich für Anforderungen an Workspace und verringern die Antwortzeiten für die Endbenutzer.

Voraussetzungen

- Die virtuelle Appliance muss hinter einem Lastausgleichsdienst konfiguriert werden. Stellen Sie sicher, dass als Port für den Lastausgleichsdienst 443 verwendet wird. Verwenden Sie für diesen Zweck nicht 8443, da diese Portnummer für Verwaltungszwecke von Workspace genutzt wird und für jede virtuelle Appliance eindeutig ist.
- Es muss entweder eine externe Datenbank – konfiguriert wie unter „Herstellen der Verbindung zu einer externen Datenbank“, auf Seite 24 beschrieben – oder eine interne Datenbank – konfiguriert wie unter VMware KB 2094258, Using embedded vPostgres in Production for VMware Workspace Portal VA 2.1 (Verwenden eingebetteter vPostgres in Produktionsumgebungen für VMware Workspace Portal VA 2.1) beschrieben – eingerichtet werden, um zusätzliche virtuelle Workspace-VA-Appliances hinzuzufügen.
- Der VMware vSphere Client oder vSphere Web Client wird zum Klonen der virtuellen Appliance und für den Zugriff auf die geklonte virtuelle Appliance zum Konfigurieren des Netzwerks benötigt.
- Hinzufügen einer IP-Adresse zu den Eigenschaften der geklonten virtuellen Appliance auf Seite 47

  Bevor Sie eine geklonte virtuelle Appliance einschalten, müssen Sie eine neue IP-Adresse zuweisen. Die IP-Adresse muss im DNS aufgelöst werden können. Wenn die Adresse nicht im Reverse-DNS vorhanden ist, müssen Sie außerdem den Hostnamen zuweisen.
- Aktivieren der SecurID-Authentifizierung auf Seite 48

  In vielen Fällen haben Unternehmen für Endbenutzer, die aus externen Netzwerken zugreifen, die RSA SecurID-basierte Authentifizierung aktiviert. Nachdem Sie die virtuelle Appliance Workspace-VA geklont haben, müssen Sie bei Verwendung der RSA SecureID-Authentifizierung den Hostnamen und die IP-Adresse des geklonten Workspace zum RSA-Server hinzufügen und einen neuen Agent auf der geklonten virtuellen Appliance erstellen.
- Aktivieren der Kerberos-Authentifizierung auf Seite 48

  Unternehmen können die Kerberos-Authentifizierung für ihre Endbenutzer aktivieren, die die Verbindung von internen Windows-Computern aus herstellen. Bei Verwendung der Kerberos-Authentifizierung können Endbenutzer sich ohne Eingabe des Benutzernamens und des Kennworts bei Workspace anmelden. Wenn Sie die Workspace-VA geklont haben und die Kerberos-Authentifizierung verwenden, müssen Sie der Domäne erneut beitreten und die Kerberos-Authentifizierung für die geklonte virtuelle Maschine aktivieren.

Vorgehensweise

1 Schalten Sie die zu klonende workspace-va-VA aus.

2 Klicken Sie mit der rechten Maustaste auf die zu klonende virtuelle Appliance und klicken Sie auf **Weiter**.

3 Geben Sie den gewünschten Namen für diese geklonte virtuelle Appliance ein. Der Name muss innerhalb des VA-Ordners eindeutig sein.

4 Wählen Sie den Host oder Cluster aus, auf dem die geklonte virtuelle Appliance ausgeführt werden soll.

5 Wählen Sie den Ressourcenpool aus, in dem die virtuelle Appliance ausgeführt werden soll, und klicken Sie auf **Weiter**.

6 Wählen Sie den Speicherort des Datenspeichers aus, in dem Sie die Dateien der virtuellen Appliance speichern möchten.

7 Wählen Sie das Format für die Festplatten der virtuellen Appliance aus. Dieses muss mit dem Format der Quelle identisch sein. Klicken Sie auf **Weiter**.

8 Wählen Sie als Option für das Gastbetriebssystem **Keine Anpassung** aus.

9 Überprüfen Sie die ausgewählten Optionen. Wenn die Informationen richtig sind, klicken Sie auf **Fertig stellen**.

Die geklonte virtuelle Appliance wird bereitgestellt. Sie können die virtuelle Appliance erst verwenden oder bearbeiten, nachdem das Klonen abgeschlossen ist.

Weiter

Weisen Sie der geklonten workspace-va eine IP-Adresse zu und schalten Sie erst dann die Maschine ein und fügen Sie die neue virtuelle Appliance dem Lastausgleichsdienst hinzu.

Hinzufügen einer IP-Adresse zu den Eigenschaften der geklonten virtuellen Appliance

Bevor Sie eine geklonte virtuelle Appliance einschalten, müssen Sie eine neue IP-Adresse zuweisen. Die IP-Adresse muss im DNS aufgelöst werden können. Wenn die Adresse nicht im Reverse-DNS vorhanden ist, müssen Sie außerdem den Hostnamen zuweisen.

Vorgehensweise

1 Wählen Sie im vSphere Client oder vSphere Web Client die virtuelle Appliance aus, die geklont wurde.

2 Wählen Sie **Übersicht > Befehle** aus und klicken Sie auf **Bearbeiten**.

3 Wählen Sie **Optionen** und in den **Optionseinstellungen** den Eintrag **Eigenschaften** aus.

4 Ändern Sie die IP-Adresse im Feld **IP-Adresse**.

5 Wenn die IP-Adresse nicht im Reverse-DNS vorhanden ist, fügen Sie im Textfeld **Hostname** den Hostnamen hinzu.

6 Klicken Sie auf **OK.**

7 Schalten Sie die geklonte Maschine ein.

Weiter

Aktivieren Sie die Authentifizierungsmethoden, die in den einzelnen geklonten virtuellen Appliances für Workspace konfiguriert sind.

Aktivieren der SecurID-Authentifizierung

In vielen Fällen haben Unternehmen für Endbenutzer, die aus externen Netzwerken zugreifen, die RSA SecurID-basierte Authentifizierung aktiviert. Nachdem Sie die virtuelle Appliance Workspace-VA geklont haben, müssen Sie bei Verwendung der RSA SecureID-Authentifizierung den Hostnamen und die IP-Adresse des geklonten Workspace zum RSA-Server hinzufügen und einen neuen Agent auf der geklonten virtuellen Appliance erstellen.

Voraussetzungen

Erstellen Sie einen neuen Agent für die RSA-Serverauthentifizierung mit dem Hostnamen und der IP-Adresse der geklonten Workspace-Appliance. Siehe „Vorbereiten des RSA SecurID-Servers für Connector Services-Administrator“, auf Seite 50.

Vorgehensweise

1 Melden Sie sich bei Connector Services-Administrator an.

2 Klicken Sie auf **Authentifizierungsadapter**.

3 Klicken Sie in der SecureID-Zeile auf **Bearbeiten**.

4 Konfigurieren Sie die SecureID-Authentifizierungsadapterseite neu, indem Sie die IP-Adresse des neuen Workspace hinzufügen. Siehe „Konfigurieren der RSA SecurID-Authentifizierung in Workspace“, auf Seite 50.

Aktivieren der Kerberos-Authentifizierung

Unternehmen können die Kerberos-Authentifizierung für ihre Endbenutzer aktivieren, die die Verbindung von internen Windows-Computern aus herstellen. Bei Verwendung der Kerberos-Authentifizierung können Endbenutzer sich ohne Eingabe des Benutzernamens und des Kennworts bei Workspace anmelden. Wenn Sie die Workspace-VA geklont haben und die Kerberos-Authentifizierung verwenden, müssen Sie der Domäne erneut beitreten und die Kerberos-Authentifizierung für die geklonte virtuelle Maschine aktivieren.

Vorgehensweise

◆ Melden Sie sich bei Connector Services-Administrator an.

   a Wählen Sie die Seite **Domäne beitreten** aus.

   b Geben Sie im Textfeld „AD-Kennwort“ das Kennwort des Benutzers in Active Directory ein, der über die Berechtigung zum Beitritt zur Domäne verfügt.

   c Klicken Sie auf **Domäne beitreten**.

   d Klicken Sie auf **Authentifizierungsadapter**.

   e Wählen Sie „KerberosldAdapter“ und auf der dann geöffneten Seite **Windows-Authentifizierung aktivieren**.

   f Klicken Sie auf **Speichern**.

Wenn View in eine Workspace-Bereitstellung mit mehreren Connectors integriert ist, stellen Sie sicher, dass auf jedem Connector, der View-Desktops unterstützt, View-Pools aktiviert und konfiguriert sind. Sie können von einem Connector ohne aktivierte View-Pools keine Verbindung zu Ihrem Desktop herstellen. Wenn Sie eine **View-Pool-Synchronisierung** von einem der Connectors aus planen, synchronisiert dieser Vorgang die Connectors mit der View-Konfiguration.

Einrichten der Benutzerauthentifizierung

8

Workspace unterstützt die folgenden Authentifizierungsmethoden: Active Directory-Kennwort, Kerberos und RSA SecureID.

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.

Weitere Informationen zum Konfigurieren der Benutzerauthentifizierung für Workspace finden Sie hier: *Workspace Administratorhandbuch*.

Dieses Kapitel behandelt die folgenden Themen:

Konfigurieren von SecurID für Workspace

Wenn Sie den RSA SecurID-Server konfigurieren, müssen Sie die Informationen zur Workspace-Appliance als Authentifizierungs-Agent auf dem RSA SecurID-Server hinzufügen und die RSA SecureID-Serverinformationen in Workspace konfigurieren.

Nach der Bereitstellung von Workspace können Sie SecurID für zusätzliche Sicherheit konfigurieren. Sie müssen sicherstellen, dass Ihr Netzwerk für die Workspace Bereitstellung korrekt konfiguriert ist. Insbesondere müssen Sie für SecurID sicherstellen, dass der richtige Port geöffnet ist, damit Benutzer außerhalb des Unternehmensnetzwerks über SecurID authentifiziert werden können.

Nach dem Ausführen des Workspace Setup-Assistenten stehen Ihnen die zum Vorbereiten des RSA SecurID-Servers erforderlichen Informationen zur Verfügung. Nachdem Sie den RSA SecurID-Server für die Workspace-Appliance vorbereitet haben, wechseln Sie zur Workspace Connector Services-Administrator-Seite „Authentifizierungsadapter“, um SecurID zu aktivieren.

- Vorbereiten des RSA SecurID-Servers für Connector Services-Administrator auf Seite 50

  Der RSA SecurID-Server muss mit Informationen über die Workspace-Appliance als Authentifizierungs-Agent konfiguriert werden. Die erforderlichen Informationen sind der Hostname und die IP-Adressen für Netzwerkschnittstellen.

- Konfigurieren der RSA SecurID-Authentifizierung in Workspace auf Seite 50

  Nachdem die Workspace-Appliance als Authentifizierungs-Agent auf dem RSA SecurID-Server konfiguriert wurde, müssen Sie Workspace RSA SecureID-Konfigurationsinformationen hinzufügen.

Vorbereiten des RSA SecurID-Servers für Connector Services-Administrator

Der RSA SecurID-Server muss mit Informationen über die Workspace-Appliance als Authentifizierungs-Agent konfiguriert werden. Die erforderlichen Informationen sind der Hostname und die IP-Adressen für Netzwerkschnittstellen.

Voraussetzungen

Workspace

- Stellen Sie sicher, dass eine der folgenden Versionen von RSA Authentication Manager im Unternehmensnetzwerk installiert und funktionsbereit ist, um die Kommunikation mit Connector Services-Administrator zu ermöglichen: RSA AM 6.1.2, 7.1 SP2 und höher oder 8.0 und höher. Workspace verwendet AuthSDK_Java_v8.1.1.312.06_03_11_03_16_51 (Agent API 8.1 SP1), das nur die vorhergehenden Versionen von RSA Authentication Manager (RSA SecurID-Server) unterstützt. Weitere Informationen zum Installieren und Konfigurieren von RSA Authentication Manager (RSA SecurID-Server) finden Sie in der RSA-Dokumentation.

Vorgehensweise

1 Fügen Sie die Workspace-Appliance auf einer unterstützten Version des RSA SecurID-Servers als Authentifizierungs-Agent hinzu. Geben Sie die folgenden Informationen ein.

Option	Beschreibung
Hostname	Der Hostname der Workspace-Appliance.
IP-Adresse	Die IP-Adresse der Workspace-Appliance.
Alternative IP-Adresse	Wenn Datenverkehr von der Workspace-Appliance über ein NAT-Gerät (Network Address Translation, Netzwerkadressübersetzung) an den RSA SecurID-Server geleitet wird, geben Sie die private IP-Adresse der Workspace-Appliance ein.

2 Laden Sie die komprimierte Konfigurationsdatei herunter, und extrahieren Sie die Datei `sdconf.rec`.

  Diese Datei müssen Sie später beim Konfigurieren der RSA SecurID in Workspace hochladen.

Weiter

Öffnen Sie die Connector Services-Administrator-Registerkarte „Erweitert“ und konfigurieren Sie SecurID auf der Seite „Authentifizierungsadapter“.

Konfigurieren der RSA SecurID-Authentifizierung in Workspace

Nachdem die Workspace-Appliance als Authentifizierungs-Agent auf dem RSA SecurID-Server konfiguriert wurde, müssen Sie Workspace RSA SecureID-Konfigurationsinformationen hinzufügen.

Voraussetzungen

- Vergewissern Sie sich, dass der RSA Authentication Manager (der RSA SecurID-Server) installiert und richtig konfiguriert ist.

- Laden Sie die komprimierte Datei vom RSA SecurID-Server herunter, und extrahieren Sie die Serverkonfigurationsdatei.

Vorgehensweise

1 Rufen Sie die Connector Services-Administrator-Seite „Authentifizierungsadapter“ auf und klicken Sie in der Zeile „SecurIDldpAdapter“ auf **Bearbeiten**.

2 Klicken Sie auf das Kontrollkästchen **SecurID aktivieren**.

3 Konfigurieren Sie die SecurID-Seite „Authentifizierungsadapter“.

Beim Konfigurieren der Seite SecurID werden die auf dem RSA SecurID-Server verwendeten Informationen und generierten Dateien benötigt.

Option	Aktion
Name	Der Name ist erforderlich. Der Standardname lautet „SecurIDldpAdapter“. Sie können diesen jederzeit ändern.
SecurID aktivieren	Aktivieren Sie dieses Kontrollkästchen, um die SecurID-Authentifizierung zu aktivieren.
Anzahl der zulässigen Authentifizierungsversuche	Die maximal zulässige Anzahl fehlgeschlagener Anmeldungen mit dem RSA SecurID-Token. Die Standardeinstellung lautet fünf Versuche.
Connector-Adresse	Geben Sie den Namen oder die IP-Adresse des lokalen Workspace-Hosts ein. Der eingegebene Wert muss mit dem Wert übereinstimmen, den Sie beim Hinzufügen der Workspace-Appliance als Authentifizierungs-Agent zum RSA SecurID-Server verwendet haben. Wenn auf Ihrem RSA SecurID-Server unter der Eingabe „Alternative IP-Adresse“ ein Wert zugewiesen wurde, geben Sie diesen Wert als Workspace-IP-Adresse ein. Wenn keine alternative IP-Adresse zugewiesen wurde, geben Sie den Wert ein, der der Eingabe „IP-Adresse“ zugewiesen wurde.
IP-Adresse des Agent	Geben Sie den für **IP-Adresse** auf dem RSA SecurID-Server festgelegten Wert ein.
Serverkonfiguration	Laden Sie die RSA SecureID-Serverkonfigurationsdatei hoch. Zuerst müssen Sie die komprimierte Datei vom RSA SecurID-Server herunterladen und die Serverkonfigurationsdatei (standardmäßig `sdconf.rec` benannt) extrahieren.
Knoten-Secret	Wenn Sie das Feld für das Knoten-Secret leer lassen, kann dieses automatisch generiert werden. Es empfiehlt sich, die Knoten-Secret-Datei auf dem RSA SecurID-Server zu löschen und bewusst nicht hochzuladen. Stellen Sie sicher, dass die Knoten-Secret-Datei auf dem RSA SecurID-Server immer mit der Knoten-Secret-Datei in der Workspace-Appliance übereinstimmt. Wenn Sie das Knoten-Secret an einem Speicherort ändern, nehmen Sie die entsprechende Änderung auch an dem anderen Speicherort vor. Wenn Sie das Knoten-Secret z. B. auf dem RSA SecurID-Server löschen oder generieren, müssen Sie die Knoten-Secret-Datei auch in der Workspace-Appliance löschen bzw. in diese hochladen.

4 Speichern Sie Ihre SecurID-Einstellungen.

Konfigurieren von Kerberos für Workspace

Kerberos-Authentifizierung ermöglicht den Benutzern Zugriff per Single Sign-On auf Workspace. Sie aktivieren die Windows-Authentifizierung, um mit dem Kerberos-Protokoll gesicherte Interaktionen zwischen den Browsern der Benutzer und Workspace zuzulassen. Sie brauchen keine direkte Konfiguration von Active Directory vorzunehmen, um die Kerberos-Funktion in Ihrer Workspace-Bereitstellung nutzen zu können.

Die Kerberos-Authentifizierung aktivieren Sie auf den Connector Services-Administrator-Seiten. Sie müssen zunächst auf der Connector Services-Administrator-Seite „Domäne beitreten“ der Domäne beitreten und dann Kerberos auf der Seite „Authentifizierungsadapter“ aktivieren.

Unterstützte Betriebssysteme für die Kerberos-Authentifizierung

Aktuell können Interaktionen zwischen dem Browser eines Benutzers und Workspace nur in Windows-Betriebssystemen von Kerberos authentifiziert werden. Für den Zugriff auf Workspace von anderen Betriebssystemen aus bietet die Kerberos-Authentifizierung keine Vorteile.

Konfigurieren Ihres Browsers

Folgende Webbrowser können zum Senden der Kerberos-Anmeldedaten an Workspace auf Computern unter Windows konfiguriert werden: Firefox, Internet Explorer und Chrome. Für alle Browser ist eine zusätzliche Konfiguration erforderlich.

Wenn Kerberos aktiviert ist, müssen Sie die Webbrowser so konfigurieren, dass beim Anmelden von Benutzern die Kerberos-Anmeldedaten an Workspace gesendet werden.

- Konfigurieren von Kerberos in Workspace auf Seite 52

  Um Workspace für die Bereitstellung von Kerberos-Authentifizierung zu konfigurieren, müssen Sie der Domäne beitreten und Kerberos-Authentifizierung in Workspace aktivieren..

- Konfigurieren von Internet Explorer für den Zugriff auf die Webschnittstelle auf Seite 53

  Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Internet Explorer gewähren möchten, müssen Sie den Internet Explorer-Browser konfigurieren.

- Konfigurieren von Firefox für den Zugriff auf die Webschnittstelle auf Seite 54

  Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist, und Sie Benutzern Zugriff auf die Webschnittstelle über Firefox gewähren möchten, müssen Sie den Firefox-Browser konfigurieren.

- Konfigurieren von Chrome für den Zugriff auf die Webschnittstelle auf Seite 55

  Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Chrome gewähren möchten, müssen Sie den Chrome-Browser konfigurieren.

Konfigurieren von Kerberos in Workspace

Um Workspace für die Bereitstellung von Kerberos-Authentifizierung zu konfigurieren, müssen Sie der Domäne beitreten und Kerberos-Authentifizierung in Workspace aktivieren..

Vorgehensweise

1 Rufen Sie Connector Services-Administrator auf und wählen Sie **Domäne beitreten** aus.

2 Geben Sie auf der Seite „Domäne beitreten“ die Informationen für die Active Directory-Domäne ein.

   a Geben Sie im Textfeld **AD-Domäne** den vollqualifizierten Namen der Active Directory-Domäne ein. Der eingegebene Domänenname muss der Windows-Domäne entsprechen, in der sich die Workspace-Appliance befindet.

   b Geben Sie im Textfeld **AD-Benutzername** den Benutzernamen eines Kontos in Active Directory ein, das über die erforderlichen Berechtigungen verfügt, um mit Systemen einer Active Directory-Domäne beizutreten.

   c Geben Sie im Textfeld **AD-Kennwort** das Kennwort für den AD-Benutzernamen ein. Dieses Kennwort wird von Workspace nicht gespeichert.

   d Klicken Sie auf **Domäne beitreten**.

   Die Seite „Domäne beitreten“ wird aktualisiert und es wird eine Meldung angezeigt, dass Sie der Domäne beigetreten sind.

3 Wählen Sie auf der Connector Services-Administrator-Seite **Authentifizierungsadapter** aus und klicken Sie in der Zeile „KerberosldpAdapter“ auf **Bearbeiten**.

   a Im Feld „Name“ wird „KerberosldpAdapter“ als Name angezeigt. Sie können diese Angaben ändern.

   b Geben Sie im Textfeld **Verzeichnis-UID-Attribut** das Kontoattribut ein, das den Benutzernamen enthält.

   c Aktivieren Sie **Windows-Authentifizierung aktivieren**, um die Authentifizierungsinteraktionen zwischen den Browsern des Benutzers und Workspace zu erweitern.

   d Aktivieren Sie **NTLM aktivieren**, um die auf dem NTLM-Protokoll (NT LAN Manager) basierende Authentifizierung zu aktivieren.

   e Aktivieren Sie **Umleitung aktivieren**, wenn Kerberos für Round-Robin-DNS und Lastausgleichsdienste nicht unterstützt wird. Authentifizierungsanforderungen werden zu „Hostnamen umleiten“ umgeleitet. Wenn dieses Kontrollkästchen aktiviert ist, geben Sie den Namen des Umleitungshosts im Textfeld **Hostnamen umleiten** ein.

   f Klicken Sie auf **Speichern**.

Konfigurieren von Internet Explorer für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Internet Explorer gewähren möchten, müssen Sie den Internet Explorer-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Workspace auf Windows-Betriebssystemen.

HINWEIS Implementieren Sie diese auf Kerberos bezogenen Schritte nicht auf anderen Betriebssystemen.

Voraussetzungen

Konfigurieren Sie Internet Explorer für jeden Benutzer oder geben Sie den Benutzern die entsprechenden Anweisungen, nachdem Sie Kerberos konfiguriert haben.

Vorgehensweise

1 Stellen Sie sicher, dass Sie bei Windows als Domänenbenutzer angemeldet sind.

2 Aktivieren Sie in Internet Explorer die automatische Anmeldung.

   a Wählen Sie **Extras > Internetoptionen > Sicherheit** aus.

   b Klicken Sie auf **Stufe anpassen**.

   c Aktivieren Sie **Automatisches Anmelden nur in der Intranetzone**.

   d Klicken Sie auf **OK.**

3 Stellen Sie sicher, dass diese Instanz der Workspace-Appliance Teil der lokalen Intranetzone ist.

   a Verwenden Sie Internet Explorer, um auf die Workspace-Anmelde-URL unter *https://Workspace-Hostname.Domänenname/authenticate/* zuzugreifen.

   b Die Zone wird unten rechts in der Statusleiste des Browserfensters angezeigt.

   Wenn die Zone das lokale Intranet ist, ist die Internet Explorer-Konfiguration fertig gestellt.

4 Wenn die Zone nicht das lokale Intranet ist, fügen Sie Workspace zur Intranetzone hinzu.

   a Wählen Sie **Extras > Internetoptionen > Sicherheit > Lokales Intranet > Sites** aus.

   b Aktivieren Sie **Intranet automatisch ermitteln**.

      War diese Option nicht aktiviert, reicht diese Aktivierung möglicherweise aus, um Workspace zur Intranetzone hinzuzufügen.

   c (Optional) Wenn Sie **Intranet automatisch ermitteln** aktiviert haben, klicken Sie mehrmals auf **OK**, bis alle Dialogfelder geschlossen sind.

   d Klicken Sie im Dialogfeld Lokales Intranet auf **Erweitert**.

      Ein zweites Dialogfeld mit dem Namen Lokales Intranet wird angezeigt.

   e Geben Sie die Workspace-URL in das Textfeld **Diese Website zur Zone hinzufügen** ein.

      https://Workspace-Hostname.Domänenname/authenticate/

   f Klicken Sie auf **Hinzufügen > Schließen > OK**.

5 Vergewissern Sie sich, dass Internet Explorer berechtigt ist, die Windows-Authentifizierung an die vertrauenswürdige Site zu übergeben.

   a Klicken Sie im Dialogfeld Internetoptionen auf die Registerkarte **Erweitert**.

   b Aktivieren Sie **Integrierte Windows-Authentifizierung aktivieren**.

      Diese Option wird erst nach dem Neustarten von Internet Explorer wirksam.

   c Klicken Sie auf **OK**.

6 Melden Sie sich bei der Workspace-Webschnittstelle unter *https://Workspace-Hostname.Domänenname/authenticate/* an, um den Zugriff zu überprüfen.

   Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle

Das Kerberos-Protokoll sichert alle Interaktionen zwischen dieser Internet Explorer-Browserinstanz und Workspace ab. Jetzt können Benutzer mit Single Sign-On auf Workspace zugreifen.

Konfigurieren von Firefox für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist, und Sie Benutzern Zugriff auf die Webschnittstelle über Firefox gewähren möchten, müssen Sie den Firefox-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Workspace auf Windows-Betriebssystemen.

HINWEIS Implementieren Sie diese auf Kerberos bezogenen Schritte nicht auf anderen Betriebssystemen.

Voraussetzungen

Konfigurieren Sie Firefox für jeden Benutzer, oder geben Sie den Benutzern die entsprechenden Anweisungen, nachdem Sie Kerberos konfiguriert haben.

Vorgehensweise

1 Geben Sie in das Textfeld URL von Firefox `about:config` ein, um auf die erweiterten Einstellungen zuzugreifen.

2 Klicken Sie **Ich werde vorsichtig sein, versprochen!**.

3 Doppelklicken Sie in der Spalte Einstellungsname auf **network.negotiate-auth.trusted-uris**.

4 Geben Sie die URL von Workspace in das Textfeld ein.

https://Workspace-Hostname

5 Klicken Sie auf **OK.**

6 Doppelklicken Sie in der Spalte Einstellungsname auf **network.negotiate-auth.delegation-uris**.

7 Geben Sie die URL von Workspace in das Textfeld ein.

https://Workspace-Hostname

8 Klicken Sie auf **OK.**

9 Testen Sie die Kerberos-Funktionalität, indem Sie sich über Firefox bei Workspace unter *https://Workspace-Hostname* anmelden.

Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle.

Das Kerberos-Protokoll sichert alle Interaktionen zwischen dieser Firefox-Browserinstanz und Workspace ab. Jetzt können Benutzer mit Single Sign-On auf Workspace zugreifen.

Konfigurieren von Chrome für den Zugriff auf die Webschnittstelle

Wenn Kerberos für Ihre Workspace-Bereitstellung konfiguriert ist und Sie Benutzern Zugriff auf die Webschnittstelle über Chrome gewähren möchten, müssen Sie den Chrome-Browser konfigurieren.

Die Kerberos-Authentifizierung funktioniert für Workspace auf Windows-Betriebssystemen.

HINWEIS Implementieren Sie diese auf Kerberos bezogenen Schritte nicht auf anderen Betriebssystemen.

Voraussetzungen

- Konfigurieren Sie Kerberos.
- Da Chrome die Internet Explorer-Konfiguration zur Aktivierung der Kerberos-Authentifizierung verwendet, müssen Sie die Internet Explorer-Konfiguration für Chrome freigeben. in der Google-Dokumentation finden Sie Informationen zum Konfigurieren von Chrome für Kerberos-Authentifizierung.

Vorgehensweise

1 Testen Sie die Kerberos-Funktionalität unter Verwendung von Chrome.

2 Melden Sie sich bei Workspace unter *https://Workspace FQDN* an.

Wenn die Kerberos-Authentifizierung erfolgreich ist, gelangen Sie über die Test-URL zur Webschnittstelle.

Wenn alle erforderlichen Kerberos-Konfigurationseinstellungen korrekt sind, sichert das entsprechende Protokoll (Kerberos) alle Interaktionen zwischen Chrome-Browserinstanzen und Workspace ab. Benutzer können mit Single Sign-On auf Workspace zugreifen.

Anpassen des Demo-Benutzerspeichers

9

Der eingebettete OpenLDAP-Dienst wird typischerweise für Demonstrations- oder Testkonfigurationen verwendet. Wenn Sie den eingebetteten OpenLDAP-Dienst verwenden, möchten Sie möglicherweise gängige LDAP-Vorgänge ausführen, wie z.˚B. Hinzufügen neuer Benutzer, Löschen vorhandener Benutzer und Ändern von Benutzerkennwörtern.

Diese Informationen sind für erfahrene Systemadministratoren bestimmt, die mit standardmäßigen LDAP-Vorgängen und -Befehlen vertraut sind.

Der eingebettete OpenLDAP-Server wird auf TCP-Port 389 ausgeführt. Auf den OpenLDAP-Server kann lokal nur über die Linux-Konsole in der workspace-va-VA zugegriffen werden. Mit den standardmäßigen LDAP-Befehlen können Sie Vorgänge auf dem eingebetteten OpenLDAP-Server ausführen. Die erforderlichen Binärdateien (`ldapadd`, `ldapsearch`, `ldapdelete` und `ldapmodify`) werden auf der virtuellen Appliance installiert.

Bei der Konfiguration von OpenLDAP auf den Appliance-Konfigurator- und Connector Services-Administrator-Seiten müssen Sie bestimmte Parameter verwenden.

Tabelle 9-1. Informationen zur OpenLDAP-Konfiguration

Attribut	Wert
Hostname	*Connector-FQDN* oder *localhost*
Suchattribut	`sAMAccountName`
Server-Port	389
Basis-DN	ou=users, dc=test, dc=example, dc=com
Bind-DN	cn=test user1, ou=users, dc=test, dc=example, dc=com
Bind-Kennwort	Kennwort

Der Demo-Benutzerspeicher enthält zu Demonstrationszwecken zehn Beispielbenutzer und eine Beispielgruppe.

Im Demo-Benutzerspeicher sind spezielle Beispieldaten enthalten. Während der Bereitstellung werden diese Daten in die Beispieldatenbank geladen.

Zum Hinzufügen von Benutzern oder Gruppen erstellen Sie neue Dateien und nennen Sie diese `ldapusers.ldif` und `ldapgroups.ldif`. Verwenden Sie die ursprünglichen Dateien `users.ldif` und `groups.ldif` als Vorlagen. Siehe „Hinzufügen eines Benutzers zum Demo-Benutzerspeicher“, auf Seite 58 und „Hinzufügen von Gruppen und Zuweisen von Benutzern zu Gruppen im Demo-Benutzerspeicher“, auf Seite 60.

Tabelle 9-2. Beispieldaten im Demo-Benutzerspeicher

Beispielname	Wert
Beispieldateien	`users.ldif` `groups.ldif`
Verzeichnispfad	`/etc/openldap`
Beispielbenutzernamen	testuser1 – testuser10
Kennwort für alle Benutzer	Kennwort
Beispielgruppe Die Beispielgruppe „testgroup1“ enthält zehn Beispielbenutzer.	testgroup1

- Hinzufügen eines Benutzers zum Demo-Benutzerspeicher auf Seite 58

  Bestimmen Sie beim Einrichten Ihres Demo-Benutzerspeichers die Anzahl der Benutzer, die Sie hinzufügen möchten, auf der Basis Ihrer Produktionsumgebung. Sie müssen genügend Benutzer hinzufügen, um mit den Tests Ergebnisse zu erzielen, die für Ihre Produktionsumgebung relevant sind.

- Hinzufügen von Gruppen und Zuweisen von Benutzern zu Gruppen im Demo-Benutzerspeicher auf Seite 60

  Bestimmen Sie beim Einrichten Ihres Demo-Benutzerspeichers die Anzahl der Gruppen und Benutzer, die Sie hinzufügen möchten, auf der Basis der Größe Ihrer Produktionsumgebung. Fügen Sie eine ausreichende Zahl von Gruppen und Benutzern hinzu, um eine Umgebung zu erstellen, die Ihrer Produktionsumgebung weitestgehend entspricht.

Hinzufügen eines Benutzers zum Demo-Benutzerspeicher

Bestimmen Sie beim Einrichten Ihres Demo-Benutzerspeichers die Anzahl der Benutzer, die Sie hinzufügen möchten, auf der Basis Ihrer Produktionsumgebung. Sie müssen genügend Benutzer hinzufügen, um mit den Tests Ergebnisse zu erzielen, die für Ihre Produktionsumgebung relevant sind.

Sie fügen einen Benutzer zum Demo-Benutzerspeicher hinzu, indem Sie die Datei `ldapusers.ldif` bearbeiten und den Befehl `ldapadd` auf der workspace-va-VM ausführen.

Voraussetzungen

Sie müssen `sAMAccountName` als Suchattribut im Demo-Benutzerspeicher verwenden. Workspace unterstützt `userPrincipalName` bei Verwendung eines Demo-Benutzerspeichers nicht.

Vorgehensweise

1 Ersetzen Sie das Tag *Wert* in der Datei `ldapusers.ldif` durch Ihre Informationen. Weitere Informationen hierzu finden Sie in der `ldapusers.ldif`-Beispieltabelle.

2 Kopieren Sie die Datei `ldif` auf die workspace-va-VM.

3 Führen Sie den Befehl `ldapadd` aus, um einen neuen Benutzer zum Demo-Benutzerspeicher hinzuzufügen.

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

  Durch Verwendung verschiedener Werte in einer einzigen `ldif`-Datei können Sie mehrere Benutzer hinzufügen.

4 Starten Sie den LDAP-Dienst neu.

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

Tabelle 9-3. `ldapusers.ldif` -Beispieldatei

`ldapusers.ldif` - Beispiel
Verwenden Sie für jeden Parameter einen eindeutigen *Wert*. dn: cn=*Wert*,ou=users,dc=test,dc=example,dc=com objectClass: Benutzer objectCategory: person cn: *Wert* sn: *Wert* sAMAccountName: *Wert* canonicalName: *Wert* mail: *Wert* givenName: *Wert* distinguishedName: cn=*Wert*,ou=users,dc=test,dc=example,dc=com objectGUID: *Wert* (z. B. cd0ff02b-f9d6-4fac-a5bc-6380d1867999.) userPassword: *Wert* (z. B. {SSHA}WbipwJh13Jdy2tItppdkFMzzNVSfkqsZ.)

Weiter

Generieren Sie ein verschlüsseltes Kennwort für die Benutzer des Demo-Benutzerspeichers. Siehe „Generieren eines SSHA-verschlüsselten Kennworts“, auf Seite 59.

Generieren eines SSHA-verschlüsselten Kennworts

Der SSHA-Algorithmus (Salted Secure Hash Algorithm) ist eine verbesserte Version des SHA-Algorithmus, bei dem der Hash zufällig festgelegt wird. Dadurch verringert sich die Wahrscheinlichkeit, dass der Hash entschlüsselt wird.

Sie müssen ein SSHA-verschlüsseltes Kennwort generieren. Sie können dasselbe Kennwort für alle Demo-Benutzerkonten verwenden. Wenn Sie für jeden Benutzer ein anderes Kennwort benötigen, verschlüsseln Sie jedes Kennwort einzeln.

Voraussetzungen

„Hinzufügen eines Benutzers zum Demo-Benutzerspeicher“, auf Seite 58.

Vorgehensweise

1 Öffnen Sie die workspace-va-VA.

2 Führen Sie den Befehl `slappasswd` aus.

3 Geben Sie ein neues Kennwort ein und bestätigen Sie es.

Der SSHA-verschlüsselte Wert wird angezeigt.

4 Fügen Sie diesen Wert zur `ldif`-Datei hinzu, um das Benutzerkennwort festzulegen.

Weiter

Fügen Sie Gruppen hinzu, und weisen Sie dem Demo-Benutzerspeicher Benutzer zu.

Hinzufügen von Gruppen und Zuweisen von Benutzern zu Gruppen im Demo-Benutzerspeicher

Bestimmen Sie beim Einrichten Ihres Demo-Benutzerspeichers die Anzahl der Gruppen und Benutzer, die Sie hinzufügen möchten, auf der Basis der Größe Ihrer Produktionsumgebung. Fügen Sie eine ausreichende Zahl von Gruppen und Benutzern hinzu, um eine Umgebung zu erstellen, die Ihrer Produktionsumgebung weitestgehend entspricht.

Sie fügen eine Gruppe zum Demo-Benutzerspeicher hinzu, indem Sie die Datei `ldapgroups.ldif` bearbeiten und den Befehl `ldapadd` auf der workspace-va-VM ausführen.

Vorgehensweise

1 Ersetzen Sie die Tags *Wert* und *Benutzer-DN* in der Datei `ldapgroups.ldif`.

Der Benutzer-DN muss der eindeutige Name (Distinguished Name, DN) eines vorhandenen Benutzers in LDAP sein. Indem Sie das Tag *Wert* ersetzen, erstellen Sie eine Gruppe, und indem Sie das Tag *Benutzer-DN* ersetzen, weisen Sie der neuen Gruppe, die Sie erstellen, einen Benutzer zu.

2 Kopieren Sie die Datei `ldif` auf die workspace-va-VM.

3 Führen Sie den Befehl `ldapadd` aus, um dem Demo-Benutzerspeicher eine Gruppe hinzuzufügen.

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

Durch Verwendung verschiedener Werte in einer einzigen `ldif`-Datei können Sie mehrere Gruppen hinzufügen.

4 Starten Sie den LDAP-Dienst neu.

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

Tabelle 9-4. `ldapgroups.ldif` -Beispieldatei

Beispielparameter
Verwenden Sie für jeden Parameter einen eindeutigen *Wert*.
dn: cn=*Wert*,ou=users,dc=test,dc=example,dc=com
objectClass: Gruppe
objectCategory: Gruppe
sAMAccountName: *Wert*
canonicalName: *Wert*
mail: *Wert*
distinguishedName: cn=*Wert*,ou=users,dc=test,dc=example,dc=com
objectGUID: *Wert* (z. B. cd0ff02b-f9d6-4fac-a5bc-6380d1867899)
member: *Benutzer-DN1* (z. B. cn=user1,ou=users,dc=test,dc=example,dc=com)
member: *Benutzer-DN2*
member: *Benutzer-DN3*
member: *Benutzer-DN4*

Weiter

Verwenden Sie den Demo-Benutzerspeicher zum Testen, bis Sie bereit sind, Workspace in die Produktionsumgebung zu überführen.

Index