Guía de instalación y configuración de VMware Horizon Mobile Manager

Horizon Mobile Manager 1.3

Este documento admite la versión de todos los productos enumerados y admite todas las versiones posteriores hasta que el documento se reemplace por una edición nueva. Para buscar ediciones más recientes de este documento, consulte http://www.vmware.com/support/pubs.

ES-001072-00

vmware®

Puede encontrar la documentación técnica más actualizada en el sitio web de WMware en:

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

En el sitio web de VMware también están disponibles las últimas actualizaciones del producto.

Si tiene algún comentario sobre esta documentación, envíelo a la siguiente dirección de correo electrónico:

docfeedback@vmware.com

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

VMware, Inc.
Paseo de la Castellana 141. Planta 8.
28046 Madrid.
Tel.:+ 34 91 418 58 01
Fax: + 34 91 418 50 55
www.vmware.com/es

Contenido

Guía de instalación y configuración de VMware Horizon Mobile Manager

Guía de instalación y configuración de VMware Horizon Mobile Manager proporciona información acerca de cómo instalar y configurar la aplicación virtual VMware® Horizon Mobile Manager™ y cómo verificar operaciones de su instalación.

La aplicación virtual Horizon Mobile Manager proporciona los componentes del lado del servidor que se utilizan en la solución Horizon Mobile. El proceso de instalación y configuración general de los componentes del lado del servidor implica:

1 Determinar qué configuración de implementación se va a utilizar

2 Implementar la aplicación virtual

3 Poner en marcha la aplicación virtual

4 Configurar ajustes para la propia aplicación

5 Instalar y configurar los elementos necesarios para la configuración de implementación elegida

6 Configurar los ajustes de Horizon Mobile Manager, según la configuración de implementación elegida

7 Reiniciar para aplicar los ajustes seleccionados

8 Determinar el método de certificación de identidad digital adecuado y, opcionalmente, sustituir los certificados predeterminados

Destinatarios

Esta información está destinada a los administradores de sistemas con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Configuraciones de implementación 1

La aplicación virtual Horizon Mobile Manager está diseñada para controlar, personalizar y gestionar áreas de trabajo corporativas en los dispositivos móviles de sus usuarios. La aplicación utiliza un servidor Apache 2.2 incrustado para proporcionar las capacidades de gestión del lado del servidor, y envía comunicaciones mediante conexiones con protocolo Secure Sockets Layer (SSL). Debe implementar la aplicación virtual para que pueda gestionar áreas de trabajo en los dispositivos cuando estos se comuniquen a través de la red corporativa o por Internet.

En la tabla siguiente se describen las configuraciones de implementación típicas de Horizon Mobile Manager.

Tabla 1-1. Configuraciones de implementación de Horizon Mobile Manager

Configuración	Descripción	Ventajas	Desventajas
Horizon Mobile Manager en zonas desmilitarizadas de Internet (DMZ).	En entornos de redes, una DMZ de Internet es una zona de confianza combinada entre los servicios de red internos e Internet. En esta configuración, la dirección IP de Horizon Mobile Manager es una dirección IP pública externa y se puede acceder a ella directamente por Internet. Los dispositivos se comunican con solicitudes SSL a la dirección IP pública de Horizon Mobile Manager.	■ La forma más sencilla de poner en marcha Horizon Mobile Manager. ■ No se necesita ninguna configuración de red especial, aparte de una dirección IP externa.	■ No es apropiada para entornos de producción, porque todos los servicios de Horizon Mobile Manager se exponen públicamente en Internet. ■ Evita las conexiones entre Horizon Mobile Manager y los servicios internos de empresa como Active Directory, LDAP o servicios de bases de datos corporativas, a no ser que los puertos de estos servicios sean accesibles a través del firewall de la empresa.
Horizon Mobile Manager en la red interna de la empresa, utilizando la traducción de direcciones de red (NAT) para traducir sus direcciones IP internas a direcciones IP disponibles externamente.	En esta configuración, Horizon Mobile Manager tiene una dirección IP privada. Los dispositivos se comunican con solicitudes SSL a una dirección IP disponible externamente, y dichas solicitudes SSL se traducen a la dirección IP privada de Horizon Mobile Manager utilizando NAT.	■ Los servicios de Horizon Mobile Manager están protegidos por el firewall de la empresa. ■ Horizon Mobile Manager puede conectarse a servicios internos como Active Directory, LDAP o servicios de bases de datos corporativas sin abrir puertos a través del firewall. ■ NAT es una configuración de red conocida y habitual en las empresas.	■ Requiere la definición de reglas de NAT que traduzcan las solicitudes IP al puerto TCP/IP 443 en la dirección IP privada de Horizon Mobile Manager. ■ El puerto 433 de Horizon Mobile Manager debe estar disponible públicamente para recibir las solicitudes procedentes de NAT. ■ Una arquitectura no del todo satisfactoria para entornos con clústeres de servidores de Horizon Mobile Manager que tengan uno o más servidores Apache de proxy inverso externos.
Horizon Mobile Manager en la red interna de la empresa, utilizando un servidor de proxy inverso en la DMZ para gestionar las solicitudes SSL de los dispositivos en Internet.	En esta configuración, el servidor de proxy gestiona las comunicaciones SSL con los dispositivos y, a continuación, inicia nuevas solicitudes para Horizon Mobile Manager en el lado accesible internamente de la red principal. El servidor de proxy inverso convierte las solicitudes de servicios de concesión, descarga e inicio de sesión de Horizon Mobile Manager en las direcciones URL específicas utilizadas por Horizon Mobile Manager.	■ Los servicios de Horizon Mobile Manager están protegidos por el firewall de la empresa. ■ Horizon Mobile Manager puede conectarse a servicios internos como Active Directory, LDAP o servicios de bases de datos corporativas sin abrir puertos a través del firewall. ■ Aprovecha con mayor facilidad la infraestructura corporativa existente. Hay muchas empresas que utilizan de forma	■ Requiere una planificación cuidadosa para configurar el servidor de proxy inverso y las reglas para comunicarse con Horizon Mobile Manager. ■ Requiere la configuración del servidor proxy inverso para las comunicaciones SSL que utilizan su propio certificado SSL. ■ Requiere la participación de equipos de redes para asegurarse de que el servidor de proxy

Tabla 1-1. Configuraciones de implementación de Horizon Mobile Manager (Continua)

Configuración	Descripción	Ventajas	Desventajas
		asidua servidores de proxy inverso para aislar los servidores de aplicaciones internos de Internet, y estos servidores de proxy pueden ampliarse para que funcionen con Horizon Mobile Manager.	inverso dispone de una ruta a Horizon Mobile Manager en una interfaz secundaria.

De las tres configuraciones, la instalación de Horizon Mobile Manager en la DMZ es la forma más rápida de empezar a ver cómo funciona la solución VMware® Horizon Mobile™. Sin embargo, como esa configuración expone públicamente a Internet los servicios de Horizon Mobile Manager, es la menos segura. El uso de la configuración de DMZ solo debe utilizarse para demostraciones de prueba de concepto y procesos de prueba. En la configuración de DMZ tenga en cuenta la visibilidad de Horizon Mobile Manager y no lo conecte a ningún Active Directory o servidor de base de datos que se esté ejecutando en la red interna. Para las demostraciones de prueba de concepto, utilice los servidores de bases de datos y LDAP integrados instalados con la aplicación virtual Horizon Mobile Manager y asigne usuarios de prueba de ese LDAP integrado a dispositivos móviles concretos para demostrar las capacidades de administración de Horizon Mobile Manager.

Aunque el uso de un servidor proxy inverso implica la configuración más compleja, también es la más segura, y una de las mejores para la implementación de producción.

Instalación de la Aplicación virtual Horizon Mobile Manager 2

Horizon Mobile Manager se distribuye como una aplicación virtual. El primer paso en el proceso de instalación es implementar la aplicación virtual Horizon Mobile Manager.

Es posible instalar la aplicación virtual Horizon Mobile Manager en cualquier plataforma de virtualización compatible con OVF 1.0. Los pasos del proceso describen la implementación en VMware vSphere®.

Para implementar la aplicación virtual en vSphere, necesitará un ordenador con Microsoft Windows con VMware vSphere® Client™ instalado.

Prerequisitos

Descargue el archivo OVA de Horizon Mobile Manager de la página de descargas de productos.

Procedimiento

1 Inicie sesión en vSphere Client.

2 Seleccione **Archivo > Implementar plantilla OVF**.

3 Haga clic en **Examinar** y a continuación busque y seleccione la ubicación del archivo OVA de Horizon Mobile Manager.

4 Haga clic en **Siguiente**.

5 Revise los detalles de la plantilla de Horizon Mobile Manager y haga clic en **Siguiente**.

6 Lea y acepte el Contrato de licencia para el usuario final y haga clic en **Siguiente**.

7 Escriba un nombre representativo para la aplicación virtual Horizon Mobile Manager y haga clic en **Siguiente**.

8 Seleccione **Formato de aprovisionamiento fino** y haga clic en **Siguiente**.

9 Revise las opciones que ha elegido y haga clic en **Finalizar**.

   Un mensaje de progreso indica que la aplicación virtual Horizon Mobile Manager se está implementando y un mensaje de éxito indica cuándo ha finalizado la implementación.

Qué hacer a continuación

Active y configure la aplicación virtual Horizon Mobile Manager. Consulte Capítulo 3, “Configuración de la Aplicación virtual Horizon Mobile Manager,” página 13.

Configuración de la Aplicación virtual Horizon Mobile Manager 3

Configure el adaptador de red para la aplicación virtual y enciéndala. Tras encender la aplicación virtual, configure la propia aplicación cambiando la contraseña predeterminada, configurando una dirección IP estática y configurando los ajustes de red de la aplicación.

Prerequisitos

Instale la aplicación virtual Horizon Mobile Manager. Consulte Capítulo 2, "Instalación de la Aplicación virtual Horizon Mobile Manager," página 11.

Determine qué configuración de implementación se va a utilizar. Consulte Capítulo 1, "Configuraciones de implementación," página 7.

Procedimiento

1 En vSphere Client, en la pestaña **Introducción** de la aplicación virtual, haga clic en **Editar configuración de máquina virtual**.

2 En la pestaña **Hardware**, configure el adaptador de red para la aplicación virtual, según las opciones apropiadas para la implementación elegida.

Configuración de implementación	Descripción
Horizon Mobile Manager en su DMZ	Conéctese a una interfaz de red en su DMZ.
Horizon Mobile Manager en su red interna, utilizando NAT para traducir una IP pública a la IP interna	Conéctese a una interfaz de red en su red interna.
Horizon Mobile Manager en su red interna, utilizando un servidor proxy inverso para delegar solicitudes externas a la IP interna	Conéctese a una interfaz de red en su red interna.

3 Active la aplicación virtual Horizon Mobile Manager en vSphere Client y haga clic en la pestaña **Consola**.

La aplicación virtual muestra mensajes mientras se está encendiendo. Lea y acepte el Contrato de licencia para el usuario final.

4 Cuando se active la aplicación virtual y aparezca el menú principal, seleccione **Iniciar sesión**.

5 Inicie sesión en el sistema operativo Linux de la aplicación virtual utilizando los valores predeterminados de la aplicación: nombre de usuario **`root`** y contraseña **`vmware`**.

6 Por motivos de seguridad, cambie la contraseña predeterminada "root".

7 Escriba **`exit`** para volver al menú principal.

8 Seleccione **Configurar red**.

9 Configure los ajustes de red para adecuarlos a la configuración de implementación que haya elegido.

Configuración de implementación	Descripción
Horizon Mobile Manager en su DMZ	Configure los ajustes de red de la aplicación para utilizar una dirección IP estática. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host.
Horizon Mobile Manager en su red interna, utilizando NAT para traducir una IP pública a la IP interna	a Configure los ajustes de red de la aplicación para utilizar una dirección IP estática interna. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host. Si la red interna requiere el uso de un servidor proxy de reenvío, configure el servidor proxy. b Cree reglas de NAT en su firewall para asignar el puerto TCP/IP 443 a la dirección IP interna de la aplicación.
Horizon Mobile Manager en su red interna, utilizando un servidor proxy inverso para delegar solicitudes externas a la IP interna	a Configure los ajustes de red de la aplicación para utilizar una dirección IP estática. Siga las indicaciones para configurar la dirección IP, la máscara de red, la puerta de enlace, los servidores DNS y el nombre de host. Si la red interna requiere el uso de un servidor proxy de reenvío, configure el servidor proxy. b Configure el servidor proxy inverso con dos interfaces de red: ■ Una interfaz en su DMZ ■ Una interfaz en su red interna c Configure el servidor proxy inverso para habilitar las conexiones HTTPS y cifre el tráfico entre Internet y el servidor proxy mediante conexiones con protocolo SSL. d Configure las reglas de proxy para que se soliciten conexiones SSL y para que se deleguen las URL a Horizon Mobile Manager en la red interna: ■ `https://<su_nombre_de_dominio>/provision` ■ `https://<su_nombre_de_dominio>/leasing` ■ `https://<su_nombre_de_dominio>/download` El servidor Apache integrado de Horizon Mobile Manager está configurado para escuchar puertos TCP/IP específicos para determinados tipos de solicitudes. Por lo tanto, si el servidor proxy inverso utiliza los módulos `mod_jk` o `mod_proxy_ajp`, utilice el puerto TCP/IP 8009 para ponerse en contacto con Horizon Mobile Manager. Si el servidor proxy inverso utiliza el módulo `mod_proxy_http`, utilice el puerto TCP/IP 8080 para ponerse en contacto con Horizon Mobile Manager.

Cuando termine de configurar los ajustes de red de la aplicación virtual en la pestaña **Consola**, volverá al menú principal.

La configuración de la aplicación virtual Horizon Mobile Manager habrá finalizado.

Qué hacer a continuación

Conéctese a la interfaz de configuración de Horizon Mobile Manager para añadir claves de licencia y configurar ajustes. Consulte Capítulo 4, “Adición de claves de licencia,” página 15 y Capítulo 5, “Configuración de los ajustes de Horizon Mobile Manager,” página 17.

Adición de claves de licencia 4

Utilice la interfaz de configuración para añadir claves de licencia que habiliten la funcionalidad de gestionar teléfonos profesionales mediante Horizon Mobile Manager. Cada clave de licencia permite que una licencia gestione un número específico de teléfonos profesionales con Horizon Mobile Manager.

Prerequisitos

- Obtenga una o más claves de licencia válidas. También se hace referencia a una clave de licencia como un número de serie en la interfaz de configuración.
- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.

Procedimiento

1 En el navegador, introduzca la URL de la interfaz de configuración de Horizon Mobile Manager, con el formato **`https://`*`dirección_ip`*`:5480`**, donde *dirección_ip* es la que se ha establecido al configurar la propia aplicación virtual.

   La interfaz web utiliza un certificado autofirmado.

2 Inicie sesión como usuario **`root`**.

   Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **Licencias**.

4 Haga clic en **Agregar licencia de teléfono profesional**.

5 Introduzca la clave de licencia (número de serie) y haga clic en **Agregar**.

Tras introducir una clave de licencia válida, el sistema muestra la información relacionada con la licencia, como la fecha de caducidad de la licencia y el número de teléfonos profesionales que puede gestionar.

Qué hacer a continuación

Si aún no lo ha hecho, configure los ajustes de Horizon Mobile Manager. Debe hacer clic en **Guardar y reiniciar** en la pestaña **Configuración** al menos una vez para finalizar el proceso de instalación de Horizon Mobile Manager. Consulte Capítulo 5, “Configuración de los ajustes de Horizon Mobile Manager,” página 17.

Configuración de los ajustes de Horizon Mobile Manager 5

Debe personalizar determinados ajustes, o aceptar los valores predeterminados, antes de que Horizon Mobile Manager esté listo para utilizarse por primera vez. Debe hace clic en **Guardar y reiniciar** en la pestaña **Configuración** para inicializar los elementos necesarios para configurar las áreas de trabajo del usuario en Horizon Mobile Manager, como la imagen base del área de trabajo.

Prerequisitos

- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.
- Añada claves de licencia. Consulte Capítulo 4, "Adición de claves de licencia," página 15.
- Si está utilizando la configuración de NAT o de servidor proxy inverso, obtenga la dirección IP o URL accesible externamente que se utiliza en su configuración de implementación. Consulte Capítulo 3, "Configuración de la Aplicación virtual Horizon Mobile Manager," página 13.
- Obtenga la información relacionada con el correo electrónico de su organización para enviar correos electrónicos mediante el servidor de correo SMTP y una dirección electrónica que pueda recibir un correo de configuración de prueba.
- Determine si desea utilizar los valores predeterminados o especifique valores personalizados para los siguientes elementos:

Base de datos

Puede utilizar la base de datos de VMware® vFabric™ Postgres incrustada (la predeterminada) o su propia base de datos externa. Las siguientes bases de datos externas son compatibles:

- Microsoft SQL Server 2008
- Oracle 11g R2

Por ejemplo, puede que quiera utilizar una base de datos externa en las siguientes situaciones:

- Para cumplir con las normativas sobre bases de datos de la compañía.
- Para proporcionar gestión y apoyo mediante las prácticas de gestión de bases de datos estándares de la compañía.
- Para mejorar el rendimiento o el equilibrador de carga a la hora de gestionar un gran número de usuarios.

	La instalación de Horizon Mobile Manager en una configuración en clúster requiere el uso de una base de datos externa.
Servicio de nombres	Determine qué servicio de directorios utilizará para ofrecer la información de las cuentas de usuario a Horizon Mobile Manager. De modo predeterminado, la aplicación virtual incluye un servicio OpenLDAP incrustado preconfigurado. Este servicio OpenLDAP incrustado es apto para el uso experimental en demostraciones de concepto o entornos de prueba. En los entornos de producción, debe utilizar el servicio de nombres LDAP o Active Directory de un solo dominio de su organización. No se admite el uso de varios dominios de Active Directory.
Administrador del sistema predeterminado	Determine qué cuenta de usuario del servicio de nombres seleccionado es la cuenta que desea utilizar como administrador del sistema predeterminado para Horizon Mobile Manager. El administrador del sistema predeterminado puede acceder a la interfaz administrativa de Horizon Mobile Manager y llevar a cabo todas las operaciones. Es una buena práctica limitar el uso de esta cuenta para la configuración inicial de Horizon Mobile Manager, que incluye la asignación de funciones de las operaciones en curso a los usuarios adecuados. Para mantener un seguimiento de auditoría coherente, las operaciones de Horizon Mobile Manager en curso las deben llevar a cabo los usuarios de Horizon Mobile Manager que tienen una función de administrador o administrador del parque asignada. Tras finalizar el procedimiento de configuración e inicialización de los elementos básicos, haga que el administrador del sistema predeterminado inicie sesión en la interfaz administrativa de Horizon Mobile Manager para asignar las funciones adecuadas de Horizon Mobile Manager a los usuarios mediante la página Funciones y trabajos.
Repositorio	Puede utilizar la ubicación predeterminada para el repositorio de Horizon Mobile Manager o especificar otra ubicación. El repositorio almacena objetos de Horizon Mobile Manager como, por ejemplo, imágenes de áreas de trabajo, aplicaciones y archivos de sistema. De forma predeterminada, la ruta del repositorio es `/opt/vmware-mmp/repo` en el sistema de archivos de la aplicación virtual Horizon Mobile Manager. Puede que quiera utilizar un repositorio externo a la aplicación virtual si está utilizando Horizon Mobile Manager en una configuración en clúster o si planea implementar muchas aplicaciones de gran tamaño en áreas de trabajo de los usuarios. Ya que las aplicaciones virtuales tienen un tamaño de disco máximo de 40 GB, si planea implementar muchas aplicaciones de gran tamaño que excedan esa capacidad, seleccione una ubicación de repositorio que tenga una capacidad de almacenamiento adecuada.

NOTA: Puede actualizar los ajustes en la pestaña **Configuración** para una instalación existente de Horizon Mobile Manager en cualquier momento. Sin embargo, la actualización de estos ajustes tras el primer uso de Horizon Mobile Manager puede hacer que sea necesario realizar esfuerzos adicionales para aplicar de forma manual los cambios realizados en el sistema tras el uso inicial. Por ejemplo, si en un principio ha elegido utilizar el servicio de nombres OpenLDAP incrustado y aprovisionar los dispositivos de los usuarios y, a continuación, actualizar la configuración para utilizar un servicio de nombres diferente, los usuarios existentes no funcionarán a menos que se añadan los mismos ID de usuarios al nuevo servicio de nombres.

Procedimiento

1 En su navegador, introduzca la dirección URL de la interfaz de configuración de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`*`:5480`**

2 Inicie sesión como usuario **root**.

Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **vmware** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **Configuración**.

4 En el campo **Nombre del administrador predeterminado**, especifique el nombre de un usuario para que sea el administrador de sistema de Horizon Mobile Manager.

El nombre especificado debe existir en el servicio de nombres que haya seleccionado para Horizon Mobile Manager. El valor predeterminado mostrado (**admin**) es una cuenta de usuario en el servicio de nombres OpenLDAP incrustado. Esta cuenta **admin** predeterminada tiene la contraseña **vmware**.

Si escoge utilizar un servicio de nombres externo, debe actualizar el valor del campo **Nombre del administrador predeterminado** con un nombre que exista en el servicio de nombres.

5 Especifique la ubicación para el repositorio del sistema de archivos de Horizon Mobile Manager.

Es posible introducir una ruta de sistemas de archivos de red o local. De forma predeterminada, la ruta del repositorio es `/opt/vmware-mmp/repo` en el sistema de archivos de la aplicación virtual. Cuando haga clic en **Guardar y reiniciar**, los objetos predeterminados proporcionados por Horizon Mobile Manager (como la imagen base del área de trabajo) se escriben en la ubicación especificada.

6 Escriba una dirección URL raíz (nivel de entrada) accesible externamente para el servidor de inicio de sesión, el servidor de descarga y el servidor de concesiones.

NOTA: Debido a que las áreas de trabajo de los dispositivos móviles gestionados se comunican periódicamente con Horizon Mobile Manager, las URL de los servidores de inicio de sesión, concesiones y descargas deben ser accesibles desde los dispositivos en los que están instaladas o se van a instalar las áreas de trabajo. Si está utilizando la configuración de implementación de servidor proxy inverso o NAT, debe introducir la URL accesible externamente que se utiliza en esa configuración.

Incluya **https://** al inicio de las URL. Incluso si ha escrito **http://**, el área de trabajo de los dispositivos utiliza el puerto seguro **443** para la comunicación con los servidores.

Estas tres URL pueden ser las mismas. Por ejemplo, en una configuración simple de una aplicación virtual Horizon Mobile Manager implementada con una dirección IP pública, esa aplicación virtual puede proporcionar el servidor con fines de administración, inicio de sesión, descarga y concesión. En este escenario, la URL especificada para los servidores de inicio de sesión, descarga y concesión es **https://*dirección_ip***, donde la *dirección_ip* es la dirección IP pública.

Servidor	Uso
Servidor de inicio de sesión	Lo utiliza el usuario del área de trabajo en el dispositivo móvil para instalar y descargar su área de trabajo.
Servidor de descarga	Proporciona software a las áreas de trabajo.
Servidor de concesiones	Gestiona las concesiones de las áreas de trabajo.

7 (Opcional) Para utilizar su propia base de datos Oracle o SQL Server en vez de la base de datos incrustada, seleccione **Utilizar base de datos externa** y seleccione un tipo de base de datos del menú desplegable. A continuación, especifique la información que permita a Horizon Mobile Manager almacenar y acceder a los datos de la base de datos.

Dirección (URL)	La dirección de la base de datos.
Nombre de usuario	El usuario de la base de datos para la conexión de la base de datos.
Contraseña	La contraseña para la conexión de la base de datos.
Nombre de usuario DBA	Un usuario de la base de datos de nivel DBA con privilegios DDL para crear objetos de base de datos utilizados por Horizon Mobile Manager.

Contraseña DBA	La contraseña para el usuario DBA.
Petición de validación	Petición SQL que se utiliza para validar las conexiones con la base de datos.

Para la base de datos externa, puede especificar ajustes avanzados adicionales, como el tamaño inicial del grupo de conexión.

8 (Opcional) Para utilizar su propio servicio de nombres en vez del servicio OpenLDAP incrustado, seleccione **Utilizar servicio externo** y seleccione el tipo.

Si está utilizando su propio servicio de asignación de nombres de Active Directory, deberá introducir el dominio de Active Directory. No se admite el uso de varios dominios de Active Directory.

Si está utilizando su propio servicio de asignación de nombres LDAP, deberá introducir la dirección URL del servidor LDAP, el DN de raíz y la consulta de búsqueda de usuario. También es posible introducir el nombre de usuario y la contraseña del DN de gestor.

9 Configure los ajustes de correo electrónico de Horizon Mobile Manager para conectarse con el servidor de correo electrónico de su organización:

a Introduzca la dirección de host SMTP y la información del puerto del servidor de correo electrónico.

b (Opcional) Para utilizar el cifrado SSL, seleccione la casilla de verificación **Utilizar SSL**.

c (Opcional) Para utilizar la autenticación, seleccione la casilla de verificación **Utilizar autenticación** y especifique el nombre de usuario y la contraseña para realizar la autenticación SMTP.

d Pruebe la configuración especificando la dirección de correo electrónico del destinatario y haciendo clic en **Enviar correo electrónico** para enviar un correo electrónico de confirmación.

Si el sistema puede enviar correctamente un correo electrónico utilizando la información SMTP, el correo electrónico de confirmación tendrá un código de verificación.

e Obtenga el código del correo electrónico de confirmación e introduzca el código en el campo **Código del correo electrónico de prueba**.

10 Haga clic en **Guardar y reiniciar** para guardar los ajustes de configuración e inicializar los elementos base necesarios para configurar las áreas de trabajo y gestionar los dispositivos de los empleados mediante Horizon Mobile Manager.

Un mensaje indica que se está llevando a cabo el reinicio.

Cuando se haya finalizado el proceso de reinicio, Horizon Mobile Manager se inicializa y puede iniciar sesión en la interfaz de administración mediante la cuenta del usuario especificada para el administrador del sistema predeterminado.

NOTA: Debe hacer clic en **Guardar y reiniciar** para asegurarse de que los elementos base estén inicializados antes de iniciar sesión en la interfaz de administración. De lo contrario, puede que algunos elementos necesarios no estén disponibles.

Qué hacer a continuación

Ahora podrá configurar los usuarios de áreas de trabajo en Horizon Mobile Manager. En su navegador, introduzca la dirección URL de la interfaz de administrador de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`***

Si especifica el servicio de nombres incrustado y no modifica el valor predeterminado para el nombre del administrador del sistema, puede iniciar sesión en la interfaz del administrador con el nombre de usuario **`admin`** y la contraseña **`vmware`**.

Para obtener más información sobre cómo utilizar Horizon Mobile Manager, tras iniciar sesión consulte la ayuda en línea.

Configuración de los ajustes de NDES para usarlos con Horizon Mobile Manager

6

Horizon Mobile Manager incluye un complemento de conector del protocolo de inscripción simple de certificados (SCEP) para el servicio de inscripción de dispositivos de red (NDES) de Microsoft. Este complemento de conector del SCEP admite una conexión entre Horizon Mobile Manager y el servidor NDES de Microsoft de su compañía para automatizar el proceso de creación de certificados digitales para los dispositivos gestionados.

Prerequisitos

- Verifique que está utilizando una versión reciente de los navegadores Chrome, Firefox, Internet Explorer o Safari.
- Añada claves de licencia. Consulte Capítulo 4, "Adición de claves de licencia," página 15.
- Configure los ajustes de Horizon Mobile Manager y haga clic en **Guardar y reiniciar** para inicializar el sistema. Consulte Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17.

Procedimiento

1 En su navegador, introduzca la dirección URL de la interfaz de configuración de Horizon Mobile Manager con el formato **`https://`*`dirección_ip`*`:5480`**

2 Inicie sesión como usuario **`root`**.

Utilice la contraseña que estableció cuando configuró la aplicación virtual Horizon Mobile Manager. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

3 Haga clic en la pestaña **Horizon** y haga clic en **SCEP**.

El conector del NDES que proporciona Horizon Mobile Manager está incluido en la lista de conectores SCEP.

4 Haga clic en **Agregar servidor SCEP**.

En la ventana Agregar un servidor SCEP, proporcione la información siguiente:

Nombre del servidor	El nombre del servidor NDES de Microsoft de su compañía.
URL externa	La URL que utilizan los clientes de NDES para comunicarse con el servidor NDES de Microsoft de su compañía.
Conector SCEP	El complemento de conector SCEP utilizado para conectar con el servidor NDES. Se muestra el conector NDES proporcionado.
URL admin	La URL que utilizan los administradores para gestionar el servidor NDES de Microsoft de su compañía.

Nombre de usuario admin	El nombre de usuario del administrador del NDES de Microsoft de su compañía.
Contraseña admin	La contraseña del administrador del NDES de Microsoft de su compañía.
Dominio	El nombre del dominio de Windows en el que se creó la cuenta de administrador del NDES de su compañía.

5 Haga clic en **Agregar** para añadir la información del servidor NDES a Horizon Mobile Manager.

Certificados digitales y Horizon Mobile Manager 7

Horizon Mobile Manager codifica la información de sesión con certificados digitales estándar, y las comunicaciones entre Horizon Mobile Manager y los dispositivos móviles se envían mediante conexiones con protocolo SSL. El entorno de implementación debe permitir la capacidad de Horizon Mobile Manager de presentar certificados válidos a los dispositivos y propagar certificados firmados que se utilizan en las áreas de trabajo en esos dispositivos.

Los certificados que se utilizan entre Horizon Mobile Manager y los dispositivos móviles son:

Certificado SSL	Cifra la sesión segura entre el servidor y el cliente (el dispositivo móvil).
Certificado de firma	Firma digitalmente las comunicaciones entre el servidor y el cliente.
Certificados de autoridad de certificación (CA) raíz e intermedia	Proporcione una cadena de confianza de certificado para determinar si se debe confiar en un certificado SSL o de firma concreto.

Cuando instale y configure Horizon Mobile Manager por primera vez, se generará automáticamente un certificado SSL autofirmado y un certificado de firma mediante una autoridad de certificación (CA) raíz interna y la URL de servidor que se especifica en la interfaz de usuario de comunicación (vea Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17). En la página Seguridad de la interfaz de administración de Horizon Mobile Manager aparece una lista de los alias correspondientes a los certificados generados de forma automática.

En su configuración predeterminada, Horizon Mobile Manager utiliza estos certificados generados automáticamente y autofirmados. Para decidir entre el uso de los certificados predeterminados o sustituirlos por uno propio, debe tener en cuenta:

- Qué enfoque es el más apropiado para la configuración de implementación que ha elegido.

- Qué requisitos puede imponer a los propietarios de dispositivos. El uso de certificados SSL autofirmados requiere que los propietarios de dispositivos actualicen los ajustes de autenticación en sus dispositivos para garantizar que estos pueden comunicarse con el servidor (vea "Requisitos de dispositivos móviles al utilizar certificados SSL autofirmados," página 26).

ADVERTENCIA: Todos los cambios que realice al sustituir los certificados predeterminados en el servidor Apache incrustado se perderán si cambia la dirección URL del servidor de concesiones empleada por Horizon Mobile Manager. La dirección URL del servidor de concesiones se establece en la interfaz de configuración de Horizon Mobile Manager (como se describe en Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17). Cuando hace clic en el botón **Guardar y reiniciar** en la interfaz de comunicación, el sistema genera automáticamente nuevos certificados predeterminados que utilizan dicha dirección URL del servidor de concesiones como dominio y que están firmados por la autoridad de certificación raíz MVP interna. Los nuevos certificados generados sustituyen los utilizados anteriormente. Por lo tanto, si sustituye los certificados predeterminados por los suyos propios y luego cambia la dirección URL del servidor de concesiones, deberá repetir el proceso de sustitución de certificados.

Enfoques para certificados según la configuración de implementación

La siguiente tabla describe las opciones apropiadas para cada configuración de implementación.

Tabla 7-1. Configuraciones de implementación de Horizon Mobile Manager y enfoques apropiados para certificados

Configuración	Opciones de certificados
Horizon Mobile Manager en su red DMZ	■ Utilice los certificados autofirmados predeterminados del servidor Apache incrustado. ■ Sustituya los certificados autofirmados predeterminados del servidor Apache incrustado. Sus certificados pueden ser autofirmados o firmados por una autoridad de certificación de confianza. Cuando sustituya un certificado predeterminado, debe cargar el certificado de la autoridad de certificación raíz y todos los certificados de la autoridad de certificación intermedia que estén en la cadena de confianza de ese certificado. Consulte "Sustitución de los certificados predeterminados por certificados firmados de confianza," página 26 y "Sustituya el certificado SSL predeterminado en una DMZ o en una configuración de implementación NAT," página 27.
Horizon Mobile Manager en la red interna de la empresa y utilizando NAT	■ Utilice los certificados autofirmados predeterminados del servidor Apache incrustado. ■ Sustituya los certificados autofirmados predeterminados del servidor Apache incrustado. Sus certificados pueden ser autofirmados o firmados por una autoridad de certificación de confianza. Cuando sustituya un certificado predeterminado, debe cargar el certificado de la autoridad de certificación raíz y todos los certificados de la autoridad de certificación intermedia que estén en la cadena de confianza de ese certificado. Consulte "Sustitución de los certificados predeterminados por certificados firmados de confianza," página 26 y "Sustituya el certificado SSL predeterminado en una DMZ o en una configuración de implementación NAT," página 27.
Horizon Mobile Manager en la red interna de la empresa y utilizando un servidor proxy inverso en la DMZ	Debido a que el uso de un servidor proxy inverso requiere que ese servidor esté configurado para comunicaciones SSL, utilice su propio certificado SSL en su servidor proxy inverso. Este certificado pueden ser autofirmado o firmado por una autoridad de certificación de confianza. En esta configuración, debe cargar el certificado de la autoridad de certificación raíz y todos los certificados de la autoridad de certificación intermedia que estén en la cadena de confianza de ese certificado SSL. Consulte "Sustitución de los certificados predeterminados por certificados firmados de confianza," página 26 y "Utilice su propio certificado SSL firmado de confianza en una configuración de implementación de servidor proxy inverso," página 29.

Este capítulo cubre los siguientes temas:

Requisitos de dispositivos móviles al utilizar certificados SSL autofirmados

Aunque los certificados generados automáticamente son únicos y permiten el uso inicial o en prueba de concepto del servidor, no están firmados por una autoridad de certificación conocida y de confianza. Como resultado, antes de que sus propietarios de dispositivos inicien la aplicación VMware® Switch para instalar sus áreas de trabajo corporativas por primera vez, deben actualizar la configuración de autenticación predeterminada de la aplicación Switch.

Cuando Horizon Mobile Manager utiliza certificados SSL autofirmados, los propietarios de dispositivos deben anular la selección de la casilla de verificación **Autenticar servidor** en la configuración de la aplicación Switch. Esa casilla de verificación está seleccionada de forma predeterminada cuando se instala la aplicación Switch. Si la casilla de verificación **Autenticar servidor** está seleccionada y el certificado SSL es un certificado autofirmado, el dispositivo intentará utilizar el almacén de confianza de Android de autoridades de certificación conocidas para verificar el certificado. Como el certificado no está firmado por una autoridad de certificación conocida, la sesión no lo autentica y el dispositivo se niega a conectarse con Horizon Mobile Manager.

Si su implementación de Horizon Mobile Manager está utilizando un certificado SSL autofirmado (ya sea uno generador automáticamente de forma predeterminada o su propio certificado autofirmado), notifique a sus propietarios de dispositivos que se aseguren de anular la selección de la casilla de verificación **Autenticar servidor** antes de iniciar la aplicación Switch para realizar la instalación inicial del área de trabajo. Cuando se anula la selección de la casilla de verificación, el dispositivo ignora el hecho de que el certificado SSL es autofirmado y permite la conexión con Horizon Mobile Manager. Para ver el ajuste **Autenticar servidor** de la aplicación Switch en el dispositivo, abra la pantalla **Configuración de la aplicación**, toque **VMware Switch** y, a continuación, toque **Administrar espacio**.

NOTA: Cuando la casilla de verificación **Autenticar servidor** no está seleccionada y el propietario del dispositivo realiza la instalación inicial, aparece un mensaje que advierte al usuario de esta situación, aunque la comunicación sea segura con el protocolo SSL.

Sustitución de los certificados predeterminados por certificados firmados de confianza

La sustitución del certificado SSL autofirmado predeterminado por un certificado que esté firmado por una autoridad de certificación (CA) de confianza evita la alteración por parte de los propietarios de dispositivos de los ajustes de la aplicación Switch.

NOTA: Aunque existen beneficios al sustituir el certificado SSL predeterminado por uno que esté firmado por una CA de confianza, normalmente no existe una razón de peso para sustituir el certificado de firma predeterminado a no ser que sospeche que el certificado internal-ca-root generado automáticamente ha quedado al descubierto.

Para una implementación DMZ o NAT, se sustituye el certificado SSL generado automáticamente en el servidor Apache incrustado por su propio certificado SSL firmado de confianza. En la configuración de servidor proxy inverso, se utiliza su propio certificado SSL firmado de confianza en su servidor proxy inverso. En todas las configuraciones de implementación, si usa su propio certificado (SSL o de firma) debe cargar en Horizon Mobile Manager el certificado de la autoridad de certificación raíz y todos los certificados de la autoridad de certificación intermedia que estén en la cadena de confianza del certificado de sustitución.

El procedimiento general para sustituir el certificado SSL predeterminado o el certificado de firma por su propio certificado firmado de confianza:

1 Genere una clave privada y una solicitud de firma de certificado (CSR).

2 Envíe la CSR a la autoridad de certificación (CA) que va a firmar su certificado.

La CA le enviará su certificado firmado, junto con la cadena de certificados raíz e intermedios de la CA de confianza que utiliza su certificado.

3 Cargue su certificado firmado y la CA certificará que ha firmado su certificado con el fin de que pueda utilizarse en Horizon Mobile Manager:

En la configuración de DMZ o NAT	Cargue su certificado SSL de confianza en el servidor Apache incrustado desde la consola de la aplicación virtual. Cargue un certificado de firma de sustitución utilizando la interfaz de administración.
En la configuración del servidor proxy inverso	Cargue su certificado SSL de confianza en el servidor proxy inverso. Cargue un certificado de firma de sustitución utilizando la interfaz de administración.
Para todas las configuraciones	Cargue los certificados de CA raíz e intermedia para todos los certificados de sustitución (SSL o de firma) utilizando la interfaz de administración.

Sustituya el certificado SSL predeterminado en una DMZ o en una configuración de implementación NAT

Para utilizar su propio certificado SSL firmado de confianza cuando utilice Horizon Mobile Manager en su DMZ o en la configuración de implementación NAT, sustituya el certificado generado automáticamente por su propio certificado.

Prerequisitos

Instale la aplicación virtual Horizon Mobile Manager y configúrela.

En vSphere Client, active la aplicación virtual, haga clic en la pestaña **Consola** e inicie sesión en el sistema operativo Linux de la aplicación virtual como usuario **`raíz`**. Utilice la contraseña que estableció cuando configuró la aplicación virtual. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

Procedimiento

1 En la consola de la aplicación virtual, escriba el comando siguiente para generar una clave privada y una CSR.

```
openssl req –out CSR.csr –new –newkey rsa:2048 –nodes –keyout privateKey.key
```

El comando le pide la información requerida para la CSR.

2 En las indicaciones, introduzca la información correcta para su empresa.

En **`Nombre común`**, introduzca el nombre de dominio completo que deben introducir los propietarios del dispositivo en la aplicación Switch para iniciar sesión en el servidor y configurar inicialmente sus áreas de trabajo. Este nombre de dominio debe ser:

- El nombre de dominio completo que se resuelve externamente en la dirección IP pública utilizada en esta implementación de Horizon Mobile Manager.
- La misma dirección URL accesible externamente que se introdujo para la **Dirección URL del servidor de inicio de sesión** (sin la parte https:// de la dirección URL) cuando se configuró la aplicación virtual.

Por ejemplo, el bloque de códigos siguiente muestra entradas para una dirección URL de servidor de inicio de sesión *nuestro.nombrededominio.com*.

```
Generando una clave privada RSA de 2048 bits
.............................................+
++...........+++
escribiendo nueva clave privada en 'privateKey.key'
-----
```

```
Se le va a pedir que introduzca información que se incorporará
a su solicitud de certificados.
Está a punto de introducir lo que se llama un Nombre distinguido o DN.
Hay algunos campos, pero puede dejar algunos en blanco.
Para algunos campos hay un valor predeterminado.
Si introduce '.', el campo quedará en blanco.
-----
Nombre del país (código de 2 letras) [AU]:US
Nombre del estado o provincia (nombre completo) [Some-State]:Massachusetts
Nombre de la localidad (p. ej., ciudad) [ ]:Cambridge
Nombre de la organización (p. ej., empresa) [Internet Widgets Pty Ltd]:NuestraEmpresa
Nombre de la unidad organizacional (p. ej., sección) [ ]:NuestraUnidad
Nombre común (p. ej., SU nombre) [ ]:nuestro.nombrededominio.com
Dirección de correo electrónico [ ]:nuestrowebmaster@nuestraempresa.com
Introduzca los atributos 'extra' siguientes que se enviarán con la solicitud de certificados
Una contraseña de comprobación [ ]:
Un nombre opcional de la empresa [ ]:
```

El comando genera dos archivos: `CSR.csr` y `privateKey.key`.

3 Envíe el archivo `CSR.csr` a la autoridad de certificación. La autoridad de certificación le envía el certificado firmado (por ejemplo, `cert.pem`), los certificados de la autoridad de certificación raíz e intermedia utilizados por su certificado, y el archivo de la cadena de certificados (por ejemplo, `chain.pem`) para usar con él.

4 Inicie sesión como administrador en la interfaz de administración de Horizon Mobile Manager. En el navegador, vaya a la dirección URL de administración de Horizon Mobile Manager, con formato **`https://`*`dirección_ip`***, donde *dirección_ip* es la dirección IP privada de Horizon Mobile Manager. Inicie sesión con la cuenta de usuario de Horizon Mobile Manager a la que se le asignó la función de administrador. Si la implementación está configurada para utilizar el servicio de nombres incrustado y no modifica el valor predeterminado para el nombre del administrador del sistema, puede iniciar sesión en la interfaz de administración con el nombre de usuario **`admin`** y la contraseña **`vmware`**.

5 Haga clic en **Seguridad** para visualizar la página Seguridad.

6 En la sección **Cadena de certificados de confianza de servidor**, cargue el certificado de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia que firmaron su certificado SSL. Haga clic en el botón **Cargar nuevo certificado** para cargar cada certificado.

Este paso asegura que, cuando se aprovisionen dispositivos móviles, el certificado de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia necesarios para confiar en las comunicaciones SSL se incluyan en el almacén de claves del área de trabajo del dispositivo.

ADVERTENCIA: No elimine ninguno de los certificados enumerados en la lista **Cadena de certificados de confianza de servidor**, en particular ningún certificado de la autoridad de certificación raíz (incluido el certificado de la autoridad de certificación interna predeterminado de MVP), excepto en circunstancias muy controladas. Eliminar un certificado de la autoridad de certificación raíz de la lista **Cadena de certificados de confianza de servidor** lo eliminará de todos los dispositivos aprovisionados en la siguiente operación de renovación de la concesión. A menos que cuente con un certificado raíz sustituto, debe borrar esos dispositivos aprovisionados y volver a aprovisionarlos. Es extremadamente poco frecuente tener que eliminar un certificado de la lista. El único motivo para eliminar un certificado de esta lista es que sospeche que el certificado esté comprometido. En esa situación, debe seguir una secuencia de pasos específica para asegurar que las áreas de trabajo ya instaladas en los dispositivos de los usuarios se mantengan operativos (según se describe en "Cambie los certificados de la autoridad de certificación raíz e intermedia para las áreas de trabajo aprovisionadas," página 32).

7 Si la instancia de Horizon Mobile Manager ya ha aprovisionado los dispositivos, espere a que pase el período de renovación de la concesión para que todos los dispositivos realicen una llamada de concesión. Cuando se renueve la concesión, los certificados de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia se envían a las áreas de trabajo. Esperar a que pase el período de renovación de la concesión asegura que la cadena de confianza de certificados se instale en los almacenes de claves de las áreas de trabajo antes de que se utilice el nuevo certificado SSL en el servidor Apache incrustado.

ADVERTENCIA: Los dispositivos que se desconecten y no tengan acceso a la red durante un período mayor al intervalo de la concesión no pueden obtener nuevos certificados en este momento. Las áreas de trabajo en los dispositivos que estén desconectados durante un período que supere el intervalo de la concesión, de modo que no obtengan los nuevos certificados, no confiarán en la comunicación SSL con el servidor cuando estos dispositivos vuelvan a tener acceso a la red. Estas áreas de trabajo deberán borrarse y reaprovisionarse para habilitar las comunicaciones.

8 Utilice el comando `scp` para asegurar la copia del certificado SSL firmado en el sistema de archivos de la aplicación virtual.

9 En el sistema de archivos de la aplicación virtual, edite el archivo `/etc/apache2/vhosts.d/mmp.conf` y compruebe que las líneas relacionadas con los archivos de certificados SSL figuren en el archivo; asimismo, asegúrese de que las rutas se dirijan a los certificados y a la clave privada generada.

Por ejemplo:

```
SSLCertificateFile /ruta/al/certificado/firmado.pem
SSLCertificateKeyFile /ruta/a/su/privateKey/generada.key
SSLCertificateChainFile /ruta/a/la/cadena/de/certificados.pem
```

10 Reinicie el servidor Apache con el comando siguiente: `/etc/init.d/apache2 graceful`

Después de reiniciar, el servidor Apache incrustado utiliza el nuevo certificado SSL.

Utilice su propio certificado SSL firmado de confianza en una configuración de implementación de servidor proxy inverso

Debido a que el uso de un servidor proxy inverso requiere que ese servidor esté configurado para comunicaciones SSL, utilice su propio certificado SSL en su servidor proxy inverso. Si bien este certificado puede estar autofirmado o puede estar firmado por una autoridad de certificación de confianza, una de las ventajas de sustituir el certificado SSL autofirmado predeterminado por un certificado que esté firmado por una autoridad de certificación de confianza es evitar que los propietarios de los dispositivos desmarquen la casilla de verificación **Autenticar servidor** en la aplicación Switch.

Para esta configuración de implementación, debe cargar en Horizon Mobile Manager el certificado de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia que estén en su cadena de confianza del certificado SSL. Se recomienda que realice una carga de la cadena de confianza antes de aprovisionar algún dispositivo, de modo que tengan la cadena de confianza correcta cuando se instalen las áreas de trabajo en los dispositivos por primera vez.

Prerequisitos

Active la aplicación virtual Horizon Mobile Manager.

Procedimiento

1 Inicie sesión en la interfaz de administración de Horizon Mobile Manager. En el navegador, vaya a la dirección URL de administración de Horizon Mobile Manager, con formato **`https://`*`dirección_ip`***, donde *dirección_ip* es la dirección IP privada de Horizon Mobile Manager. Inicie sesión con el usuario de Horizon Mobile Manager al que se le asignó la función de administrador. Si la implementación está configurada para utilizar el servicio de nombres incrustado y no modifica el valor predeterminado para el nombre del administrador del sistema, puede iniciar sesión en la interfaz de administración con el nombre de usuario **`admin`** y la contraseña **`vmware`**.

2 Haga clic en **Seguridad** para visualizar la página Seguridad.

3 En la sección **Cadena de certificados de confianza de servidor**, cargue el certificado de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia que firmaron su certificado SSL. Haga clic en el botón **Cargar nuevo certificado** para cargar cada certificado.

   Este paso asegura que, cuando se aprovisionen dispositivos móviles, el certificado de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia necesarios para confiar en las comunicaciones SSL se incluyan en el almacén de claves del área de trabajo del dispositivo.

ADVERTENCIA: No elimine ninguno de los certificados enumerados en la lista **Cadena de certificados de confianza de servidor**, en particular ningún certificado de la autoridad de certificación raíz (incluido el certificado de la autoridad de certificación interna predeterminado de MVP), excepto en circunstancias muy controladas. Eliminar un certificado de la autoridad de certificación raíz de la lista **Cadena de certificados de confianza de servidor** lo eliminará de todos los dispositivos aprovisionados en la siguiente operación de renovación de la concesión. A menos que cuente con un certificado raíz sustituto, debe borrar esos dispositivos aprovisionados y volver a aprovisionarlos. Es extremadamente poco frecuente tener que eliminar un certificado de la lista. El único motivo para eliminar un certificado de esta lista es que sospeche que el certificado esté comprometido. En esa situación, debe seguir una secuencia de pasos específica para asegurar que las áreas de trabajo ya instaladas en los dispositivos de los usuarios se mantengan operativos (según se describe en "Cambie los certificados de la autoridad de certificación raíz e intermedia para las áreas de trabajo aprovisionadas," página 32).

En este momento, los dispositivos se pueden aprovisionar con el servidor proxy inverso.

Sustituya el certificado de firma predeterminado

En general, no hay razones fundadas para sustituir el certificado de firmas predeterminado a menos que sospeche que el certificado internal-ca-root generado automáticamente esté comprometido.

Prerequisitos

Active la aplicación virtual Horizon Mobile Manager.

Procedimiento

1 Inicie sesión como administrador en la interfaz de administración y haga clic en **Seguridad** para visualizar la página Seguridad.

2 Haga clic en el botón **Generar una solicitud de firma de certificado** en la sección **Certificado de firma de servidor** para generar la CSR que enviará a la autoridad de certificación.

3 Envíe la CSR a la autoridad de certificación por correo electrónico.

4 Cuando la autoridad de certificación le devuelva el nuevo certificado de firmas, y los certificados de la autoridad de certificación raíz e intermedia que firmó, expanda la sección **Cadena de certificados de confianza de servidor** en la página Seguridad y haga clic en **Cargar nuevo certificado** para cargar cada certificado de la autoridad de certificación raíz e intermedia.

ADVERTENCIA: No elimine ninguno de los certificados enumerados en la lista **Cadena de certificados de confianza de servidor**, en particular ningún certificado de la autoridad de certificación raíz (incluido el certificado de la autoridad de certificación interna predeterminado de MVP) hasta después de Step 5 y que haya pasado el período de renovación de la concesión.

5 Espere a que pase el período de renovación de la concesión para que todos los dispositivos realicen una llamada de concesión. Cuando se renueve la concesión, los certificados de la autoridad de certificación raíz y los certificados de la autoridad de certificación intermedia se envían a las áreas de trabajo. Esperar a que pase el período de renovación de la concesión asegura que la cadena de confianza de certificados para el certificado de firmas sustituto se instale en los almacenes de claves de las áreas de trabajo antes de que el nuevo certificado de firmas sea el certificado activo.

ADVERTENCIA: Los dispositivos que se desconecten y no tengan acceso a la red durante un período mayor al intervalo de la concesión no pueden obtener nuevos certificados en este momento. Las áreas de trabajo en los dispositivos que estén desconectados durante un período que supere el intervalo de la concesión, de modo que no obtengan los nuevos certificados, no funcionarán correctamente cuando estos dispositivos vuelvan a tener acceso a la red. Estas áreas de trabajo deberán borrarse y reaprovisionarse.

6 En la página Seguridad, expanda la sección **Certificados de firma de servidor** y haga clic en **Cargar nuevo certificado** para cargar el nuevo certificado de firmas enviado por la autoridad de certificación.

7 Utilice la lista desplegable **Certificado de firma** para seleccionar el nuevo certificado de firmas y convertirlo en el certificado activo.

ADVERTENCIA: No elimine de la lista **Certificado de firma de servidor** el certificado de firmas utilizado anteriormente hasta después de Step 8 y de que haya pasado un segundo período de renovación de la concesión.

8 Espere a que pase el período de renovación de la concesión para que todos los dispositivos realicen otra llamada de concesión. Cuando se renueva la concesión, el nuevo certificado de firmas se envía a las áreas de trabajo como certificado de firmas activo. Esperar a que pase el período de renovación de la concesión asegura que las áreas de trabajo utilicen el nuevo certificado para firmar los mensajes antes de que elimine de la lista el certificado de firmas antiguo.

ADVERTENCIA: Los dispositivos que se desconecten y no tengan acceso a la red durante un período mayor al intervalo de la concesión no utilizar el nuevo certificado de firmas activo en este momento. Las áreas de trabajo en los dispositivos que estén desconectados durante un período que supere el intervalo de la concesión no funcionarán correctamente cuando esos dispositivos vuelvan a tener acceso a la red. Estas áreas de trabajo deberán borrarse y reaprovisionarse.

9 En la página Seguridad, expanda la lista **Certificados de firma de servidor** y elimine el certificado de firmas antiguo. En este momento, también puede eliminar los certificados de la autoridad de certificación raíz e intermedia asociados con el certificado de firmas antiguo, a menos que también se utilicen para el nuevo certificado de firmas.

En este momento, el certificado de firmas sustituto es el certificado activo utilizado por los dispositivos.

Cambie los certificados de la autoridad de certificación raíz e intermedia para las áreas de trabajo aprovisionadas

Las áreas de trabajo aprovisionadas utilizan la cadena de confianza de certificados especificada en la interfaz de administración para verificar las identidades del certificado SSL del lado del servidor y el certificado de firmas utilizados por Horizon Mobile Manager. Esta cadena de confianza de certificados se implementa en el área de trabajo cuando el área de trabajo se aprovisiona en el dispositivo. Si cree que un certificado de la cadena de confianza de certificados está comprometido, debe seguir esta secuencia de pasos para sustituir el certificado comprometido.

Seguir esta secuencia de pasos asegura que la nueva cadena de certificados de confianza se implemente en las áreas de trabajo aprovisionadas antes de que elimine los certificados individuales de la cadena de confianza. Si no sigue estos pasos y se rompe la cadena de confianza de certificados que ha sido implementada (por ejemplo, al eliminar un certificado de la autoridad de certificación raíz antes de que las áreas de trabajo puedan obtener el certificado de la autoridad de certificación raíz sustituto), las áreas de trabajo en los dispositivos dejarán de funcionar correctamente, y deberá borrar y volver a aprovisionar las áreas de trabajo.

Prerequisitos

Active la aplicación virtual Horizon Mobile Manager.

Procedimiento

1 Inicie sesión como administrador en la interfaz de administración de Horizon Mobile Manager y haga clic en **Seguridad** para visualizar la página Seguridad.

2 Haga clic en **Cargar nuevo certificado** para añadir el nuevo certificado de la autoridad de certificación raíz y cada uno de los certificados de la autoridad de certificación intermedia a la sección **Cadena de certificados de confianza de servidor**.

3 Espere a que pase el período de renovación de la concesión para que todos los dispositivos hagan una llamada de concesión al servidor. Cuando se renueve la concesión, el conjunto especificado de certificados de la autoridad de certificación raíz y certificados de la autoridad de certificación intermedia (incluidos los nuevos y los antiguos) se implementa en las áreas de trabajo.

4 Una vez transcurrido el período de renovación de la concesión, puede hacer clic en el botón **Eliminar** junto al certificado comprometido en la sección **Cadena de certificados de confianza de servidor**.

En la siguiente renovación de la concesión, la cadena de confianza de certificados se vuelve a implementar en las áreas de trabajo aprovisionadas, sin incluir el certificado comprometido eliminado. A partir de entonces, las áreas de trabajo utilizan la cadena de certificados de confianza actualizada.

ADVERTENCIA: Los dispositivos que se desconecten y no tengan acceso a la red durante un período mayor al intervalo de la concesión no pueden obtener nuevos certificados. Las áreas de trabajo en los dispositivos que estén desconectados durante un período que supere el intervalo de la concesión, de modo que no obtengan los nuevos certificados, no funcionarán correctamente cuando estos dispositivos vuelvan a tener acceso a la red. Estas áreas de trabajo deberán borrarse y reaprovisionarse.

Recupere un certificado de la autoridad de certificación raíz eliminado por accidente de la cadena de confianza de certificados

Si un administrador de Horizon Mobile Manager hace clic en **Eliminar** junto a un certificado de la autoridad de certificación raíz en la lista **Cadena de certificados de confianza de servidor** por accidente, el sistema muestra una advertencia que indica que eliminar el certificado de la autoridad de certificación raíz podría producir un error grave. Las áreas de trabajo ya aprovisionadas pueden perder la capacidad de realizar comunicaciones de confianza con el servidor cuando se elimina el certificado de la autoridad de certificación

raíz. Si el administrador selecciona continuar con la eliminación del certificado de la autoridad de certificación raíz sin seguir el procedimiento de sustitución y, a continuación, debe restaurar la configuración anterior, puede utilizar el procedimiento siguiente para restaurar el certificado de la autoridad de certificación raíz eliminado en la cadena de confianza de certificados.

Prerequisitos

En vSphere Client, active la aplicación virtual, haga clic en la pestaña **Consola** e inicie sesión en el sistema operativo Linux de la aplicación virtual como usuario **`raíz`**. Utilice la contraseña que estableció cuando configuró la aplicación virtual. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

Procedimiento

1 Escriba los comandos siguientes.

```
su tcserver
mkdir /opt/vmware-mmp/repo/security/certs-for-devices/internal-ca-root
cp /opt/vmware-mmp/repo/security/root/cert.pem /opt/vmware-mmp/repo/security/certs-for-
devices/internal-ca-root/
```

2 En la interfaz administrativa, actualice la página Seguridad. El certificado de la autoridad de certificación raíz se restaura en la lista **Cadena de certificados de confianza de servidor**.

Qué hacer a continuación

Después de restaurar el certificado de la autoridad de certificación raíz eliminado, debe borrar las áreas de trabajo y volver a aprovisionarlas a fin de que la cadena de confianza de certificados restaurada se implemente en los dispositivos.

Pruebas de verificación manual 8

Utilice estas pruebas manuales para verificar que su instalación de Horizon Mobile Manager puede suministrar y gestionar áreas de trabajo en teléfonos inteligentes VMware® Ready™.

Antes de iniciar estas pruebas, verifique que dispone de los siguientes elementos:

- Una instancia de Horizon Mobile Manager instalada, configurada y encendida.
- Un teléfono inteligente VMware Ready con:
  - Acceso a datos (Wi-Fi, 3G, LTE) a esa instancia de Horizon Mobile Manager.
  - Una conexión Wi-Fi activa.
  - Una tarjeta SIM instalada.
  - La aplicación VMware Switch instalada. La aplicación VMware Switch está disponible en Google Play.

    Si no ha configurado esta instancia de Horizon Mobile Manager para que utilice un certificado SSL firmado de confianza, verifique que la casilla de verificación **Autenticar servidor** no está activada en la configuración de Switch. Consulte "Requisitos de dispositivos móviles al utilizar certificados SSL autofirmados," página 26.
- Nombre y contraseña para el administrador predeterminado del sistema de Horizon Mobile Manager (vea Capítulo 5, "Configuración de los ajustes de Horizon Mobile Manager," página 17).
- Tres usuarios de prueba (sus nombres y contraseñas). Estos usuarios deben estar presentes en el servicio de nombres que utilice su instancia de Horizon Mobile Manager. El servicio de nombres se especifica durante la instalación y configuración de la aplicación virtual Horizon Mobile Manager. Si su instancia está utilizando el servicio OpenLDAP incrustado preconfigurado, utilice los tres usuarios preconfigurados como **`usuario20`**, **`usuario21`** y **`usuario22`**. La contraseña de los tres usuarios preconfigurados es **`vmware`**.
- Cinco archivos de imagen (en formato JPG o PNG) para los procedimientos de prueba de personalización y fondo de pantalla. Las imágenes deben tener los siguientes tamaños:
  - Imagen de logotipo de sitio de Horizon Mobile Manager: 80 píxeles por 50 píxeles.
  - Imagen de la pantalla de inicio de sesión: 600 píxeles por 400 píxeles.
  - Imagen de logotipo de empresa en el dispositivo: 200 píxeles por 200 píxeles.
  - Imágenes de fondo de pantalla de área de trabajo (dos archivos): 960 píxeles por 640 píxeles.
- La dirección URL del servidor de inicio de sesión para la instancia de Horizon Mobile Manager.
- Una URL que se pueda utilizar en un acceso directo en el área de trabajo (como la URL del sitio Web de su empresa).

Las pruebas en las que esté presente la aplicación cliente de correo electrónico de VMware requieren una cuenta de cliente de correo electrónico (que utilizará el usuario del dispositivo) y acceso Wi-Fi al servidor de correo electrónico (Microsoft Exchange o VMware Zimbra).

Se utilizan los siguientes términos en las pruebas de verificación:

administrador	Hace referencia a un usuario que tenga asignada la función de Administrador en Horizon Mobile Manager.
administrador del parque	Hace referencia a un usuario que tenga asignada la función de Administrador del parque en Horizon Mobile Manager.
teléfono personal	Hace referencia al lado personal del teléfono. Tras la instalación de un área de trabajo, el teléfono tiene dos lados: el teléfono personal y el área de trabajo. Cuando el teléfono tiene instalado un área de trabajo, puede cambiar entre los dos lados tocando el icono **Switch**.

Este capítulo cubre los siguientes temas:

Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios

En entornos de producción, se asignan funciones a personas de una organización en función de sus responsabilidades para llevar a cabo operaciones administrativas y de gestión. Mediante esta prueba se verifica que se pueden asignar funciones a dichos usuarios.

Durante la configuración inicial de la aplicación virtual Horizon Mobile Manager, se especifica una cuenta de usuario como administrador del sistema predeterminado. El administrador del sistema predeterminado puede iniciar sesión en la interfaz de administración y llevar a cabo todas las operaciones. Sin embargo, tras la configuración inicial, para mantener un seguimiento de auditoría coherente, las operaciones en curso las deben llevar a cabo los usuarios que tienen una función específica de administrador o administrador del parque. El

sistema únicamente muestra a los usuarios conectados las funciones que corresponden a los tipos de operaciones que tiene derecho a realizar su función asignada. Si desea obtener una descripción de las operaciones asociadas a las funciones estándares, consulte la ayuda en línea de administración de Horizon Mobile Manager.

NOTA: Si su instancia utiliza el servicio OpenLDAP integrado, puede utilizar **`usuario20`** y **`usuario21`** para llevar a cabo esta prueba. Asigne la función de administrador a **`usuario20`** y la función de administrador del parque a **`usuario21`**. La contraseña para ambos usuarios es **`vmware`**.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Procedimiento

1 Inicie sesión en Horizon Mobile Manager como administrador del sistema predeterminado (el que se especificó durante la configuración de esta instancia de Horizon Mobile Manager). Si su organización ha conservado los valores predeterminados durante el proceso de configuración, utilice el nombre **`admin`** y la contraseña **`vmware`**.

2 Haga clic en **Funciones y trabajos** en el panel de navegación de la izquierda y, a continuación, haga clic en **Editar.**

3 Asigne la función de administrador o administrador del parque a aquellos usuarios de su organización a los que desee confiar esas responsabilidades:

   a En la columna Agregar funciones, busque el usuario. Cuando el sistema muestre el nombre del usuario, haga clic en **Agregar funciones**. Seleccione la función apropiada para ese usuario. Por ejemplo, si está utilizando los usuarios preconfigurados para realizar esta prueba, asigne la función de administrador a **`usuario20`**.

   b Repita Step 3a para asignar funciones a otros usuarios. Por ejemplo, si está utilizando los usuarios preconfigurados para realizar esta prueba, asigne la función de administrador del parque a **`usuario21`**.

4 Haga clic en **Guardar**.

Qué hacer a continuación

Compruebe que las funciones asignadas están en vigor:

1 Inicie sesión en la interfaz de administración como usuario únicamente con la función de administrador del parque (por ejemplo, **`usuario21`**). Compruebe que en el panel de navegación de la izquierda aparecen los siguientes nombres: **Panel de control**, **Usuarios**, **Grupos**, **Conjuntos de directivas**, **Plantillas**, **Imágenes de áreas de trabajo** y **Aplicaciones**. Las opciones **Funciones y trabajos**, **Personalización** y **Seguridad** no aparecen en el panel de navegación de la izquierda, ya que el derecho para realizar sus operaciones asociadas pertenece a la función de administrador.

2 Inicie sesión en la interfaz de administración como usuario únicamente con la función de administrador (por ejemplo, **`usuario20`**). Compruebe que en el panel de navegación de la izquierda aparecen los siguientes nombres de página: **Panel de control**, **Funciones y trabajos**, **Personalización** y **Seguridad**. No se muestran más opciones, ya que la función de administrador únicamente tiene derechos para realizar las operaciones asociadas a las opciones mostradas.

Crear una plantilla

Esta prueba sirve para crear una plantilla. Una plantilla define un área de trabajo corporativa que se puede implementar en los dispositivos móviles de los usuarios. Una plantilla determina el software que se incluye en el área de trabajo, así como el fondo de pantalla y los accesos directos de la pantalla de inicio del área de trabajo.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Complete los pasos que se describen en "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Haga clic en **Plantillas** en el panel de navegación de la izquierda y, a continuación, haga clic en **Crear nueva plantilla**.

3 Escriba un nombre y una descripción, por ejemplo:

- **Nombre:** **`Plantilla de ventas`**
- **Descripción:** **`Plantilla para empleados de la organización de ventas`**

4 En la sección **Todas las aplicaciones**, haga clic en el icono **+** verde de la aplicación VMware View para incluirla en el área de trabajo. Compruebe que aparecen las dos aplicaciones en la sección **Aplicaciones implementadas**: VMware Email y VMware View.

5 En la sección **Personalización**:

a Cambie el fondo de pantalla haciendo clic en **Cargar nuevo**. Escriba un nombre para el fondo de pantalla (como **`Nuestro fondo de pantalla`**) y busque uno de sus archivos de imagen de 960 x 640 píxeles. Haga clic en **Guardar** y utilice el menú desplegable para seleccionar su fondo de pantalla.

b Haga clic en **Agregar acceso directo** y escriba un nombre y una URL (como, por ejemplo, el sitio web principal de su empresa).

6 Haga clic en **Guardar**.

Qué hacer a continuación

Compruebe que se ha creado la plantilla:

1 En el panel de navegación de la izquierda, compruebe que aparece el nombre de su plantilla en **Plantilla**.

2 Haga clic en la plantilla y compruebe que muestra las dos aplicaciones (VMware Email y VMware View), así como el acceso directo especificado.

Crear un conjunto de directivas

Esta prueba sirve para crear un conjunto de directivas. Un conjunto de directivas controla las acciones que pueden realizar los usuarios del dispositivo en el área de trabajo corporativa, así como las configuraciones de seguridad tales como la fortaleza de las contraseñas y su caducidad.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Complete los pasos que se describen en "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Haga clic en **Conjunto de directivas** en el panel de navegación de la izquierda y, a continuación, haga clic en **Crear nuevo conjunto de directivas**.

3 Escriba un nombre y una descripción, por ejemplo:

- **Nombre:** `Directivas del grupo de ventas`
- **Descripción:** `Configuración de directivas para empleados de la organización de ventas`

4 En la sección **Renovación de concesión**, seleccione un intervalo de 20 minutos. No cambie la configuración de deshabilitación automática o borrado automático.

5 Expanda la sección **Contraseña**. Compruebe que la opción **Solicitar contraseña** está seleccionada y que la opción **Fortaleza de la contraseña** está ajustada en **PIN**.

6 Haga clic en **Guardar**.

Qué hacer a continuación

Compruebe que se ha creado el conjunto de directivas:

1 En el panel de navegación de la izquierda, compruebe que aparece el nombre de su conjunto de directivas en **Conjuntos de directivas**.

2 Haga clic en su conjunto de directivas y compruebe que muestra la descripción y el intervalo de renovación de concesión que ha especificado.

Cree un grupo y añada un usuario al grupo

Esta prueba sirve para crear un grupo que se utiliza para asociar al usuario del dispositivo con el área de trabajo corporativa. Para que el dispositivo de un usuario pueda ser aprovisionado con un área de trabajo corporativa, el usuario de dicho dispositivo móvil debe pertenecer a un grupo. Un grupo de usuarios determina qué software se instala y qué directivas se aplican al área de trabajo corporativa implementada en el dispositivo.

Prerequisitos

Compruebe que tiene los usuarios tal y como se describe en Capítulo 8, "Pruebas de verificación manual," página 35.

Complete los pasos que se describen en "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36, "Crear una plantilla," página 38 y "Crear un conjunto de directivas," página 38.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Haga clic en **Grupos** en el panel de navegación de la izquierda y, a continuación, haga clic en **Crear nuevo grupo**.

3 Escriba un nombre y una descripción, por ejemplo:

- **Nombre:** `Grupo de ventas`

- **Descripción:** `Empleados de la organización de ventas`

4 Seleccione la plantilla y el conjunto de directivas que ha creado en "Crear una plantilla," página 38 y "Crear un conjunto de directivas," página 38.

5 En el campo de búsqueda de la columna **Agregar usuarios**, escriba el nombre del usuario del dispositivo al que identificó para su uso en estas pruebas de verificación. Los usuarios disponibles son aquellos del servicio de nombres especificado en la configuración de su instancia de Horizon Mobile Manager. Si esta instancia está utilizando el servicio OpenLDAP integrado, escriba **`usuario23`**.

6 Cuando el sistema muestre el nombre del usuario en la lista, haga clic en **Agregar** en la fila de dicho usuario. El nombre del usuario aparece en la columna Usuarios del grupo para indicar que dicho usuario está asignado a este grupo.

7 Haga clic en **Guardar**.

Qué hacer a continuación

Compruebe que se ha creado el grupo y que el usuario seleccionado se ha asignado a él:

1 En el panel de navegación de la izquierda, compruebe que aparece el nombre de su grupo en **Grupos**.

2 Haga clic en su grupo y compruebe que el usuario seleccionado aparece en la lista y que se muestra **Instalación pendiente** en el estado del área de trabajo. El estado es **Instalación pendiente** porque el área de trabajo aún no se ha aprovisionado al dispositivo del usuario.

Configure los elementos de personalización del área de trabajo y Horizon Mobile Manager

Esta prueba sirve para configurar los elementos de personalización que aparecen en el dispositivo móvil y en la interfaz de administración.

Prerequisitos

Compruebe que tiene los archivos de imagen descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Complete los pasos que se describen en "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador (como **`usuario20`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Haga clic en **Personalización** en el panel de navegación de la izquierda y, a continuación, haga clic en **Editar**.

3 En la sección **Personalización de sitios**, actualice los siguientes elementos:

   a Cambie el título del sitio a **`Nuestro sitio`** y el título de la pantalla de inicio de sesión a **`Nuestro Horizon Mobile Manager`**.

   b Cambie el logotipo del sitio haciendo clic en el botón **Examinar** correspondiente y seleccionando su archivo de imagen de 600 x 400 píxeles.

   c Cambie la imagen de la pantalla de inicio de sesión haciendo clic en el botón **Examinar** correspondiente y seleccionado su archivo de imagen de 80 x 50 píxeles.

4 En la sección **Personalización del área de trabajo**, actualice los siguientes elementos:

   a Cambie el nombre de la empresa (por ejemplo, **`Nuestra empresa`**). Este nombre aparece en el dispositivo cuando el usuario aprovisiona el área de trabajo por primera vez.

   b Cambie el texto de los términos de uso para utilizar el área de trabajo corporativa. Este texto aparece en el dispositivo cuando el usuario aprovisiona el área de trabajo por primera vez. Por ejemplo, puede escribir:
   `El uso que haga del área de trabajo corporativa de nuestra empresa se regirá por los términos de este acuerdo.`

   c Cambie la imagen del logotipo de la empresa haciendo clic en el botón **Examinar** correspondiente y seleccionando su archivo de imagen de 200 x 200 píxeles. Esta imagen aparece en el dispositivo cuando el usuario toca el icono de Switch para entrar en el área de trabajo.

5 Haga clic en **Guardar**.

Qué hacer a continuación

Compruebe los elementos de personalización de sitios:

1 Compruebe que el título que aparece en el titular superior es el título especificado en el campo **Título del sitio**.

2 Cierre la sesión y actualice el explorador. Compruebe que en la pantalla de inicio de sesión aparecen el logotipo del sitio y las imágenes de la pantalla de inicio de sesión.

Los elementos de personalización del área de trabajo se comprueban en "Instale el área de trabajo en un dispositivo móvil," página 41.

Instale el área de trabajo en un dispositivo móvil

Esta prueba sirve para aprovisionar un dispositivo con un área de trabajo.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Complete los pasos que se describen en "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36, "Crear una plantilla," página 38, "Crear un conjunto de directivas," página 38, "Cree un grupo y añada un usuario al grupo," página 39 y "Configure los elementos de personalización del área de trabajo y Horizon Mobile Manager," página 40.

Procedimiento

1 En el dispositivo móvil, toque el icono de **Switch**.

   Aparece el formulario Configurar VMware Switch.

2 Escriba el nombre de usuario y la contraseña de la cuenta de usuario que corresponde al usuario agregado al grupo en "Cree un grupo y añada un usuario al grupo," página 39.

   Si el usuario especificado no pertenece a ningún grupo definido en Horizon Mobile Manager, dicho usuario no podrá iniciar sesión y no se podrá aprovisionar el área de trabajo al dispositivo.

3 Escriba la dirección de dominio completa utilizada para el servidor de inicio de sesión de su instancia de Horizon Mobile Manager.

   Esta dirección se especifica en el campo **Dirección URL del servidor de inicio de sesión** al configurar la aplicación virtual. No es necesario que escriba la parte de la dirección que empieza por **`https://`**

4 Toque **Ir**. Una vez establecida la conexión, compruebe que los elementos de personalización de la empresa especificados en "Configure los elementos de personalización del área de trabajo y Horizon Mobile Manager," página 40 aparecen en el dispositivo.

5 Toque **Siguiente**.

Comienza el proceso de descarga e instalación del área de trabajo. Puede ver el progreso consultando las notificaciones que aparecen en el dispositivo. Una vez finalizada la instalación, se envía al dispositivo la siguiente notificación: `VMware Switch está listo. Toque su área de trabajo.`

6 Toque la notificación para abrir el área de trabajo y siga las instrucciones que aparecen en pantalla, incluyendo la creación de una contraseña.

Los requisitos de contraseña se especifican en "Crear un conjunto de directivas," página 38.

7 (Opcional) Introduzca las credenciales de correo electrónico para configurar el acceso para la prueba de la aplicación de correo electrónico. Utilice la cuenta de correo electrónico identificada para su uso en estas pruebas.

Puede aplazar el proceso de configuración de correo electrónico tocando **Configuración manual** y, a continuación, **Descartar**.

El dispositivo muestra la pantalla de inicio del área de trabajo.

Qué hacer a continuación

Compruebe que aparecen el fondo de pantalla y el acceso directo especificados en "Configure los elementos de personalización del área de trabajo y Horizon Mobile Manager," página 40. Toque el icono de visualización de la aplicación y compruebe la presencia de la aplicación agregada a la plantilla en "Crear una plantilla," página 38.

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Ver detalles sobre las interacciones con un dispositivo administrado

Esta prueba sirve para, como administrador del parque, ver los detalles sobre las interacciones de Horizon Mobile Manager con un dispositivo administrado.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 En el panel de navegación de la izquierda, haga clic en **Usuarios**.

3 Haga clic en el usuario que corresponde al dispositivo móvil aprovisionado.

Por ejemplo, si utilizó **`usuario23`** en "Instale el área de trabajo en un dispositivo móvil," página 41, seleccione ese usuario.

El sistema muestra información detallada sobre las interacciones entre el dispositivo móvil y Horizon Mobile Manager, como el historial de actualizaciones realizadas en el dispositivo, el estado de aprovisionamiento y el grupo, el conjunto de directivas y la plantilla asociados.

NOTA: La imagen gráfica del dispositivo muestra información de cuando el área de trabajo se aprovisionó por primera vez. Dicha información no se actualiza con los datos de los cambios realizados posteriormente en el dispositivo.

Qué hacer a continuación

Compruebe que en el historial de interacciones aparece la interacción de aprovisionamiento llevada a cabo en "Instale el área de trabajo en un dispositivo móvil," página 41.

Deshabilite y vuelva a habilitar el área de trabajo de un usuario

Esta prueba sirve para, como administrador del parque, deshabilitar el área de trabajo del usuario y, a continuación, volver a habilitarlo. Cuando el área de trabajo está deshabilitada, el usuario del dispositivo no puede acceder a ella. Cuando se vuelve a habilitar, el usuario puede acceder al área de trabajo.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 En el panel de navegación de la izquierda, haga clic en **Usuarios** y seleccione el usuario que corresponde al dispositivo aprovisionado.

El sistema muestra la página de detalles de dicho usuario.

3 En la página de detalles, haga clic en **Deshabilitar** para desactivar el usuario y, a continuación, haga clic en **Aceptar** en el mensaje de confirmación.

4 En el teléfono personal, toque **Configuración** > **Cuenta y sincronización** y, a continuación, toque el usuario asociado con la aplicación Switch (la cuenta de usuario con el icono de **`Switch`**).

5 Toque **Configuración** > **Sincronizar ahora** para iniciar la sincronización con Horizon Mobile Manager.

El dispositivo se comunica con el servidor de Horizon Mobile Manager y recibe la orden de deshabilitar el área de trabajo.

6 Abra las notificaciones que aparecen en el dispositivo móvil para ver la notificación de que Switch se ha desactivado.

7 En la lista de aplicaciones del teléfono personal, toque el icono de **Switch**. Aparece un mensaje que informa de que Switch se ha deshabilitado.

8 En la interfaz de administración de Horizon Mobile Manager, utilice el icono de actualización situado en el título superior para actualizar la página de detalles de usuarios. La página muestra el estado desactivado para ese usuario.

9 Haga clic en **Habilitar** para volver a activar el acceso al área de trabajo del usuario.

10 En el teléfono personal, repita Step 4 y Step 5 para sincronizar el dispositivo móvil con el servidor. Cuando vea la notificación de que se ha restaurado el acceso, toque el icono de **Switch** para confirmar que puede abrir el área de trabajo en el dispositivo.

Qué hacer a continuación

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Actualice las aplicaciones en el área de trabajo aprovisionada

Esta prueba sirve para agregar y eliminar aplicaciones del área de trabajo aprovisionada y actualizar el dispositivo administrado.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 En el panel de navegación de la izquierda, haga clic en la plantilla que define el área de trabajo aprovisionada y, a continuación, haga clic en **Editar.**

3 En la sección **Aplicaciones implementadas**, elimine la aplicación agregada en "Crear una plantilla," página 38 (la aplicación VMware View) haciendo clic en el icono rojo **X** de la aplicación.

4 Agregue otra aplicación a la sección **Aplicaciones implementadas** arrastrando el icono de la aplicación desde la sección **Todas las aplicaciones** a la sección **Aplicaciones implementadas**. Agregue una aplicación diferente a la que ha eliminado en Step 3.

5 Haga clic en **Implementar**. Aparece un mensaje avisándole de que los cambios afectarán a los usuarios asociados con la plantilla. Haga clic en **Aceptar**.

6 En el teléfono personal, sincronice el teléfono con Horizon Mobile Manager:

   a Toque **Configuración** > **Cuenta y sincronización**.

   b Toque el usuario asociado con la aplicación Switch.

   c Toque **Configuración** > **Sincronizar ahora**.

   El dispositivo se comunica con el servidor de Horizon Mobile Manager y actualiza el área de trabajo en función de la plantilla actualizada.

7 Cambie al área de trabajo y compruebe que el conjunto de aplicaciones refleja las selecciones realizadas en Step 3 y Step 4.

Qué hacer a continuación

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Actualice el fondo de pantalla y los accesos directos para el área de trabajo aprovisionada

Esta prueba sirve para actualizar el fondo de pantalla y los accesos directos utilizados en la pantalla de inicio del área de trabajo y actualizar el dispositivo administrado.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **usuario21** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 En el panel de navegación de la izquierda, haga clic en la plantilla que define el área de trabajo aprovisionada y, a continuación, haga clic en **Editar**.

3 En la sección **Personalización**, haga clic en **Cargar nuevo** para cargar la otra imagen de fondo de pantalla de 960 x 640 píxeles (tal y como se describe en Capítulo 8, "Pruebas de verificación manual," página 35), y utilice el control desplegable para seleccionarla como el fondo de pantalla actual.

4 Haga clic en **Agregar acceso directo** y agregue otro acceso directo a la lista (por ejemplo, **communities.vmware.com**).

5 Haga clic en **Implementar.**

6 En el teléfono personal, sincronice el dispositivo con el servidor tal y como se describe en "Actualice las aplicaciones en el área de trabajo aprovisionada," página 44.

7 Cambie al área de trabajo y compruebe que el fondo de pantalla y los accesos directos de la pantalla de inicio reflejan sus selecciones.

Qué hacer a continuación

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Actualice la directiva de contraseñas del área de trabajo

Esta prueba sirve para actualizar la directiva de contraseñas del área de trabajo aprovisionada e implementar nuevas directivas en el dispositivo administrado.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **usuario21** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 En el panel de navegación de la izquierda, haga clic en el conjunto de directivas utilizado para el área de trabajo aprovisionada (el conjunto de directivas creado en "Crear un conjunto de directivas," página 38) y, a continuación, haga clic en **Editar**.

3 Haga clic en **Fortaleza de la contraseña** para expandir esta sección y, a continuación, seleccione **Manual** en la fortaleza de la contraseña. Ajuste la longitud de la contraseña en **6**, el mínimo de dígitos en **1** y el mínimo de caracteres especiales en **1**.

4 Haga clic en **Implementar** y, en el mensaje de alerta, haga clic en **Aceptar**.

5 En el teléfono personal, sincronice el dispositivo con el servidor tal y como se describe en "Actualice las aplicaciones en el área de trabajo aprovisionada," página 44.

6 Toque el icono de **Switch** para cambiar al área de trabajo. En el formulario de validación de contraseña, escriba la contraseña definida al aprovisionar el área de trabajo por primera vez (en "Instale el área de trabajo en un dispositivo móvil," página 41).

7 En el formulario de creación de contraseña, cree una contraseña nueva. Como prueba, escriba **1234**. Aparece un mensaje que describe la nueva directiva.

8 Escriba una contraseña que coincida con el conjunto de directivas en Step 3 y, a continuación, confirme la contraseña nueva.

Qué hacer a continuación

Compruebe que aparece el área de trabajo.

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Actualice la directiva de servicios de ubicación

Esta prueba sirve para cambiar la configuración de directivas del área de trabajo para los servicios de ubicación e implementar la nueva configuración en el dispositivo administrado.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 En el teléfono personal, deshabilite los servicios de ubicación.

Toque **Configuración** > **Servicios de ubicación** y, a continuación, desmarque las casillas de verificación correspondientes.

2 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

3 Haga clic en el conjunto de directivas utilizado por el área de trabajo aprovisionada y, a continuación, haga clic en **Editar**.

4 En la sección **Funciones**, seleccione la casilla de verificación **Servicios de ubicación obligatorios** si aún no está seleccionada. Compruebe que la precisión de ubicación está ajustada en **Precisión alta**.

5 Haga clic en **Implementar** y, en el mensaje de alerta, haga clic en **Aceptar**.

6 En el teléfono personal, sincronice el dispositivo con el servidor tal y como se describe en "Actualice las aplicaciones en el área de trabajo aprovisionada," página 44. Compruebe que, al tocar el icono de **Switch** para entrar en el área de trabajo, se muestra una alerta avisando de que se está infringiendo una directiva.

Si el administrador del parque especifica que los servicios de ubicación son obligatorios y el usuario del dispositivo deshabilita los servicios de ubicación en el dispositivo, se estará infringiendo una directiva y Horizon Mobile Manager deshabilitará el área de trabajo.

7 Vuelva a habilitar los servicios de ubicación en el dispositivo y cambie al área de trabajo. Compruebe que puede entrar en el área de trabajo.

8 Cambie al teléfono personal y modifique la configuración de la aplicación Switch para deshabilitar el acceso de esta a los servicios de ubicación:

a Toque **Configuración** > **Cuentas y sincronización** y, a continuación, toque la cuenta de usuario de Switch.

b Toque **Administrar la configuración de Switch**. En la pantalla Administrar la configuración de VMware Switch, toque **Ubicación**.

c Seleccione **Oculto** para ocultar los servicios de ubicación de la aplicación Switch.

9 Sincronice el dispositivo con el servidor. Compruebe que, al tocar el icono de **Switch** para entrar en el área de trabajo, se muestra una alerta avisando de que se está infringiendo una directiva.

Si el administrador del parque especifica que los servicios de ubicación son obligatorios y el usuario del dispositivo desactiva los servicios de ubicación en la configuración de Switch, se estará infringiendo una directiva y Horizon Mobile Manager desactivará el área de trabajo.

10 Repita Step 8a y Step 8b para abrir la configuración de ubicación de la aplicación Switch. Toque la configuración **Buena** para que coincida con la configuración **Precisión alta** en Horizon Mobile Manager (descrita en Step 4).

11 Toque el icono de **Switch** para cambiar al área de trabajo y compruebe que puede cambiar al área de trabajo.

Qué hacer a continuación

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Actualice la configuración de directivas para las funciones Cortar/Copiar/Pegar y Cámara

Esta prueba sirve para cambiar la configuración de directivas para utilizar las funciones cortar/copiar/pegar y la cámara en el área de trabajo, e implementar las nuevas directivas en el dispositivo administrado.

Cuando las funciones cortar/copiar/pegar no están activadas en el conjunto de directivas, el usuario no puede copiar texto del área de trabajo en el lado personal del dispositivo. Cuando la función de cámara no está activada en el conjunto de directivas, el usuario no puede utilizar la cámara en el área de trabajo.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, “Pruebas de verificación manual,” página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 En el teléfono personal, cambie al área de trabajo y compruebe que puede utilizar la cámara: visualice las aplicaciones, toque el icono de **Cámara** y tome una fotografía.

2 Copie texto en una aplicación del área de trabajo, cambie al teléfono personal y compruebe que puede pegar el texto en la aplicación.

3 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde “Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios,” página 36).

4 Haga clic en el conjunto de directivas utilizado por el área de trabajo aprovisionada y, a continuación, haga clic en **Editar**.

5 En la sección **Funciones**, desmarque las casillas de verificación correspondientes para deshabilitar las funciones cortar/pegar/copiar y la función de cámara. Haga clic en **Implementar** y, a continuación, haga clic en **Aceptar** en el mensaje de alerta.

6 En el teléfono personal, sincronice el dispositivo con el servidor (tal y como se describe en “Actualice las aplicaciones en el área de trabajo aprovisionada,” página 44). Repita Step 1 y Step 2 para comprobar que no puede utilizar la cámara en el área de trabajo ni copiar y pegar texto desde el área de trabajo en el teléfono personal.

Qué hacer a continuación

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Inicie un restablecimiento de la contraseña en el área de trabajo aprovisionada

Esta prueba sirve para forzar un restablecimiento de contraseña en el área de trabajo aprovisionada. Normalmente, esta acción se lleva a cabo cuando el usuario del dispositivo ha olvidado la contraseña del área de trabajo. Una vez restablecida la contraseña, se solicita al usuario que configure una contraseña nueva sin tener que validar la anterior.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Abra la página de detalles del usuario que corresponde al área de trabajo aprovisionada (tal y como se describe en "Deshabilite y vuelva a habilitar el área de trabajo de un usuario," página 43).

3 Haga clic en **Restablecer contraseña**. En el mensaje de confirmación, haga clic en **Aceptar**.

4 En el teléfono personal, sincronice el dispositivo con el servidor tal y como se describe en "Actualice las aplicaciones en el área de trabajo aprovisionada," página 44.

5 Cambie al área de trabajo. Compruebe que se le solicita que configure una contraseña nueva sin tener que validar la anterior.

6 Cree una contraseña nueva.

Qué hacer a continuación

Compruebe que el dispositivo muestra el área de trabajo después de crear la contraseña nueva.

Toque el icono de **Switch** en el área de trabajo para cambiar al teléfono personal.

Borre el área de trabajo aprovisionada del dispositivo

Esta prueba sirve para borrar el área de trabajo aprovisionada del dispositivo. Normalmente, esta acción se lleva a cabo cuando el usuario informa de la pérdida o el robo del dispositivo. Al borrar el área de trabajo aprovisionada, todos los datos del área de trabajo del dispositivo se eliminan y no se pueden recuperar.

Prerequisitos

Compruebe que tiene los elementos descritos en Capítulo 8, "Pruebas de verificación manual," página 35.

Compruebe que el área de trabajo se ha aprovisionado correctamente en el teléfono inteligente.

Procedimiento

1 Inicie sesión en la interfaz administrativa como administrador del parque (como **`usuario21`** desde "Cree administradores y administradores del parque mediante la asignación de funciones a los usuarios," página 36).

2 Abra la página de detalles del usuario que corresponde al área de trabajo aprovisionada (tal y como se describe en "Deshabilite y vuelva a habilitar el área de trabajo de un usuario," página 43).

3 Haga clic en **Borrar**. En el mensaje de confirmación, haga clic en **Aceptar**.

4 En el teléfono personal, sincronice el dispositivo con el servidor (tal y como se describe en "Actualice las aplicaciones en el área de trabajo aprovisionada," página 44). Se envía una notificación al dispositivo avisando de que el administrador ha borrado el área de trabajo.

5 Toque el icono de **Switch** para cambiar al área de trabajo.

6 Compruebe que aparece el formulario Configurar VMware Switch.

Dado que se ha eliminado el área de trabajo, aparece el formulario Configurar VMware Switch para comenzar el proceso de aprovisionamiento.

Qué hacer a continuación

En este momento, puede volver a aprovisionar el área de trabajo repitiendo los pasos "Instale el área de trabajo en un dispositivo móvil," página 41, o también puede cancelar el proceso de aprovisionamiento.

Uso del servicio OpenLDAP incrustado 9

El servicio OpenLDAP incrustado se utiliza normalmente con fines de demostración y en configuraciones de prueba. Cuando se usa el servicio OpenLDAP incrustado, es posible que desee realizar operaciones de LDAP comunes, como añadir nuevos usuarios, eliminar usuarios existentes y cambiar contraseñas de usuarios.

Esta información está destinada a los administradores de sistemas con experiencia que estén familiarizados con las operaciones y los comandos estándar de LDAP.

El servidor OpenLDAP incrustado utiliza el puerto TCP 389. El servidor OpenLDAP es únicamente accesible localmente desde la consola de Linux para la aplicación virtual Horizon Mobile Manager. Puede utilizar comandos estándar de LDAP para realizar operaciones en el servidor OpenLDAP incrustado. Los archivos binarios necesarios (`ldapadd`, `ldapsearch`, `ldapdelete` y `ldapmodify`) están instalados en la aplicación virtual.

De forma predeterminada, cuando se instala y se configura la aplicación virtual, se preconfigura el servicio OpenLDAP incrustado con entradas que tienen nombres comunes (`cn`) que siguen el patrón **`Usuario empresa 1`**, **`Usuario empresa 2`** y así sucesivamente. Los usuarios se preconfiguran con los siguientes atributos:

- `userPassword`: **`vmware`**
- `sn`: **`Usuario`**
- `uid`: Sigue el patrón **`usuario1`**, **`usuario2`** y así sucesivamente.
- `ou`: **`personas`**

Por ejemplo, la entrada preconfigurada para **`Usuario empresa 1`** tiene los siguientes valores de atributos.

```
cn: Usuario empresa 1
sn: Usuario
mail: usuario1@mvp.org
uid: usuario1
```

Durante la configuración de la aplicación virtual se especifica la cuenta de usuario que se va a utilizar como el administrador predeterminado del sistema. Esta cuenta puede acceder a la interfaz de administración de Horizon Mobile Manager y llevar a cabo todas las operaciones. Si se ha utilizado el valor predeterminado durante la configuración de la aplicación virtual, esta cuenta de usuario es la entrada preconfigurada del servicio LDAP incrustado que tiene su atributo `cn` establecido en **`Usuario Admin`**, su atributo `uid` establecido en **`admin`** y su atributo `userPassword` establecido en **`vmware`**.

Nombre distintivo de la base (DN), Bind DN y Bind PW

El Nombre distintivo de la base (`DN`) para el servidor OpenLDAP incrustado es **`dc=mvp, dc=org`**.

El parámetro `bind DN` es **`admin`** y el parámetro `bind PW` es **`vmware.`**

Cambio de la contraseña para la entrada predeterminada del administrador del sistema

Para cambiar la contraseña de la entrada de administrador preconfigurada (`uid:` **`admin`**), cree un archivo LDAP Data Interchange Format (formato de intercambio de datos LDAP, (LDIF)) con los parámetros de atributos apropiados y ejecute el comando `ldapmodify` para cambiar los valores existentes del archivo LDIF.

1 Inicie sesión en la aplicación virtual desde su consola.

2 Utilice un editor de texto para crear un nuevo archivo LDIF en el sistema de archivos. Por ejemplo, `vi /home/tcserver/changepass.ldif`

3 Introduzca las líneas apropiadas en el archivo LDIF y guarde el archivo. En este ejemplo, la contraseña para el `uid` **`admin`** queda cambiada a **`classic*CD`**.

```
dn: uid=admin,ou=people,dc=mvp,dc=org
changetype: modificar
replace: userPassword
userPassword: classic*CD
```

4 Ejecute el comando `ldapmodify`.

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/changepass.ldif
```

Si su instancia de Horizon Mobile Manager utiliza una cuenta de usuario preconfigurada como administrador predeterminado del sistema, la próxima vez que inicie sesión en la interfaz de administración de Horizon Mobile Manager, hágalo con el nombre de usuario **`admin`** y la nueva contraseña.

Cómo añadir un usuario al servicio OpenLDAP incrustado

En entornos de demostración, es posible que desee tener cuentas de usuario que se correspondan con personas de su organización o equipo, o bien emplear nombres que no sean los preconfigurados. Puede utilizar un archivo LDIF y la operación `ldapadd` estándar para añadir nuevas entradas al servicio OpenLDAP. En este ejemplo, un archivo LDIF con el nombre addentry.ldif define una entrada para la persona Stacy Barr, con el `uid:`**`sbarr`** y `userPassword:`**`stacy*b`**.

```
dn: uid=sbarr,ou=people,dc=mvp,dc=org
objectclass: top
objectClass: person
objectClass: organizationalPerson
objectClass: inetOrgPerson
cn: Stacy Barr
sn: Barr
uid:sbarr
mail: s.barr@mvp.org
userPassword: stacy*b
```

Para añadir la entrada al servicio OpenLDAP incrustado, ejecute el comando `ldapadd` en la consola de la aplicación virtual.

```
/usr/bin/ldapadd –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/addentry.ldif
```

Cómo eliminar un usuario del servicio OpenLDAP incrustado

Utilice el comando `ldapdelete` en la consola de la aplicación virtual para eliminar una entrada del servicio OpenLDAP incrustado.

Por ejemplo, para eliminar la entrada **user50** preconfigurada, ejecute:

```
/usr/bin/ldapdelete –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware
"uid=user50,ou=people,dc=mvp,dc=org"
```

Cambio de las contraseñas de usuarios

Del mismo modo que en los pasos para cambiar la configuración de la cuenta de administrador predeterminado, puede utilizar un archivo LDIF y la operación `ldapmodify` estándar para cambiar las contraseñas de los usuarios. Para cambiar más de una contraseña de usuario utilizando un único archivo LDIF en una operación `ldapmodify`, cree un bloque de cuatro líneas en el archivo de cada usuario, separando cada bloque con una línea en blanco.

Por ejemplo, para cambiar las contraseñas de los usuarios preconfigurados **usuario21**, **usuario22**, **usuario23** y **usuario24**, cree un archivo LDIF con el nombre **changeuserpwd.ldif** que contenga las líneas siguientes.

```
dn: uid=usuario21,ou=people,dc=mvp,dc=org
changetype: modificar
replace: userPassword
userPassword: usuario*21

dn: uid=usuario22,ou=people,dc=mvp,dc=org
changetype: modificar
replace: userPassword
userPassword: usuario*22

dn: uid=usuario23,ou=people,dc=mvp,dc=org
changetype: modificar
replace: userPassword
userPassword: usuario*23

dn: uid=usuario24,ou=people,dc=mvp,dc=org
changetype: modificar
replace: userPassword
userPassword: usuario*24
```

Al ejecutar el comando `ldapmodify` con el archivo LDIF se cambiarán las contraseñas en una operación.

```
/usr/bin/ldapmodify –c –H ldap://127.0.0.1:389 –D 'cn=admin,dc=mvp,dc=org' –w vmware –
f /home/tcserver/changeuserpwds.ldif
```

Uso de otros comandos OpenLDAP

Puede utilizar comandos OpenLDAP estándar con el servicio OpenLDAP incrustado.

Cómo determinar las versiones de sus componentes de Horizon Mobile 10

Al abrir una solicitud de asistencia, los datos de versión, compilación y números de modelo de los componentes clave de su entorno de Horizon Mobile resultan de utilidad para ayudar a diagnosticar la fuente de un problema.

Los componentes principales de un entorno de Horizon Mobile son los siguientes:

- Dispositivo móvil VMware Ready
- Componente VMware Ready
- Aplicación VMware Switch
- Imagen base del área de trabajo
- Aplicación virtual VMware Horizon Mobile Manager

Cada componente tiene un identificador propio.

Tabla 10-1. Identificadores de los componentes de Horizon Mobile

Componente	Identificador
Dispositivo móvil	Número de modelo (en el dispositivo móvil)
Componente VMware Ready	Número de versión de software (en el dispositivo móvil)
Componente Vmware Switch	Número de versión de software (en el dispositivo móvil)
Imagen base del área de trabajo	■ Número de versión de software (en el dispositivo móvil) ■ ID de compilación y nombre de imagen (en la interfaz de administración)
Horizon Mobile Manager	Versión de software y número de compilación (en la consola de la instalación virtual y en la interfaz de configuración)

Información de versión en el dispositivo móvil

NOTA: Los pasos para obtener la información de versión pueden ser diferentes dependiendo de su dispositivo móvil específico.

Es posible obtener en el dispositivo móvil el número de modelo del dispositivo y la información de versión de software para los componentes VMware Ready, VMware Switch e imagen base del área de trabajo.

Número de modelo de dispositivo

Obtenga el número de modelo del dispositivo. Normalmente, el número de modelo se encuentra en la información del dispositivo **Acerca del teléfono**.

Versiones de software de VMware Ready, VMware Switch y la imagen base del área de trabajo

Obtenga los números de versión para estos componentes viendo la lista de todas las aplicaciones, localizando VMware Switch en esa lista y abriendo su configuración. Por ejemplo:

1 Abra **Configuración** > **Aplicaciones** > **Todas**.

2 En la lista de todas las aplicaciones, toque **VMware Switch**.

3 Toque **Administrar espacio**. Se mostrará Configuración de Manage VMware Switch.

4 Toque **Diagnósticos**. Aparecerán los números de versión de software de VMware Ready, VMware Switch y del área de trabajo aprovisionada. Si no se ha proporcionado un área de trabajo en el dispositivo, no aparecerá ninguna información de área de trabajo.

Información que se puede obtener en la aplicación virtual Horizon Mobile Manager

Además de la información disponible en el dispositivo móvil en sí, podrá obtener información adicional sobre el área de trabajo que se suministra en un dispositivo móvil de usuario utilizando la interfaz de administración de Horizon Mobile Manager.

1 Inicie sesión en la interfaz de administración como administrador del parque.

2 Abra la página de detalles de usuario haciendo clic en **Usuarios** y, a continuación, haga clic en el nombre del usuario en la lista que aparece.

3 Despliegue la sección **Contenedor de área de trabajo** si aún no lo está. La fila Nombre muestra el nombre de la imagen base del área de trabajo. Tome nota del nombre.

4 Para asociar el nombre con un ID de compilación, vea la lista de imágenes de áreas de trabajo disponibles para esta instancia de Horizon Mobile Manager haciendo clic en **Imágenes de áreas de trabajo**.

5 Haga clic en la entrada de lista que muestra el nombre de la imagen base del área de trabajo. En la ventana Detalles de imagen de área de trabajo, la fila ID de compilación muestra el número de compilación de esa imagen de área de trabajo.

Información acerca de la aplicación virtual Horizon Mobile Manager

Puede ver la información de identificación de su instalación de Horizon Mobile Manager en las siguientes ubicaciones:

Utilizando vSphere Client

Seleccione la aplicación virtual Horizon Mobile Manager y vea su consola haciendo clic en **Consola**. Se mostrarán los números de versión y de compilación de la aplicación virtual Horizon Mobile Manager.

Utilizando la interfaz de configuración

Inicie sesión en la interfaz de configuración como se describe en Capítulo 4, “Adición de claves de licencia,” página 15. La información de versión y compilación se muestra en la pestaña **Sistema**.

Utilizando la interfaz de administración

Inicie sesión en la interfaz de administración como administrador del parque o administrador. Haga clic en **Acerca de** para ver el hash de identificación y la información de ramificación.

Recopile los registros de diagnóstico 11

Cuando abre una solicitud de ayuda, el soporte técnico de VMware puede pedirle los registros de los componentes incrustados de la aplicación virtual. Puede recopilar estos registros y entregarlos en un archivo comprimido junto su solicitud de asistencia.

Puede recopilar los registros para esos componentes incrustados:

- Servidor Apache
- Base de datos de vFabric Postgres
- Sistema operativo Linux

Prerequisitos

En vSphere Client, active la aplicación virtual, haga clic en la pestaña **Consola** e inicie sesión en el sistema operativo Linux de la aplicación virtual como usuario **`raíz`**. Utilice la contraseña que estableció cuando configuró la aplicación virtual. Si no ha cambiado la contraseña predeterminada, introduzca **`vmware`** como contraseña.

Procedimiento

1 Comprima los archivos de registro del servidor Apache:

   a Escriba el comando: `tar czf apachelog1.tgz /home/tcserver/tcserver-current/mmp/logs/`

   b Escriba el comando: `tar czf apachelog2.tgz /home/tcserver/tcserver-current/mmp-config/logs/`

2 Comprima los archivos de registro de la base de datos de vFabric Postgres mediante el comando: `tar czf postgreslog.tgz /opt/vmware/vpostgres/1.0/data/pg_log/`

3 Comprima los archivos de registro del sistema operativo Linux mediante el comando: `tar czf suselog.tgz /var/log/`

Qué hacer a continuación

Copie los archivos comprimidos resultantes (.tgz) a una ubicación desde la cual pueda enviarlos al servicio técnico de VMware.

Índice