Implementación y configuración de Access Point

Unified Access Gateway 2.8

vmware®

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

https://docs.vmware.com/es/

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

Implementar y configurar VMware Access Point 5

1 Preparar la implementación de Access Point 6
- Access Point como puerta de enlace segura 6
- Utilizar Access Point en vez de una red privada virtual 7
- Requisitos de red y del sistema de Access Point 8
- Reglas del firewall para dispositivos de Access Point basados en DMZ 10
- Access Point Topologías de equilibrio de carga 11
- Diseño de la DMZ para Access Point con varias tarjetas de interfaz de red 14

2 Implementar dispositivo de Access Point 18
- Utilizar el asistente de plantillas OVF para implementar Access Point 18
  - Propiedades de la implementación de Access Point 19
  - Implementar Access Point mediante el asistente de plantillas OVF 20
- Configurar Access Point en las páginas de configuración del administrador 23
  - Configurar las opciones del sistema de Access Point 24
- Actualizar certificados SSL firmados del servidor 26

3 Utilizar PowerShell para implementar Access Point 27
- Requisitos del sistema para implementar Access Point con PowerShell 27
- Utilizar PowerShell para implementar el dispositivo de Access Point 28

4 Casos prácticos de implementación 31
- Implementación de Access Point con Horizon View y Horizon Air Hybrid-Mode 31
  - Configurar las opciones de Horizon 35
- Implementación de Access Point como proxy inverso 37
  - Configurar proxy inverso para VMware Identity Manager 39
- Implementación de Access Point con AirWatch Tunnel 40
  - Implementación del proxy de túnel para AirWatch 41
  - Implementación de túnel por aplicación con AirWatch 41
  - Configurar el túnel por aplicación y las opciones del proxy en AirWatch 42

5 Configurar Access Point con certificados TLS/SSL 44
- Configurar certificados TLS/SSL para dispositivos de Access Point 44
  - Seleccionar el tipo de certificado correcto 44
  - Convertir archivos de certificado al formato PEM de una línea 46
  - Sustituir el certificado TLS/SSL predeterminado para Access Point 47

Cambiar los protocolos de seguridad y los conjuntos de cifrado que se utilizan para la comunicación TLS o SSL 49

6 Configurar autenticación en la DMZ 50

Configurar certificado o autenticación de tarjeta inteligente en el dispositivo de Access Point 50

Configurar autenticación mediante certificado en Access Point 51

Obtener los certificados de la autoridad de certificación 53

Configurar la autenticación RSA SecurID en Access Point 54

Configurar RADIUS para Access Point 55

Configurar autenticación RADIUS 56

Configurar la autenticación adaptativa RSA en Access Point 58

Configurar la autenticación adaptativa RSA en Access Point 59

Generar metadatos SAML de Access Point 61

Crear un autenticador SAML utilizado por otros proveedores de servicios 62

Copiar metadatos SAML del proveedor de servicios en Access Point 62

7 Solucionar problemas relacionados con la implementación de Access Point 64

Solucionar errores de implementación 64

Recopilar registros del dispositivo de Access Point 66

Habilitar el modo de depuración 67

Implementar y configurar VMware Access Point

Implementación y configuración de Access Point proporciona información sobre el diseño de la implementación de VMware Horizon®, VMware Identity Manager™ y VMware AirWatch® que utiliza VMware Access Point™ para acceso externo seguro a las aplicaciones de su organización. Estas aplicaciones pueden ser de Windows o de software como servicio (SaaS) y escritorios. Esta guía también proporciona instrucciones para implementar dispositivos virtuales de Access Point y cambiar las opciones de configuración tras la implementación.

Público al que se dirige

Esta información está destinada a cualquier usuario que desee implementar y utilizar dispositivos de Access Point. Esta información está elaborada para administradores de sistemas Linux y Windows con experiencia que estén familiarizados con la tecnología de máquinas virtuales y las operaciones de centros de datos.

Preparar la implementación de Access Point

1

Access Point funciona como una puerta de enlace segura para usuarios que deseen acceder a aplicaciones y escritorios remotos desde fuera del firewall corporativo.

Este capítulo cubre los siguientes temas:

- Access Point como puerta de enlace segura
- Utilizar Access Point en vez de una red privada virtual
- Requisitos de red y del sistema de Access Point
- Reglas del firewall para dispositivos de Access Point basados en DMZ
- Access PointTopologías de equilibrio de carga
- Diseño de la DMZ para Access Point con varias tarjetas de interfaz de red

Access Point como puerta de enlace segura

Access Point es un dispositivo de seguridad de capa 7 que normalmente se instala en una zona desmilitarizada (DMZ). Access Point se utiliza para garantizar que el único tráfico que entra al centro de datos corporativo lo hace en nombre de usuarios con autenticación sólida.

Access Point dirige las solicitudes de autenticación al servidor correspondiente y desecha todas las solicitudes sin autenticar. Los usuarios solo pueden acceder a los recursos para los que tengan autorización.

Los dispositivos virtuales de Access Point también garantizan que el tráfico de un usuario autenticado se pueda dirigir solo a recursos de escritorios y aplicaciones para los que el usuario tenga autorización. Este nivel de protección implica la inspección específica de protocolos de escritorio y la coordinación de las direcciones de red y las directivas que pueden cambiar con rapidez, para poder controlar con precisión el acceso.

Los dispositivos de Access Point residen normalmente dentro de una zona desmilitarizada (DMZ) y actúan como un host proxy para conexiones dentro de la red de confianza de la empresa. Este diseño proporciona una capa de seguridad adicional al proteger los escritorios virtuales, los hosts de las aplicaciones y los servidores de la parte pública de Internet.

Access Point Es un dispositivo con seguridad reforzada diseñado específicamente para DMZ. Se han implementado las siguientes opciones de seguridad.

- Revisiones de software y kernel de Linux actualizados
- Compatibilidad con varias NIC para el tráfico de Internet e intranets
- SSH inhabilitado
- Servicios FTP, Teleta, Rlogin o Rsh inhabilitados
- Servicios no deseados inhabilitados

Utilizar Access Point en vez de una red privada virtual

Access Point y las soluciones VPN genéricas son similares ya que ambos garantizan que el tráfico se reenvía a una red interna únicamente en nombre de usuarios con autenticación sólida.

Entre las ventajas de Access Point sobre la VPN se incluyen las siguientes:

- Access Control Manager. Access Point aplica reglas de acceso automáticamente. Access Point reconoce las autorizaciones de los usuarios y las direcciones necesarias para conectarse internamente, que pueden cambiar rápidamente. Una VPN hace lo mismo, ya que la mayoría de las VPN permiten a un administrador configurar las reglas de conexión de red para cada usuario o grupo de usuarios individualmente. Al principio, esto funciona bien con una VPN, pero mantener las reglas necesarias exige un esfuerzo administrativo importante.
- Interfaz de usuario. Access Point no modifica la clara interfaz de usuario de Horizon Client. Con Access Point, cuando Horizon Client se inicia, los usuarios autenticados se encuentran en sus entornos de View y tienen acceso controlado a sus escritorios y aplicaciones. En una VPN, es obligatorio configurar primero el software de la VPN y autenticar por separado antes de iniciar Horizon Client.
- Rendimiento. Access Point está diseñado para maximizar la seguridad y el rendimiento. Con Access Point, PCoIP, HTML Access y los protocolos WebSocket están seguros sin necesidad de encapsulaciones adicionales. Las VPN se implementan como VPN SSL. Esta implementación cumple con creces los requisitos de seguridad y, con TLS habilitado, se consideran seguras, pero el protocolo subyacente de SSL/TLS está basado simplemente en TCP. Los protocolos actuales de vídeo remoto aprovechan los transportes basados en UDP sin conexión, por lo que sus ventajas de rendimiento pueden verse mermadas si deben utilizar un transporte basado en TCP. Esto no se aplica a todas las tecnologías de VPN, ya que las que también funcionan con DTLS o IPsec en lugar de SSL/TLS ofrecen un buen rendimiento con los protocolos de escritorio de View.

Requisitos de red y del sistema de Access Point

Para implementar el dispositivo de Access Point, su sistema debe cumplir los requisitos de hardware y software.

Versiones compatibles de productos de VMware

Debe utilizar versiones específicas de los productos de VMware con versiones concretas de Access Point. Consulte las notas de la versión del producto si desea ver la información más reciente sobre compatibilidad, así como la sección Matrices de interoperabilidad de productos de VMware en la página http://www.vmware.com/resources/compatibility/sim/interop_matrix.php. La información incluida en las notas de la versión y la matriz de interoperabilidad sustituyen a la información de esta guía.

Access Point 2.8 se puede utilizar como una puerta de enlace segura con las siguientes opciones de VMware:

- VMware AirWatch 8.4 y versiones posteriores
- VMware Identity Manager 2.7 y versiones posteriores
- VMware Horizon 6.2 y versiones posteriores
- VMware Horizon Air Hybrid Mode 1.0 y versiones posteriores
- VMware Horizon Air 15.3 y versiones posteriores

Requisitos de hardware del servidor ESXi

El dispositivo de Access Point se debe implementar en una versión de vSphere que sea compatible con los productos de Horizon y las versiones que usted esté utilizando.

Si tiene previsto utilizar vSphere Web Client, verifique que el complemento de integración de clientes esté instalado. Para obtener más información, consulte la documentación de vSphere. Si no instala este complemento antes de iniciar el asistente de implementación, este le indicará que lo haga. Para ello, deberá cerrar el navegador y salir del asistente.

NOTA: Configure el reloj (UTC) en el dispositivo de Access Point para que tenga la hora correcta. Por ejemplo, abra una ventana de la consola en la máquina virtual de Access Point y seleccione la zona horaria correcta con la ayuda de los botones de flecha. Compruebe también que la hora del host ESXi esté sincronizada con el servidor NTP y que VMware Tools, que se está ejecutando en la máquina virtual del dispositivo, sincronice la hora de la máquina virtual con la hora del ihost ESX.

Requisitos del dispositivo virtual

El paquete de OVF para el dispositivo de Access Point selecciona automáticamente la configuración de la máquina virtual que Access Point necesita. Aunque esta configuración se puede cambiar, VMware recomienda no cambiar los valores de espacio en disco, memoria o CPU a valores inferiores a los predeterminados de OVF.

Verifique que el almacén de datos que utiliza para el dispositivo tenga suficiente espacio en disco y cumpla los demás requisitos del sistema.

- El tamaño de descarga del dispositivo virtual es 2,5 GB
- El requisito mínimo de disco de aprovisionamiento fino es 2,5 GB
- El requisito mínimo de disco de aprovisionamiento grueso es 20 GB

La siguiente información es necesaria para implementar el dispositivo virtual

- Dirección IP estática
- Dirección IP del servidor DNS
- Contraseña para el usuario raíz
- URL de la instancia del servidor del equilibrador de carga al que el dispositivo de Access Point se dirige

Requisitos de configuración de red

Puede utilizar una, dos o tres interfaces de red. Access Point necesitará una dirección IP estática para cada una de ellas. Muchas implementaciones de DMZ utilizan redes diferentes para asegurar los distintos tipos de tráfico. Configure Access Point en función del diseño de red de la DMZ en la que se implementó.

- Las interfaces de red son adecuadas para las POC (pruebas de concepto) de las pruebas. Con una NIC, el tráfico de administración, el interno y el externo fluyen todos por la misma subred.
- Con dos interfaces de red, el tráfico externo fluye por una subred y el tráfico de administración e interno fluye por otra.
- La opción más segura es utilizar tres interfaces de red. Con una tercera NIC, el tráfico de administración, el interno y el externo tendrán cada uno su propia subred.

IMPORTANTE: Compruebe que asignó un grupo de IP a cada red. El dispositivo de Access Point podrá entonces obtener la configuración de la puerta de enlace y la máscara de subred en el momento de la implementación. Para agregar un grupo de IP en vCenter Server, si está utilizando vSphere Client nativo, vaya a la pestaña **Grupos de IP** del centro de datos. Si está utilizando vSphere Web Client, también puede crear un perfil de protocolo de red. Vaya a la pestaña **Administrar** y seleccione la pestaña **Perfiles de protocolos de red**. Si desea obtener más información, consulte la sección Configuración de perfiles de protocolos para redes de máquinas virtuales.

Requisitos de retención de registro

Los archivos de registro se configuran de forma predeterminada para que ocupen menos espacio que el que ocupa el disco en su totalidad. Los registros de Access Point van rotando de forma predeterminada. Syslog permite conservar estas entradas de registro. Consulte Recopilar registros del dispositivo de Access Point.

Reglas del firewall para dispositivos de Access Point basados en DMZ

Los dispositivos de Access Point basados en DMZ requieren la configuración de ciertas reglas del firewall en los firewall del front-end y el back-end. Durante la instalación, se configuran los servicios de Access Point para la escucha en determinados puertos de la red predeterminados.

La implementación de un dispositivo de Access Point basado en DMZ incluye normalmente dos firewall.

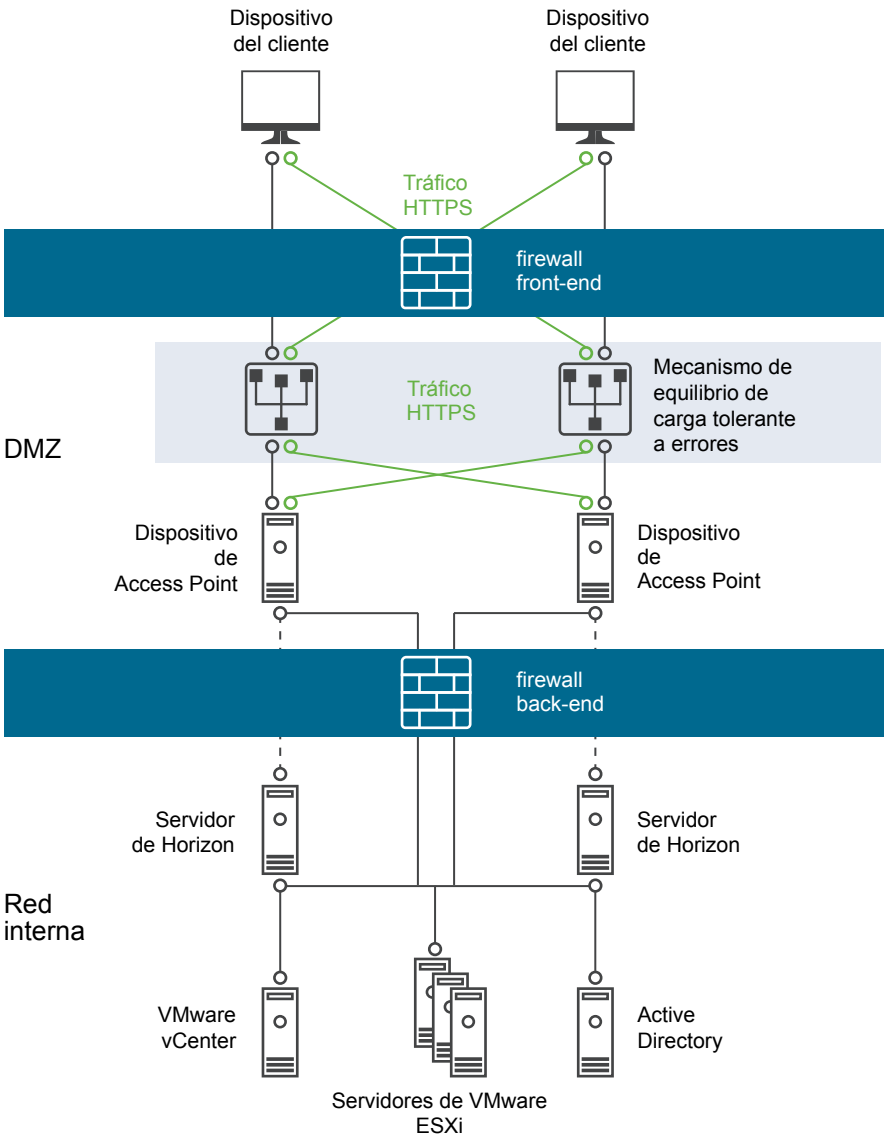
- Se necesita un firewall de front-end dirigido a la red externa, que protege tanto la DMZ como la red interna. Este firewall se configura para permitir que el tráfico de la red externa llegue a la DMZ.
- Se necesita un firewall de back-end entre la DMZ y la red interna, que proporciona un segundo nivel de seguridad. Este firewall se configura para aceptar solo el tráfico que se origina desde los servicios dentro de la DMZ.

La directiva del firewall controla estrictamente las comunicaciones entrantes de los servicios de la DMZ, lo que reduce en gran medida los riesgos para la red interna.

Para permitir que los dispositivos de clientes externos se conecten a un dispositivo de Access Point dentro de la DMZ, el firewall de front-end debe permitir el tráfico en determinados puertos. De forma predeterminada, los dispositivos de clientes externos y los clientes web externos (HTML Access) se conectan a un dispositivo de Access Point dentro de la DMZ sobre TCP, puerto 443. Si utiliza el protocolo Blast, el puerto 443 debe estar abierto en el firewall. Si utiliza el protocolo PCOIP, el puerto 4172 debe estar abierto en el firewall.

La figura siguiente muestra un ejemplo de configuración que incluye firewall de front-end y de back-end.

Figura 1-1. Topología de doble firewall



Access Point Topologías de equilibrio de carga

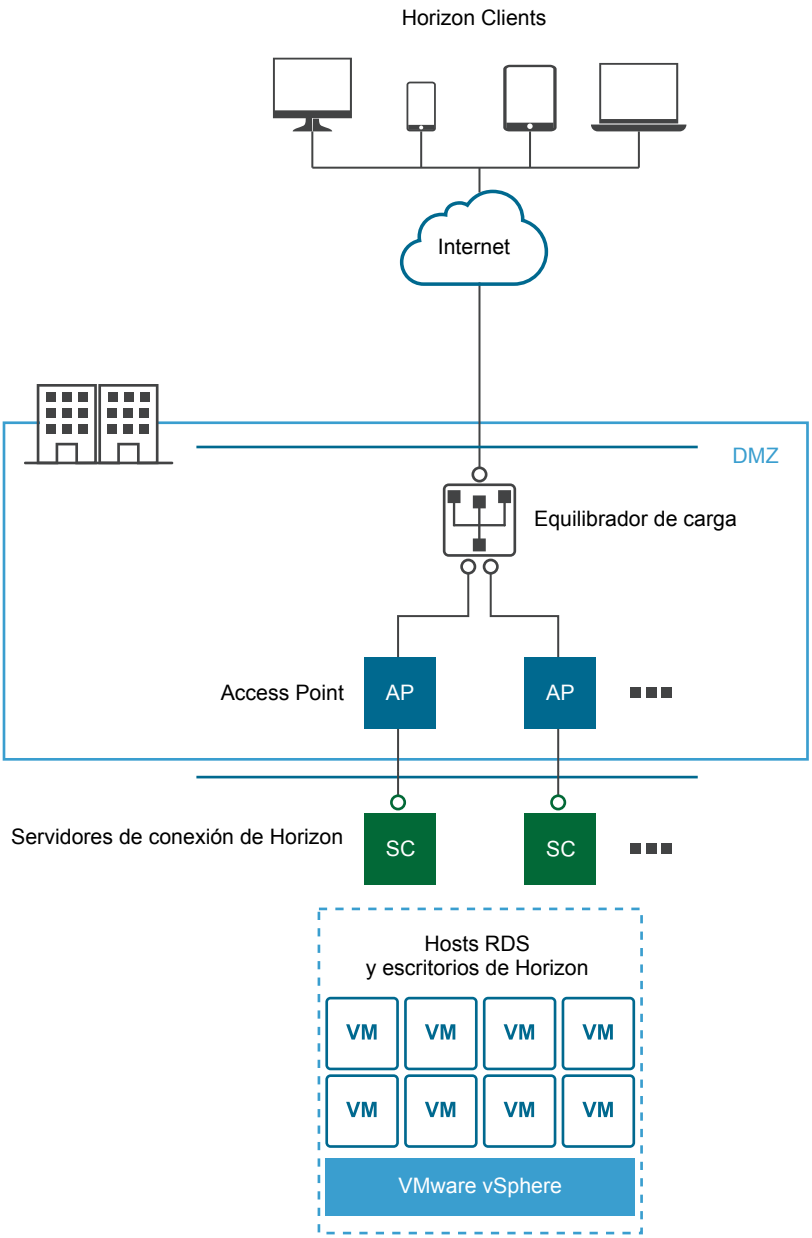
Puede implementar cualquiera de las muchas topologías distintas.

Los dispositivos de Access Point de la DMZ se pueden configurar para que se dirijan a un servidor o a un equilibrador de carga que lidere un grupo de servidores. Los dispositivos de Access Point funcionan con soluciones estándar de equilibrio de carga externas que se configuran para HTTPS.

Si el dispositivo de Access Point se dirige a un equilibrador de carga que lidera a los servidores, la selección de la instancia del servidor será dinámica. Por ejemplo, es posible que el equilibrador de carga realice una selección en función de la disponibilidad y del conocimiento que tenga con respecto al número de sesiones en curso de cada instancia del servidor. Las instancias del servidor incluidas en el firewall corporativo suelen tener un equilibrador de carga para permitir el acceso interno. Con Access Point podrá dirigir el dispositivo de Access Point al mismo equilibrador de carga que generalmente se está utilizando.

También es posible que uno o varios dispositivos de Access Point se dirijan a una instancia individual del servidor. En ambos casos, utilice un equilibrador de carga que lidere a dos o más dispositivos de Access Point en la DMZ.

Figura 1-2. Varios dispositivos de Access Point detrás de un equilibrador de carga



Protocolos de Horizon

Cuando un usuario de Horizon Client se conecta a un entorno de Horizon, se utilizan varios protocolos distintos. La primera conexión es siempre el protocolo principal XML-API sobre HTTPS. Si la autenticación es correcta, también se utilizan uno o varios protocolos secundarios.

- Protocolo principal de Horizon

  El usuario introduce un nombre de host en Horizon Client y con esto se inicia el protocolo principal de Horizon. Se trata de un protocolo de control para autorización de autenticación y administración de sesión. Utiliza mensajes XML estructurados sobre HTTPS (HTTP sobre SSL). Este protocolo se conoce en ocasiones como el protocolo de control XML-API de Horizon. En un entorno con equilibrado de carga, tal y como se muestra más arriba en la figura Varios dispositivos de Access Point detrás de un equilibrador de carga, el equilibrador de carga dirige esta conexión a uno de los dispositivos de Access Point. El equilibrador de carga suele seleccionar el dispositivo en primer lugar, basándose en la disponibilidad y, a continuación, entre los dispositivos disponibles, dirige el tráfico en función del menor número de sesiones existentes. Esta configuración distribuye uniformemente el tráfico de los distintos clientes entre el conjunto de dispositivos disponibles de Access Point

- Protocolos secundarios de Horizon

  Una vez que Horizon Client establece una comunicación segura con uno de los dispositivos de Access Point, el usuario se autentica. Si este intento de autenticación no falla, se realizan una o varias conexiones secundarias desde Horizon Client. Estas conexiones secundarias pueden incluir lo siguiente:

  - Túnel HTTPS utilizado para encapsular protocolos TCP como RDP, MMR/CDR y el canal de marco de cliente. (TCP 443).
  - Protocolo de visualización Blast Extreme (TCP 443 y UDP 443).
  - Protocolo de visualización PCoIP (TCP 4172 y UDP 4172).

Estos protocolos secundarios de Horizon se deben dirigir al mismo dispositivo de Access Point al que se dirigió el protocolo principal de Horizon. Access Point podrá entonces autorizar los protocolos secundarios en función de la sesión del usuario autenticado. Una característica importante de seguridad de Access Point es que solo reenvía el tráfico al centro de datos corporativo si el tráfico se dirige en nombre de un usuario autenticado. Si los protocolos secundarios se dirigen de forma incorrecta a un dispositivo de Access Point distinto al dispositivo del protocolo principal, no estarán autorizados y se enviarán a la DMZ. Se producirá un error de conexión. Un problema frecuente es que los protocolos secundarios se dirigen de forma incorrecta si el equilibrador de carga no está configurado correctamente.

Diseño de la DMZ para Access Point con varias tarjetas de interfaz de red

Access Point es un dispositivo de seguridad de capa 7 que normalmente se instala en una zona desmilitarizada (DMZ). Access Point se utiliza para garantizar que el único tráfico que entra al centro de datos corporativo lo hace en nombre de usuarios con autenticación sólida.

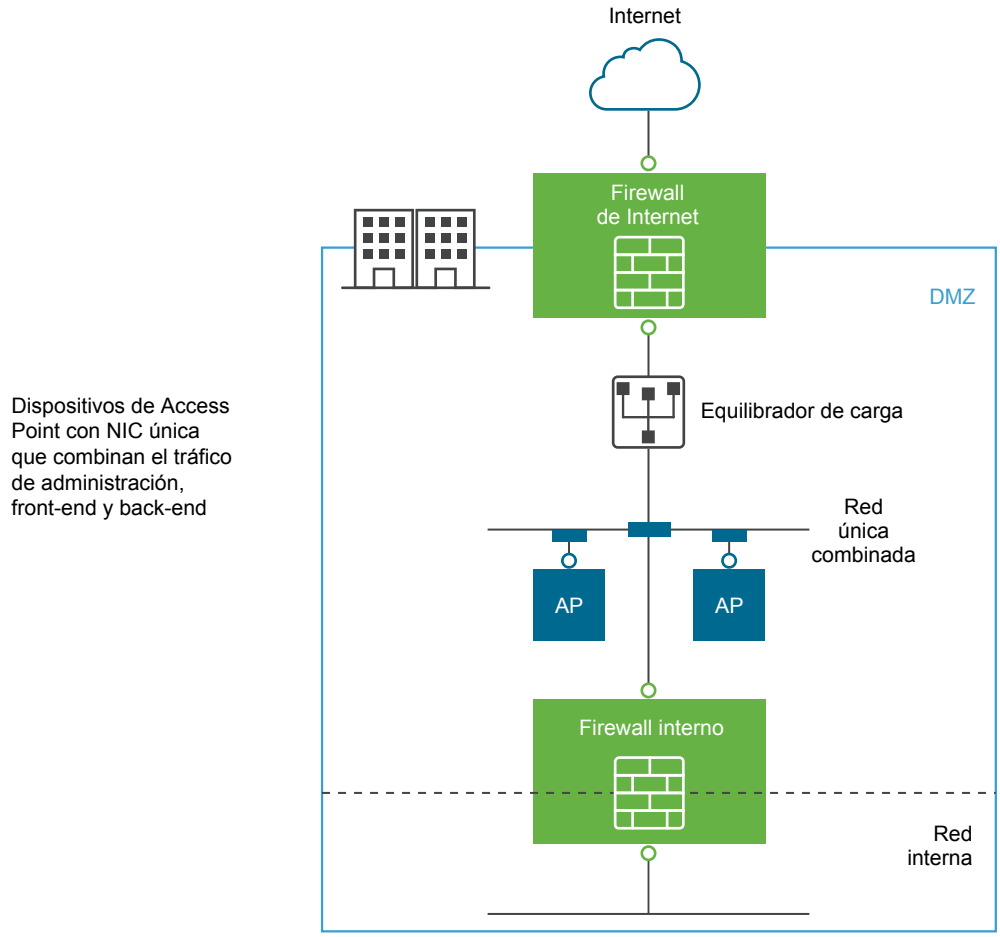
Una de las opciones de configuración de Access Point es el número de tarjetas de interfaz de red virtual (NIC) que se van a utilizar. Al implementar Access Point, se selecciona la configuración de implementación para la red. Puede especificar una configuración de una, dos o tres NIC, que se especifica como onenic, twonic o threenic.

Si se reduce el número de puertos abiertos en cada LAN virtual y se separan los distintos tipos de tráfico de red, la seguridad puede mejorar significativamente. Las ventajas se traducen principalmente en términos de separación y aislamiento de los distintos tipos de tráfico de red como parte de una estrategia de diseño de seguridad extrema de la DMZ. Para conseguirlo, debe implementar distintos conmutadores físicos dentro de la DMZ con varias LAN virtuales dentro de la AMZ o como parte de una DMZ completamente administrada por VMware NSX.

Implementación típica de DMZ con una sola NIC

La implementación más sencilla de Access Point es la que tiene una sola NIC en la que todo el tráfico de la red se junta en una sola red. El tráfico del firewall orientado a Internet se dirige a uno de los dispositivos disponibles de Access Point. A continuación, Access Point redirige el tráfico autorizado a través del firewall interno hacia los recursos de la red interna. Access Point desecha el tráfico no autorizado.

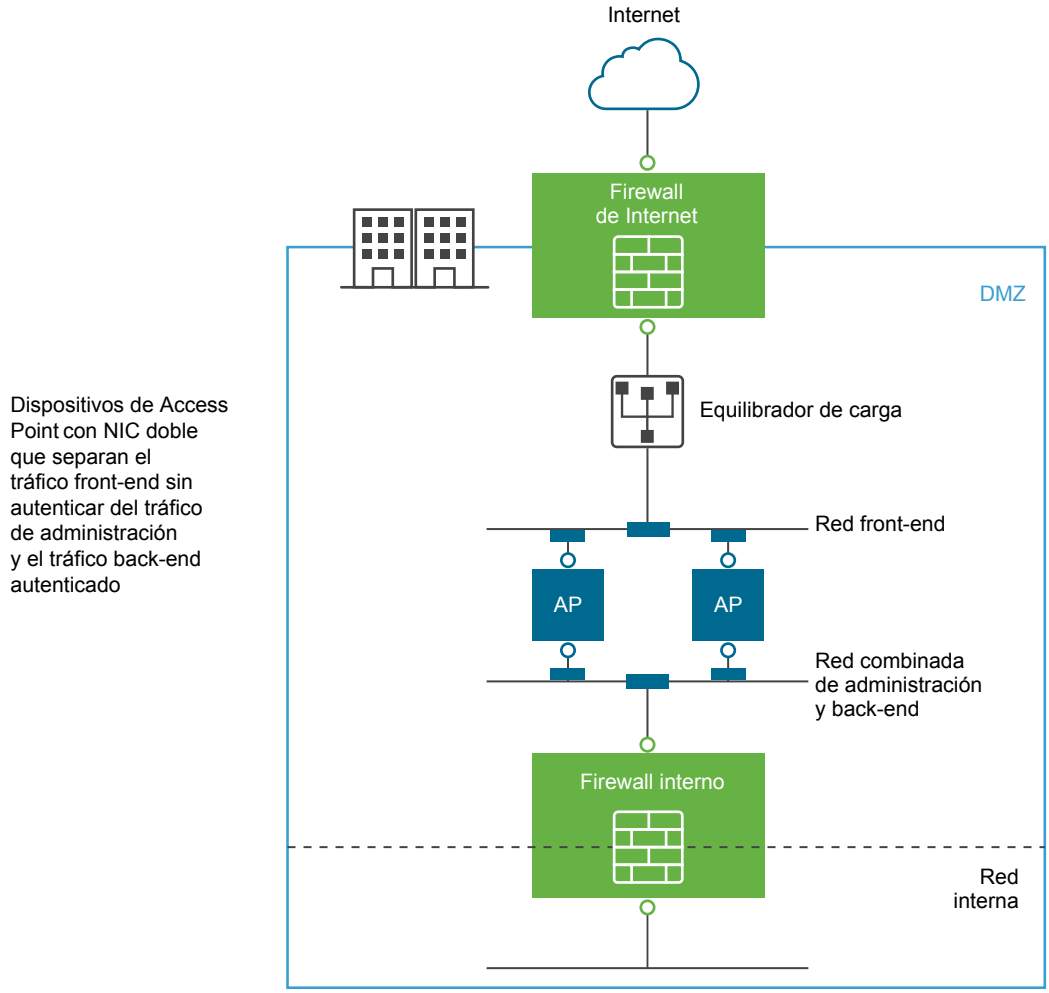
Figura 1-3. Opción de una sola NIC de Access Point



Separar el tráfico del usuario sin autenticar del tráfico de administración y back-end

Una mejora sobre la implementación de una sola NIC es especificar dos NIC. La primera se sigue utilizando para acceso sin autenticar orientado a Internet, pero el tráfico autenticado back-end y el tráfico de administración se derivan a otra red.

Figura 1-4. Opción de dos NIC de Access Point



En una implementación de dos NIC, el tráfico que se dirige a la red interna a través de un firewall interno debe tener autorización de Access Point. El tráfico no autorizado no se encuentra en esta red back-end. El tráfico de administración como la API de REST para Access Point solo se encuentra en esta segunda red

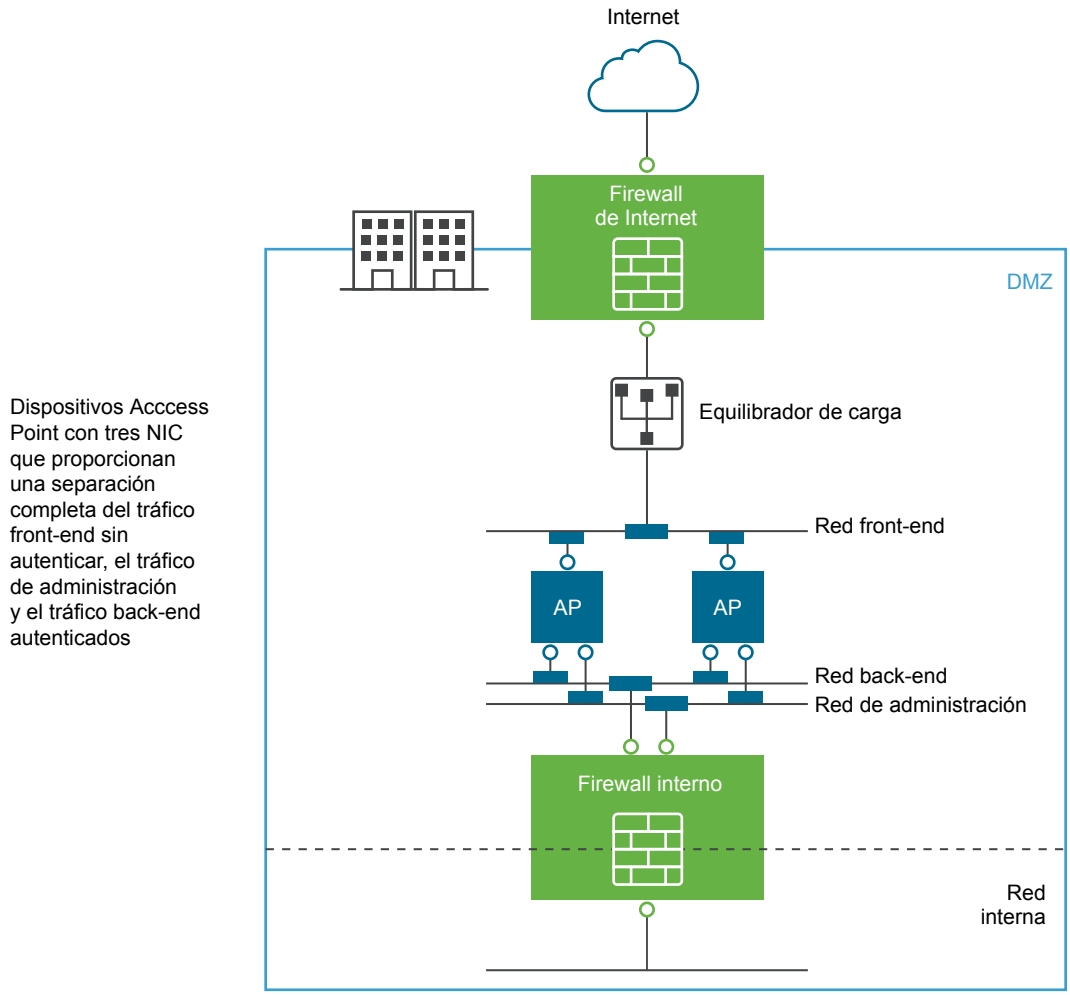
Si un dispositivo de una red front-end sin autenticar se pone en peligro, por ejemplo, el equilibrador de carga, en esta implementación de dos NIC no será posible volver a configurar dicho dispositivo para desviar Access Point. Combina reglas de firewall de capa 4 con seguridad de Access Point de capa 7. De forma similar, si el firewall orientado a Internet se configuró erróneamente para admitir el puerto TCP 9443, la API de REST de administración de Access Point seguiría sin exponerse a los usuarios de Internet. Un principio de seguridad máxima utiliza varios niveles de protección, entre ellos, saber que un solo error de configuración o un ataque al sistema no crea necesariamente una vulnerabilidad general

En una implementación de dos NIC, es habitual poner sistemas de infraestructura adicionales tales como servidores DNS, servidores del administrador de autenticación RSA SecurID en la red back-end dentro de la DMZ para que estos servidores no puedan estar visibles en la red orientada a Internet. Al poner sistemas de infraestructura dentro de la DMZ, se crea una protección contra los ataques de capa 2 procedentes de la LAN orientada a Internet desde un sistema front-end y se reduce de forma eficaz la superficie general de ataque.

La mayor parte del tráfico de red de Access Point se compone de los protocolos de visualización para Blast y PCoIP. Con un solo NIC, el tráfico del protocolo de visualización hacia y desde Internet se combina con el tráfico hacia y desde los sistemas back-end. Si se utilizan dos o más NIC, el tráfico se distribuye entre las redes y las NIC front-end y back-end. De esta forma se reduce el cuello de botella de una sola NIC y se generan ventajas de rendimiento.

Access Point admite una separación mayor al permitir también la separación del tráfico de administración en una LAN de administración específica. El tráfico de administración HTTPS dirigido al puerto 9443 será entonces solo posible si procede de la LAN de administración.

Figura 1-5. Opción de tres NIC de Access Point



Implementar dispositivo de Access Point 2

Access Point se empaqueta como OVF y se implementa en un vSphere ESX o un host ESXi como un dispositivo virtual previamente configurado.

Para instalar el dispositivo de Access Point se pueden utilizar dos métodos principales.

- Se pueden utilizar vSphere Client o vSphere Web Client para implementar la plantilla de OVF de Access Point. Se le pedirá la configuración básica, incluida la configuración de implementación de la NIC, la dirección IP y las contraseñas de la interfaz de administración. Tras la implementación de OVF, inicie sesión en la interfaz de usuario del administrador de Access Point para configurar las opciones del sistema de Access Point, configurar los servicios perimetrales en varios casos prácticos y configurar la autenticación en la DMZ. Consulte Implementar Access Point mediante el asistente de plantillas OVF.
- Se pueden utilizar los scripts de PowerShell para implementar Access Point y configurar los servicios perimetrales seguros en varios casos prácticos. Debe descargar el archivo zip, configurar el script de PowerShell para su entorno y ejecutar el script para implementar Access Point. Consulte Utilizar PowerShell para implementar el dispositivo de Access Point.

Este capítulo cubre los siguientes temas:

- Utilizar el asistente de plantillas OVF para implementar Access Point
- Configurar Access Point en las páginas de configuración del administrador
- Actualizar certificados SSL firmados del servidor

Utilizar el asistente de plantillas OVF para implementar Access Point

Para implementar Access Point, debe implementar la plantilla OVF mediante vSphere Client o vSphere Web Client, encender el dispositivo y configurar las opciones.

Una vez que Access Point esté implementado, en la interfaz de usuario (IU) deberá configurar el entorno de Access Point, los recursos de escritorios y aplicaciones y los métodos de autenticación que se van a utilizar en la DMZ.

Propiedades de la implementación de Access Point

Cuando se implementa OVF, se establece el número de interfaces de red (NIC) necesarias, la dirección IP y la contraseña del administrador. El resto de las propiedades de implementación se pueden configurar en las páginas de administración de Access Point.

Tabla 2-1. Opciones de implementación Access Point

Propiedad de implementación	Descripción
Configuración de implementación	Especifica cuántas interfaces de red están disponibles en la máquina virtual de Access Point. De forma predeterminada, esta propiedad no se configura, por lo que se utiliza una controladora de interfaz de red (NIC).
Dirección IP externa (con conexión a Internet)	(Obligatorio) Especifica las direcciones IPv6 o IPv4 públicas utilizadas para acceder a esta máquina virtual en Internet. **NOTA:** El nombre del equipo se configura a través de una consulta de DNS de esta dirección IPv4 o IPv6 de Internet. Valor predeterminado: ninguno.
Dirección IP de red de administración	Especifica la dirección IP de la interfaz que está conectada a la red de administración. Si no está configurada, el servidor de administración realiza la escucha en la interfaz con conexión a Internet. Valor predeterminado: ninguno.
Dirección IP de red back-end	Especifica la dirección IP de la interfaz que está conectada a la red back-end. Si no está configurada, el tráfico de la red enviado a los sistemas back-end se dirige a través de otras interfaces de red. Valor predeterminado: ninguno.
Direcciones de servidor DNS	(Obligatorio) Especifica una o varias direcciones IPv4 separadas por espacios de los servidores de nombres de dominio para esta máquina virtual (por ejemplo: 192.0.2.1 192.0.2.2). Puede especificar hasta tres servidores. De forma predeterminada, esta propiedad no se configura, por lo que el sistema utiliza el servidor DNS que está asociado a la NIC con conexión a Internet. **ADVERTENCIA:** Si se deja esta opción en blanco y no hay ningún servidor DNS asociado a la NIC con conexión a Internet, el dispositivo no se implementará correctamente.
Contraseña para el usuario raíz	(Obligatorio) Especifica la contraseña para el usuario root de esta máquina virtual. La contraseña debe ser una contraseña válida de Linux. Valor predeterminado: ninguno.
Contraseña para el usuario admin	(Obligatorio) Si no configura esta contraseña, no podrá acceder a la consola de administración ni a la API de REST en el dispositivo de Access Point. La contraseña debe tener al menos 8 caracteres, una mayúscula, una minúscula, un dígito y un carácter especial, entre los que se incluyen el signo ! @ # $ % * ( ). Valor predeterminado: ninguno.

Tabla 2-1. Opciones de implementación Access Point (Continua)

Propiedad de implementación	Descripción
Idioma que se va a utilizar en los mensajes localizados	(Obligatorio) Especifica el idioma que se va a utilizar al generar mensajes de error. ■ **en_US** para inglés ■ **ja_JP** para japonés ■ **fr_FR** para francés ■ **de_DE** para alemán ■ **zh_CN** para chino simplificado ■ **zh_TW** para chino tradicional ■ **ko_KR** para coreano Valor predeterminado: en_US.
URL del servidor de registro del sistema	Especifica el servidor de registro del sistema que se utiliza para registrar eventos de Access Point. Este valor puede ser una URL, un nombre de host o una dirección IP. El esquema y el número de puerto son opcionales (por ejemplo: syslog://server.example.com:514). De forma predeterminada, esta propiedad no está configurada, por lo que no se registra ningún evento en el servidor de registro del sistema.

Implementar Access Point mediante el asistente de plantillas OVF

Para implementar el dispositivo de Access Point, puede iniciar la sesión en vCenter Server y utilizar el asistente para Implementar plantilla OVF.

NOTA: Si se utiliza vSphere Web Client para implementar OVF, también se pueden especificar las direcciones de máscara de red, la puerta de enlace y el servidor DNS de cada red. Si se utiliza el cliente nativo vSphere Client, verifique que se asignó un grupo de IP a cada red. Para agregar un grupo de IP en vCenter Server mediante vSphere Client nativo, vaya a la pestaña Grupos de IP del centro de datos. Si está utilizando vSphere Web Client, también puede crear un perfil de protocolo de red. Vaya a la pestaña Administrar y seleccione la pestaña Perfiles de protocolos de red.

Prerequisitos

- Familiarícese con las opciones de implementación disponibles en el asistente. Consulte Requisitos de red y del sistema de Access Point.
- Determine el número de interfaces de red y direcciones IP estáticas que se deben configurar para el dispositivo de Access Point. Consulte Requisitos de configuración de red.
- Descargue el archivo del instalador `.ova` para el dispositivo de Access Point desde el sitio web de VMware en la dirección https://my.vmware.com/web/vmware/downloads, o determine la URL que se utilizará (por ejemplo: `http://ejemplo.com/vapps/euc-access-point-`*`Y.Y`*`.0.0-`*`xxxxxxx`*`_OVF10.ova`), donde *Y.Y* es el número de versión y *xxxxxxx* el de compilación.

Procedimiento

1 Utilice el cliente nativo vSphere Client o vSphere Web Client para iniciar la sesión en una instancia de vCenter Server.

Para una red IPv4, use vSphere Web Client o el vSphere Client nativo. Para una red IPv6, use vSphere Web Client.

2 Seleccione un comando de menú para iniciar el asistente de implementación de plantillas OVF.

Opción	Comando de menú
vSphere Client	Seleccione **Archivo > Implementar plantilla OVF**.
vSphere Web Client	Seleccione cualquier objeto de inventario que sea un objeto padre válido de una máquina virtual, como un centro de datos, una carpeta, un clúster, un grupo de recursos o un host, y en el menú **Acciones** seleccione **Implementar plantilla OVF**.

3 En la página de selección de origen del asistente, navegue a la ubicación del archivo `.ova` que descargó o introduzca una URL y haga clic en **Siguiente**.

Se abrirá una página de detalles. Revise los detalles, la versión y los requisitos de tamaño del producto.

4 Siga las indicaciones del asistente y tenga en cuenta las siguientes directrices al completar los pasos del asistente.

Opción	Descripción
Seleccione una configuración de implementación	Para una red IPv4, puede usar una, dos o tres interfaces de red (NIC). Para una red IPv6, use tres NIC. Access Point necesita una dirección IP estática independiente para cada NIC. Muchas implementaciones de DMZ utilizan redes diferentes para asegurar los distintos tipos de tráfico. Configure Access Point en función del diseño de red de la DMZ en la que se implementó.
Formato del disco	En entornos de evaluación y pruebas, seleccione el formato Aprovisionamiento delgado. En entornos de producción, seleccione uno de los formatos de Aprovisionamiento grueso. Thick Provision Eager Zeroed es un tipo de formato de disco virtual compatible con funciones de clúster como la tolerancia a fallos, pero se tarda mucho más en crear que otros tipos de discos virtuales.
Directiva de almacenamiento de VM	(Solo para vSphere Web Client) Esta opción está disponible si las directivas de almacenamiento están habilitadas en el recurso de destino.

Opción	Descripción
Configuración de redes/Asignación de red	Si se utiliza vSphere Web Client, la página Configuración de redes permite asignar cada NIC a una red y especificar la configuración de protocolos. a Seleccione IPv4 o IPv6 en la lista desplegable **Protocolo IP**. b Seleccione la primera fila de la tabla **Internet** y, a continuación, haga clic en la flecha abajo para seleccionar la red de destino. Si selecciona IPv6 como el protocolo IP, debe seleccionar la red que tenga capacidades IPv6. Después de seleccionar la fila, podrá introducir también las direcciones IP del servidor DNS, la puerta de enlace y la máscara de red en la parte inferior de la ventana. c Si utiliza más de una NIC, seleccione la fila siguiente **ManagementNetwork**, seleccione la red de destino y, a continuación, podrá introducir las direcciones IP del servidor DNS, la puerta de enlace y la máscara de red de esa red. Si solo utiliza una NIC, todas las filas se asignarán a la misma red. d Si dispone de una tercera NIC, seleccione también la tercera fila y complete los ajustes. Si solo utiliza dos NIC, en esta tercera fila **BackendNetwork**, seleccione la misma red utilizada para **ManagementNetwork**. Con vSphere Web Client, después de completar los pasos del asistente se crea automáticamente un perfil de protocolo de red, si no existe ninguno. Si utiliza el cliente nativo vSphere Client (en lugar de Web Client), la página de asignación de red le permite asignar cada NIC a una red, pero no hay campos para especificar las direcciones del servidor DNS, la puerta de enlace y la máscara de red. Como se describe en los requisitos previos, ya se debe haber asignado un grupo de IP a cada red o creado un perfil de protocolo de red.
Personalizar la plantilla Propiedades	Los cuadros de texto de la página Propiedades son específicos de Access Point y puede que no sean necesarios para otros tipos de dispositivos virtuales. El texto de la página del asistente explica el uso de cada ajuste. Si el texto aparece recortado en la parte derecha del asistente, redimensione la ventana arrastrando desde la esquina inferior izquierda. Debe introducir valores en los siguientes cuadros de texto: ■ **IPMode:STATICV4/STATICV6**. Si introduce STATICV4, debe introducir la dirección IPv4 para la NIC. Si introduce STATICV6, debe introducir la dirección IPv6 para la NIC. ■ **Lista de reglas de reenvío separadas por comas con el formato {tcp|udp}/listening-port-number/destination-ip-address:destination-port-nu** ■ **Dirección IPv4 para la NIC 1 (ETH0)**. Introduzca la dirección IPv4 para la NIC si introdujo STATICV4 como modo de NIC. ■ **Lista de rutas personalizadas de IPv4 separadas por comas para la NIC 1 (eth0) con el formato ipv4-network-address/bits.ipv4-gateway-address** ■ **dirección IPv6**. Introduzca la dirección IPv6 para la NIC si introdujo STATICV6 como modo de NIC. ■ **Direcciones de servidor DNS**. Introduzca las direcciones IPv4 o IPv6 de los servidores de nombre de dominio para la máquina virtual. ■ **Dirección IP de red de administración** si especificó 2 NIC y **Dirección IP de red back-end** si especificó 3 ■ **Opciones de contraseña**. Introduzca la contraseña del usuario raíz de esta máquina virtual y la del usuario administrador que accede a la consola de administración y habilita el acceso de API de REST.

Opción	Descripción
	El resto de valores son opcionales o ya tienen introducido un valor predeterminado. Tenga en cuenta los requisitos de contraseña indicados en la página del asistente. Para obtener una descripción de las propiedades de la implementación, consulte Propiedades de la implementación de Access Point.

5 En la página Listo para completar, seleccione **Encender después de la implementación** y haga clic en **Finalizar**.

En el área de estado de vCenter Server, aparecerá una tarea de implementar plantilla OVF que permite supervisar la implementación. También se puede abrir una consola en la máquina virtual para ver los mensajes de la consola que se muestran durante el arranque del sistema. También hay disponible un registro de esos mensajes en el archivo `/var/log/boot.msg`.

6 Después de completar la implementación, verifique que los usuarios finales se puedan conectar al dispositivo. Para ello, abra una ventana del navegador e introduzca la URL siguiente:

```
https://FQDN-of-AP-appliance
```

En esta URL, *FQDN-of-AP-appliance* es el nombre de dominio plenamente cualificado, que el servidor DNS puede resolver, del dispositivo de Access Point.

Si la implementación se realizó correctamente, aparecerá la página web proporcionada por el servidor al que Access Point se dirige. Si la implementación no se realizó correctamente, se puede borrar la máquina virtual del dispositivo y volver a implementar el dispositivo. El error más habitual es no introducir correctamente las huellas del certificado.

El dispositivo de Access Point se implementa e inicia automáticamente.

Qué hacer a continuación

Inicie sesión en la interfaz de usuario (UI) del administrador de Access Point y configure los recursos de escritorios y aplicaciones para permitir el acceso remoto desde Internet a través de Access Point y los métodos de autenticación que se van a utilizar en la DMZ. La URL de la consola de administración tiene el formato `https://<mycoAccessPointappliance.com:9443/admin/index.html`.

Configurar Access Point en las páginas de configuración del administrador

Una vez que OVF esté implementado y el dispositivo de Access Point encendido, inicie sesión en la interfaz de usuario del administrador de Access Point para configurar las opciones siguientes.

- Configuración del sistema de Access Point y certificado de servidor SSL.
- Configuración del servicio perimetral para Horizon, proxy inverso, túnel por aplicación y configuración de proxy para AirWatch.
- Configuración de autenticación para RSA SecurID, RADIUS, certificado X.509 y autenticación adaptativa RSA.

- Configuración de proveedor de servicios y proveedor de identidades de SAML.

Se puede acceder a las siguientes opciones desde las páginas de configuración.

- Descargar archivos zip de Access Point.
- Exportar la configuración de Access Point para recuperar las opciones de configuración.
- Importar la configuración de Access Point para crear y actualizar una configuración completa de Access Point.

Configurar las opciones del sistema de Access Point

En las páginas de configuración del administrador puede configurar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar las comunicaciones entre los clientes y el dispositivo de Access Point.

La URL de la interfaz del usuario administrador de Access Point tiene el formato `https://<mycoAccessPointappliance.com>:9443/admin/index.html`. Para iniciar sesión, introduzca el nombre y la contraseña del usuario administrador que configuró al implementar el OVF.

Prerequisitos

- Revisar las propiedades de implementación de Access Point. La siguiente información es necesaria
  - Dirección IP estática para el dispositivo de Access Point
  - Dirección IP del servidor DNS
  - Contraseña de la consola de administración
  - URL de la instancia del servidor o el equilibrador de carga al que el dispositivo de Access Point se dirige
  - URL del servidor syslog para guardar los archivos de registro de eventos

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la sección Configuración avanzada, haga clic en el icono de engranaje de **Configuración del sistema**.

3 Edite los siguientes valores de la configuración del dispositivo de Access Point.

Opción	Valor predeterminado y descripción
Configuración regional	Especifica la configuración regional que se va a utilizar al generar mensajes de error. ■ **en_US** para inglés ■ **ja_JP** para japonés ■ **fr_FR** para francés ■ **de_DE** para alemán ■ **zh_CN** para chino simplificado ■ **zh_TW** para chino tradicional ■ **ko_KR** para coreano
Contraseña del administrador	Esta contraseña se estableció cuando implementó el dispositivo. Puede restablecerla. La contraseña debe tener al menos 8 caracteres, una mayúscula, una minúscula, un dígito y un carácter especial, entre los que se incluyen el signo ! @ # $ % * ( ).
Conjuntos de clave de cifrado	En la mayoría de los casos no es necesario cambiar la configuración predeterminada. Se trata de los algoritmos criptográficos que se utilizan para cifrar las comunicaciones entre los clientes y el dispositivo de Access Point. La configuración del cifrado se utiliza para habilitar varios protocolos de seguridad.
Respetar el orden del cifrado	La opción predeterminada es NO. Seleccione **SÍ** para habilitar el control del orden de la lista de cifrado de TLS.
SSL 3.0 habilitado	La opción predeterminada es NO. Seleccione **SÍ** para habilitar el protocolo de seguridad SSL 3.0.
TLS 1.0 habilitado	La opción predeterminada es NO. Seleccione **SÍ** para habilitar el protocolo de seguridad TLS 1.0.
TLS 1.1 habilitado	La opción predeterminada es SÍ. El protocolo de seguridad TLS 1.1 está habilitado.
TLS 1.2 habilitado	La opción predeterminada es SÍ. El protocolo de seguridad TLS 1.2 está habilitado.
URL de syslog	Introduzca la URL del servidor syslog que se utiliza para registrar los eventos de Access Point. Este valor puede ser una URL, un nombre de host o una dirección IP. Si no configura la URL del servidor syslog, no se registrará ningún evento. Introdúzcala como `syslog://server.example.com:514`.
URL de comprobación de estado	Introduzca una URL a la que se conecta el equilibrador de carga y comprueba el estado de Access Point.
Cookies que se deben almacenar en caché	Conjunto de cookies que Access Point almacena en caché. El valor predeterminado es ninguno.
Modo de IP	Seleccione el modo de IP estática, STATICV4 O STATICV6.
Tiempo de espera de la sesión	El valor predeterminado es **36.000.000** milisegundos.
Modo inactivo	Habilite **SÍ** para pausar el dispositivo de Access Point a fin de conseguir un estado coherente a la hora de realizar las tareas de mantenimiento
Intervalo monitor	El valor predeterminado es **60**.

4 Haga clic en **Guardar**.

Qué hacer a continuación

Configure las opciones del servicio perimetral de los componentes con los que Access Point está implementado. Una vez configuradas las opciones del servicio perimetral, configure las de autenticación.

Actualizar certificados SSL firmados del servidor

Puede reemplazar los certificados firmados cuando caduquen.

En entornos de producción, VMware recomienda encarecidamente sustituir el certificado predeterminado lo antes posible. El certificado de servidor TLS/SSL que se genera al implementar un dispositivo de Access Point no está firmado por una entidad de certificación de confianza.

Prerequisitos

- Certificado firmado y clave privada nuevos guardados en un equipo al que puede acceder
- Convierta los archivos del certificado al formato PEM y los archivos .pem al formato de una línea. Consulte Convertir archivos de certificado al formato PEM de una línea

Procedimiento

1. En la consola de administración, haga clic en **Seleccionar**.
2. En la sección Configuración avanzada, haga clic en el icono de engranaje de Configuración de certificado de servidor SSL.
3. En la fila Clave privada, haga clic en **Seleccionar** y desplácese hasta el archivo de clave privada.
4. Haga clic en **Abrir** para cargar el archivo.
5. En la fila Cadena de certificados, haga clic en Seleccionar y desplácese hasta el archivo de cadena de certificados.
6. Haga clic en **Abrir** para cargar el archivo.
7. Haga clic en **Guardar**.

Qué hacer a continuación

Si la autoridad de certificación que firmó el certificado no es muy conocida, configure los clientes para que confíen en los certificados raíz e intermedio.

Utilizar PowerShell para implementar Access Point

3

Se puede utilizar un script de PowerShell para implementar Access Point. El script de PowerShell se presenta como un script de ejemplo que puede adaptar a las necesidades específicas de su entorno.

Cuando utilice el script de PowerShell, para implementarAccess Point, el script hace una llamada al comando de OVF Tool y valida la configuración para generar automáticamente la sintaxis correcta de la línea de comandos. Este método también permite realizar una configuración avanzada como por ejemplo, que el certificado de servidor TLS/SSL se aplique en el momento de la implementación.

Este capítulo cubre los siguientes temas:

- Requisitos del sistema para implementar Access Point con PowerShell
- Utilizar PowerShell para implementar el dispositivo de Access Point

Requisitos del sistema para implementar Access Point con PowerShell

Para implementar Access Point con el script de PowerShell, debe utilizar versiones específicas de los productos de VMware.

- Host de vSphere ESX con un vCenter Server.
- El script de PowerShell se ejecuta en Windows 8.1 o versiones posteriores, o en Windows Server 2008 R2 o versiones posteriores.

  Este equipo también puede ser un vCenter Server que se ejecuta en Windows o un equipo Windows independiente.
- El equipo Windows que ejecute el script debe tener el comando VMware OVF Tool instalado.

  Debe instalar OVF Tool 4.0.1 o una versión posterior de https://www.vmware.com/support/developer/ovf/.

Debe seleccionar la red y el almacén de datos de vSphere que desea utilizar.

Es necesario asociar un perfil de protocolo de red de vSphere con todos los nombres de red a los que se haga referencia. Este perfil especifica las opciones de configuración de red, como la máscara de subred IPv4, la puerta de enlace, etc. La implementación de Access Point utiliza estos valores para asegurarse de que sean correctos.

Utilizar PowerShell para implementar el dispositivo de Access Point

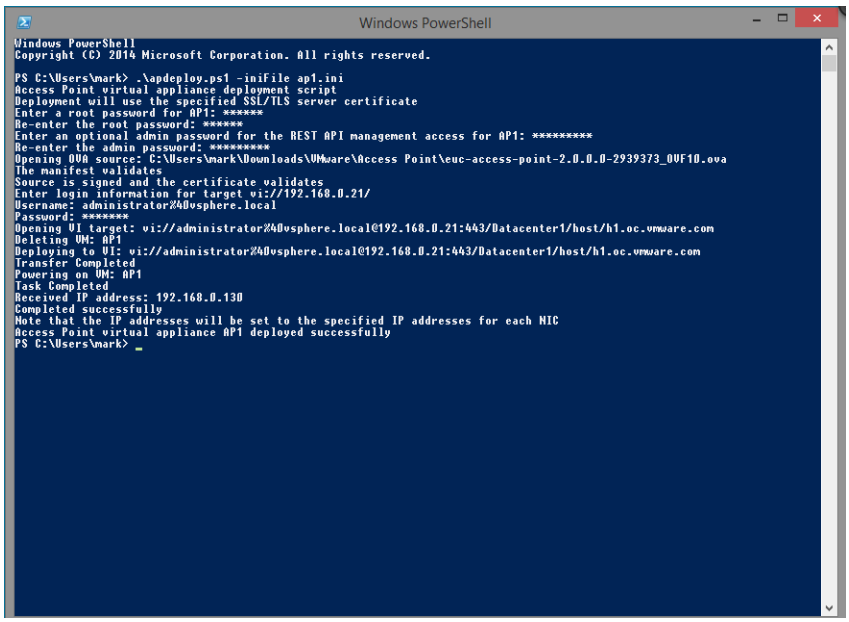
Los scripts de PowerShell preparan su entorno con todas las opciones de configuración. Si ejecuta el script de PowerShell para implementar Access Point, la solución estará lista para producción desde la primera vez que arranque el sistema.

Prerequisitos

- Compruebe que los requisitos del sistema sean correctos y estén disponibles para su uso.

  Este es un script de ejemplo para implementar Access Point en su entorno.

  Figura 3-1. Script de PowerShell de ejemplo



Procedimiento

1. Descargue el archivo OVA Access Point en My VMware en el equipo Windows.
2. Descargue los archivos ap-deploy-XXX.zip en una carpeta del equipo Windows.

   Los archivos zip están disponibles en https://communities.vmware.com/docs/DOC-30835.
3. Abra el script de PowerShell y cambie el directorio por la ubicación de su script.

4 Cree un archivo de configuración .INI para el dispositivo virtual de Access Point.

Por ejemplo, implemente un nuevo dispositivo de Access Point AP1. El archivo de configuración se llama ap1.ini. Este archivo contiene todas las opciones de configuración de AP1. Puede utilizar los archivos .INI de ejemplo incluidos en el archivo .ZIP para crear el archivo .INI y modificar la configuración correctamente.

NOTA: Puede tener archivos .INI únicos para varias implementaciones de Access Point en su entorno. Debe cambiar las direcciones IP y los parámetros del nombre en el archivo .INI correctamente para poder implementar varios dispositivos.

Ejemplo del archivo .INI para modificar.

```
name=AP1
source=C:\APs\euc-access-point-2.8.0.0-000000000_OVF10.ova
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esx1.myco.int
ds=Local Disk 1
netInternet=VM Network
netManagementNetwork=VM Network
netBackendNetwork=VM Network

[Horizon/WebReverseProxy/AirwatchTunnel]
proxyDestinationUrl=https://192.168.0.209

# For IPv4, proxydestinationURL=https://192.168.0.209
# For IPv6, proxyDEstinationUrl=[fc00:10:112:54::220]
```

5 Para asegurarse de que la ejecución del script se realiza correctamente, escriba el comando set-executionpolicy de PowerShell.

```
set-executionpolicy -scope currentuser unrestricted
```

Debe ejecutar este comando una vez y solo si está restringido actualmente.

Si se muestra alguna advertencia relacionada con el script, ejecute el comando para desbloquearla:

```
unblock-file -path .\apdeploy.ps1
```

6 Ejecute el comando para iniciar la implementación. Si no especifica ningún archivo .INI, el script utilizará de forma predeterminara ap.ini.

```
.\apdeploy.ps1 -iniFile ap1.ini
```

7 Introduzca las credenciales cuando se le soliciten y complete el script.

NOTA: Si se le solicita que añada la huella digital del equipo de destino, introduzca **yes**.

El dispositivo de Access Point ya está implementado y disponible para producción.

Para obtener más información sobre los scripts de PowerShell, consulte https://communities.vmware.com/docs/DOC-30835.

Casos prácticos de implementación

4

Los escenarios de implementación descritos en este capítulo pueden ayudarle a identificar y organizar la implementación de Access Point en su entorno.

Puede implementar Access Point con Horizon View, Horizon Air Hybrid-Mode, VMware Identity Manager y VMware AirWatch.

Este capítulo cubre los siguientes temas:

- Implementación de Access Point con Horizon View y Horizon Air Hybrid-Mode
- Implementación de Access Point como proxy inverso
- Implementación de Access Point con AirWatch Tunnel

Implementación de Access Point con Horizon View y Horizon Air Hybrid-Mode

Puede implementar Access Point con Horizon View y Horizon Air Hybrid-Mode. Para el componente de View de VMware Horizon, los dispositivos deAccess Point cumplen la misma función que desempeñaban anteriormente los servidores de seguridad de View.

Caso de implementación

Access Point ofrece acceso remoto seguro a aplicaciones y escritorios virtuales locales de un centro de datos del cliente. Esto funciona como una implementación local de Horizon View u Horizon Air Hybrid-Mode para su administración unificada.

Access Point ofrece a la empresa una gran seguridad con respecto a la identidad del usuario y controla de forma precisa el acceso a sus aplicaciones y escritorios autorizados.

Los dispositivos virtuales de Access Point se suelen implementar en una zona desmilitarizada de red (DMZ). La implementación en la DMZ garantiza que todo el tráfico que entra al centro de datos para recursos de escritorios y aplicaciones es tráfico que está controlado en nombre de usuarios con autenticación sólida. Los dispositivos virtuales de Access Point también garantizan que el tráfico de un usuario autenticado se pueda dirigir solo a los recursos de escritorios y aplicaciones para los que dicho usuario tenga autorización. Este nivel de protección implica la inspección específica de protocolos de escritorio y la coordinación de las direcciones de red y las directivas que pueden cambiar con rapidez, para poder controlar con precisión el acceso.

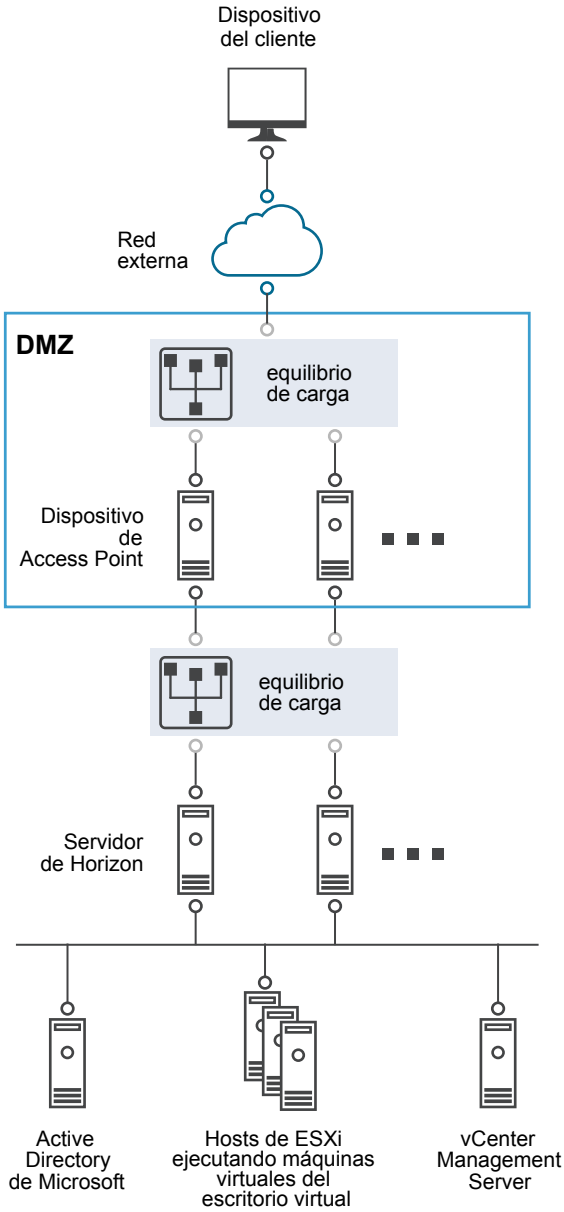
Debe comprobar los requisitos para poder implementar Access Point correctamente con Horizon.

- Cuando el dispositivo de Access Point se dirige a un equilibrador de carga que lidera a los servidores de Horizon, la selección de la instancia del servidor será dinámica.
- Access Point sustituye al servidor de seguridad de Horizon.
- El puerto 443 debe estar disponible para Blast TCP/UDP.
- La puerta de enlace segura Blast y la puerta de enlace segura PCoIP deben estar habilitadas al implementar Access Point con Horizon. De esta forma se garantiza que los protocolos de visualización puedan utilizarse como servidores proxy de forma automática a través de Access Point. Las opciones BlastExternalURL y pcoipExternalURL especifican las direcciones de conexión utilizadas por los clientes de Horizon para dirigir estas conexiones de protocolos de visualización a través de las puertas de enlace adecuadas en Access Point. Esto proporciona una mayor seguridad, ya que estas puertas de enlace garantizan que el tráfico de los protocolos de visualización esté controlado en nombre de un usuario autenticado. Access Point omite el tráfico de los protocolos de visualización sin autorización.
- Deshabilite las puertas de enlace seguras en las instancias del servidor de conexión de View y habilítelas en los dispositivos de Access Point.

La diferencia principal con el servidor de seguridad de View es que Access Point tiene las siguientes características.

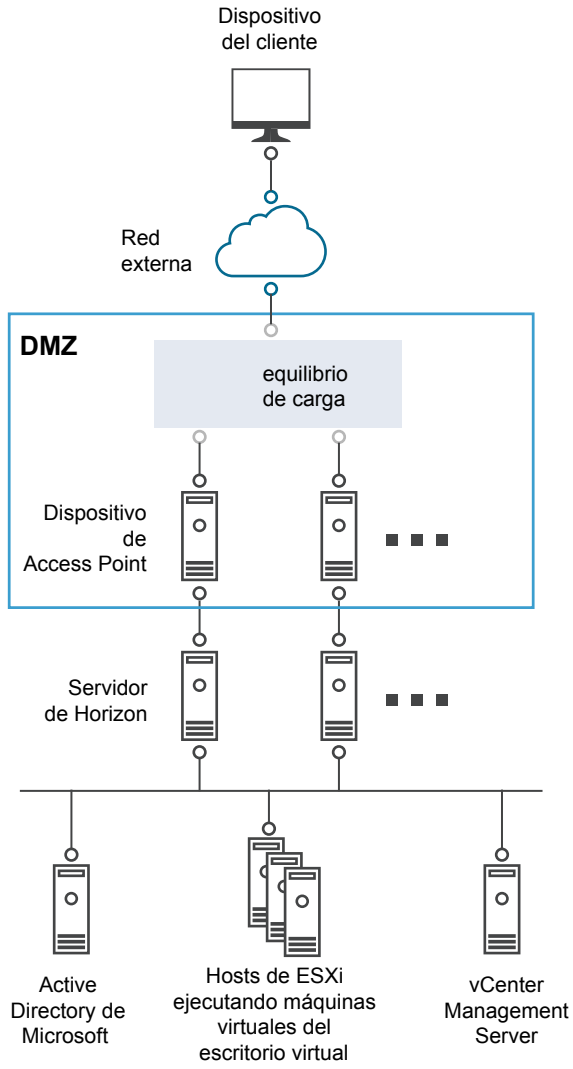
- Implementación segura. Access Point se implementa como una máquina virtual basada en Linux reforzada, bloqueada y preconfigurada
- Escalable. Puede conectar Access Point a un servidor de conexión de View individual, o también puede conectarlo a través de un equilibrador de carga que lidere varios servidores de conexión de View, lo que ofrece una mayor disponibilidad. Actúa como una capa entre las instancias de Horizon Client y los servidores de conexión de View back-end. Dado que la implementación es rápida, se puede ampliar o reducir de forma inmediata para satisfacer las necesidades de las empresas en constante cambio.

Figura 4-1. Dispositivo de Access Point que se dirige a un equilibrador de carga



También puede tener uno o varios dispositivos de Access Point que se dirigen a una instancia individual del servidor. En ambos casos, utilice un equilibrador de carga que lidere a dos o más dispositivos de Access Point en la DMZ.

Figura 4-2. Dispositivo Access Point que se dirige a una instancia del servidor de Horizon



Autenticación

La autenticación de usuario es muy similar al servidor de seguridad de View. Entre los métodos de autenticación de usuario que se admiten en Access Point se incluyen:

- Nombre de usuario y contraseña de Active Directory
- Pantalla completa. Si desea obtener información sobre la pantalla completa, consulte la documentación de Horizon.
- Autenticación en dos fases RSA SecurID, certificada formalmente por RSA para SecurID
- RADIUS a través de un número de soluciones de proveedores de seguridad en dos fases de terceros
- Certificados de usuario PIV X.509, CAC o tarjeta inteligente
- SAML

Estos métodos de autenticación se admiten en combinación con el servidor de conexión de View. Access Point no necesita comunicarse directamente con Active Directory. Esta comunicación funciona como proxy a través del servidor de conexión de View, que puede acceder directamente a Active Directory. Una vez que la sesión de usuario se autentique de conformidad con la directiva de autenticación, Access Point puede reenviar solicitudes al servidor de conexión de View para pedir información de autorización, así como solicitudes de inicio de aplicaciones y escritorios. Access Point también administra los controladores de protocolos de aplicaciones y escritorios para permitirles reenviar solo el tráfico de protocolos autorizado.

Access Point gestiona la autenticación de tarjeta inteligente. Esto incluye opciones para que Access Point se comunique con los servidores del Protocolo de estado de certificados en línea (OCSP) con el fin de comprobar la revocación del certificado X.509, entre otras cuestiones.

Configurar las opciones de Horizon

Puede implementar Access Point desde Horizon View y Horizon Air Hybrid-Mode. Para el componente de View de VMware Horizon, el dispositivo de Access Point cumple la misma función que desempeñaba anteriormente el servidor de seguridad de View.

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la línea Configuración de servicio perimetral de Configuración general, haga clic en **Mostrar**.
3. Haga clic en el icono de engranaje de **Configuración de Horizon**.
4. En la página Configuración de Horizon, cambie de NO a **SÍ** para habilitar Horizon
5. Configure los siguientes recursos de las opciones del servicio perimetral de Horizon

Opción	Descripción
Identificador	Establecido de forma predeterminada en View. Access Point se puede comunicar con servidores que utilizan el protocolo XML de View, como el servidor de conexión de View, Horizon Air y Horizon Air Hybrid-Mode.
URL del servidor de conexión	Introduzca la dirección del servidor Horizon o del equilibrador de carga. Introdúzcala como https://00.00.00.00
Huellas digitales de la URL de destino del proxy	Introduzca la lista de huellas digitales del servidor de Horizon. Si no proporciona una lista de huellas digitales, los certificados del servidor los deberá emitir una entidad de certificación de confianza. Introduzca los dígitos hexadecimales de las huellas digitales. Por ejemplo, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3

6 Para configurar la función del método de autenticación y otras opciones avanzadas, haga clic en **Más**.

Opción	Descripción
Métodos de autenticación	Seleccione los métodos de autenticación que desea utilizar. El método predeterminado es la autenticación pass-through del nombre de usuario y la contraseña. Los métodos de autenticación que configuró en Access Point se muestran en los menús desplegables. Para configurar la autenticación que incluye la aplicación de un segundo método de autenticación si el primer intento de autenticación falla: a Seleccione un método de autenticación en el menú desplegable. b Haga clic en **+** y seleccione Y u O. c Seleccione el segundo método de autenticación en el tercer menú desplegable. Para pedir a los usuarios que se autentiquen a través de dos métodos de autenticación, cambie de O a Y en el menú desplegable.
URL de comprobación de estado	Si hay un equilibrador de carga configurado, introduzca la URL que este utiliza para conectarse y compruebe el estado del dispositivo de Access Point.
SP de SAML	Introduzca el nombre del proveedor de servicios de SAML del agente XMLAPI de View. Este nombre debe coincidir con el nombre de los metadatos del proveedor de servicios configurado o tener un valor especial de DEMO.
PCOIP habilitado	Cambie de NO a **SÍ** para especificar si la puerta de enlace segura de PCoIP está habilitada.
URL externa de proxy	Introduzca la URL externa del dispositivo de Access Point. Los clientes utilizan esta URL para conexiones seguras a través de la puerta de enlace segura de PCoIP. Esta conexión se utiliza para tráfico de PCoIP. El valor predeterminado es la dirección IP de Access Point y el puerto 4172.
Solicitud de la sugerencia de tarjeta inteligente	Cambie de NO a **SÍ** para habilitar que el dispositivo de Access Point sea compatible con la función de sugerencias del nombre de usuario de tarjeta inteligente. Con la función de sugerencias de tarjeta inteligente, el certificado de la tarjeta inteligente de un usuario se puede asignar a varias cuentas de usuario del dominio de Active Directory.
Blast habilitado	Para utilizar la puerta de enlace segura de Blast, cambie de NO a **SÍ**.
URL externa de Blast	Introduzca la URL de FQDN del dispositivo de Access Point que el usuario final utiliza para realizar una conexión segura desde los navegadores web a través de la puerta de enlace segura de Blast. Introdúzcala como https://exampleappliance:443
Túnel habilitado	Si se utiliza el túnel seguro de View, cambie de NO a **SÍ**. El cliente utiliza la URL externa para conexiones de túnel a través de la puerta de enlace segura de View. El túnel se utiliza para RDP, USB y tráfico de redirección multimedia (MMR).
URL externa de túnel	Introduzca la URL externa del dispositivo de Access Point. Se utilizará el valor predeterminado de Access Point si no se estableció ninguno.
Coincidir con el nombre de usuario de Windows	Cambie de NO a **SÍ** para hacer coincidir el nombre de usuario de RSA SecurID y de Windows. Si el valor es SÍ, la autenticación de SecurID se establece en true y se aplicará la coincidencia del nombre de usuario de SecurID y de Windows.

Opción	Descripción
Ubicación de la puerta de enlace	Cambie de NO a **SÍ** para habilitar la ubicación desde el lugar en el que las solicitudes se originan. El servidor de seguridad y Access Point establecen la ubicación de la puerta de enlace. La ubicación puede ser interna o externa.
SSO de Windows habilitado	Cambie de NO a **SÍ** para habilitar la autenticación RADIUS. Al iniciar sesión en Windows, se utilizan las credenciales que se utilizaron en la primera solicitud de acceso correcta de RADIUS.

7 Haga clic en **Guardar**.

Implementación de Access Point como proxy inverso

Access Point se puede utilizar como un proxy inverso de web y puede actuar bien como un proxy inverso normal o como un proxy inverso de autenticación en la DMZ.

Caso de implementación

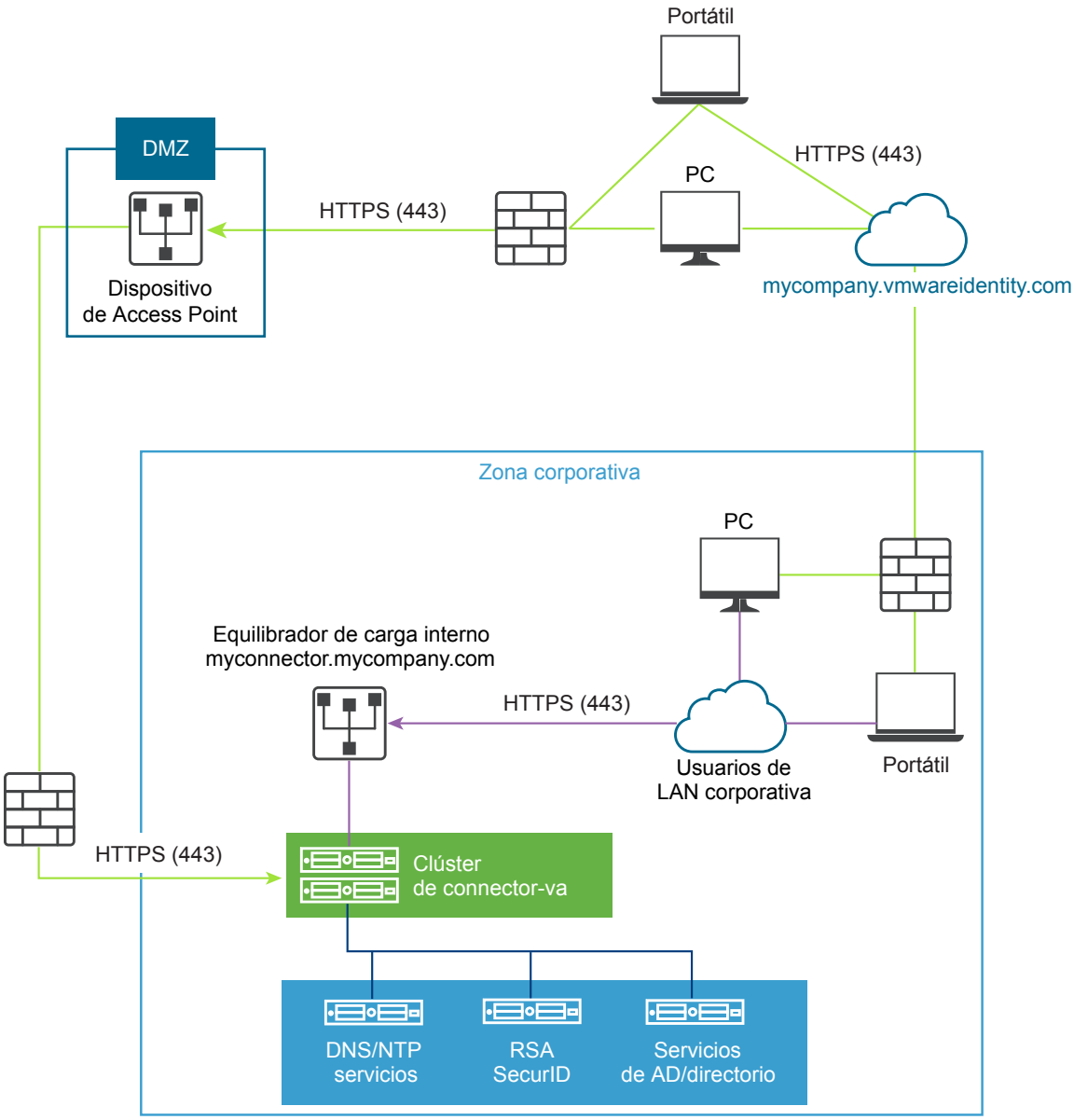
Access Point ofrece acceso remoto seguro para la implementación local de VMware Identity Manager. Los dispositivos de Access Point se suelen implementar en una zona desmilitarizada de red (DMZ). Con VMware Identity Manager, el dispositivo de Access Point funciona como un proxy inverso de web entre el navegador de un usuario y el servicio VMware Identity Manager del centro de datos. Access Point también habilita el acceso remoto al catálogo de VMware Identity Manager para iniciar las aplicaciones de Horizon.

Requisitos para la implementación de Access Point con VMware Identity Manager

- DNS dividido
- El dispositivo de VMware Identity Manager debe tener un nombre de dominio plenamente cualificado (FQDN) como nombre de host.

- Access Point debe utilizar un DNS interno. Esto significa que la propiedad proxyDestinationURL debe utilizar un FQDN.

Figura 4-3. Dispositivo de Access Point que se dirige al conector



Información sobre el proxy inverso

Access Point, como solución, proporciona a los usuarios remotos acceso al portal de aplicaciones para Single Sign-On y acceso a sus recursos. Debe habilitar el proxy inverso de autenticación en un administrador del servicio perimetral. Actualmente se admiten los métodos de autenticación RSA SecurID y RADIUS.

NOTA: Debe generar metadatos de proveedor de identidad antes de habilitar la autenticación en el proxy inverso de web.

Access Point ofrece acceso remoto a VMware Identity Manager y a aplicaciones web con o sin autenticación desde un cliente basado en navegador y, a continuación, inicia el escritorio de Horizon.

- Los clientes basados en navegador son compatibles si utilizan RADIUS y RSA SecurID como métodos de autenticación.

La compatibilidad del proxy inverso es limitada con la versión Access Point 2.8 en VMware Identity Manager, así como los recursos web internos como el WIKI y la confluencia. La lista de recursos se ampliará en el futuro.

NOTA: Las propiedades `authCookie` y `unSecurePattern` no son válidas para el proxy inverso de autenticación. Debe utilizar la propiedad `authMethods` para definir el método de autenticación.

Configurar proxy inverso para VMware Identity Manager

Puede configurar el servicio de proxy inverso de web para utilizar Access Point con VMware Identity Manager.

Prerequisitos

Requisitos para la implementación de Access Point con VMware Identity Manager.

- DNS dividido
- El servicio de VMware Identity Manager debe tener nombre de dominio plenamente cualificado (FQDN) como nombre de host.
- Access Point debe utilizar un DNS interno. Esto significa que la URL de proxyDestination debe utilizar un FQDN.

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la línea Configuración de servicio perimetral de Configuración general, haga clic en **Mostrar**.
3. Haga clic en el icono de engranaje de **Configuración de proxy inverso**.
4. En la página Configuración de proxy inverso, cambie de NO a **SÍ** para habilitar el proxy inverso.
5. Configure los siguientes recursos de las opciones del servicio perimetral de Horizon.

Opción	Descripción
Identificador	El identificador del servicio perimetral se establece en WEB_REVERSE_PROXY.
URL de destino del proxy	Introduzca la dirección del servidor de VMware Identity Manager. Por ejemplo, introduzca **`https://vmwareidentitymgr.example.com`**.

Opción	Descripción
Huellas digitales de la URL de destino del proxy	Introduzca una lista de las huellas digitales que se pueden aceptar del certificado de servidor SSL para la URL de proxyDestination. Si incluye el asterisco*, se admite cualquier certificado. Una huella digital tiene el formato [alg=]xx:xx, donde alg puede ser sha1, el valor predeterminado o md5. 'xx' son dígitos hexadecimales. Por ejemplo, sha=C3 89 A2 19 DC 7A 48 2B 85 1C 81 EC 5E 8F 6A 3C 33 F2 95 C3 Si no configura las huellas digitales, los certificados del servidor los deberá emitir una autoridad de certificación de confianza.
Patrón de proxy	Introduzca las rutas de URI coincidentes que se reenvían a la URL de destino. Por ejemplo, introduzca `(/|/SAAS(.*)|/hc(.*)|/web(.*)|/catalog-portal(.*))`.

6 Para configurar otras opciones avanzadas, haga clic en **Más**.

Opción	Descripción
Métodos de autenticación	El método predeterminado es la autenticación pass-through del nombre de usuario y la contraseña. Los métodos de autenticación que configuró en Access Point se muestran en los menús desplegables. Los métodos de autenticación que configuró en Access Point se muestran en el menú desplegable.
URL de comprobación de estado	Si hay un equilibrador de carga configurado, introduzca la URL que este utiliza para conectarse y compruebe el estado del dispositivo de Access Point.
SP de SAML	Introduzca el nombre del proveedor de servicios de SAML del agente XML API de View. Este nombre debe coincidir con el nombre de los metadatos del proveedor de servicios configurado o tener un valor especial de `DEMO`.
Código de activación	Introduzca el código de activación generado por el servicio de VMware Identity Manager y que se importó a Access Point para establecer la confianza entre VMware Identity Manager y Access Point.
URL externa	El valor predeterminado es la URL del host de Access Point y el puerto 443. Puede introducir otra URL externa. Introdúzcala como `https://<host:port>`.

7 Haga clic en **Guardar**.

Implementación de Access Point con AirWatch Tunnel

El dispositivo de Access Point está implementado en la DMZ. La implementación implica la instalación de los componentes de Access Point y los componentes de AirWatch como por ejemplo, los servicios de proxy de túnel y el agente.

Para implementar AirWatch Tunnel en su entorno AirWatch, es necesario instalar el hardware inicial, así como configurar la información del servidor y las aplicaciones en la consola de administración de AirWatch. Para ello, debe descargar un archivo de instalador y ejecutar el instalador en su servidor de AirWatch Tunnel.

Puede instalar manualmente cada uno de los servicios perimetrales una vez que OVF se haya instalado y los valores hayan cambiado.

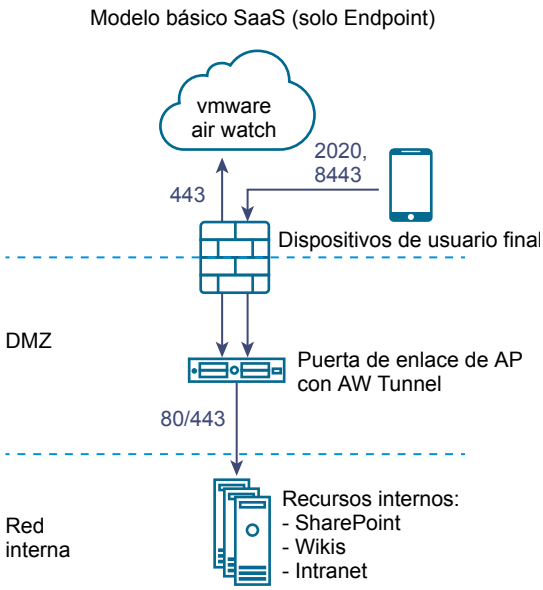
Para obtener más información sobre cómo implementar Access Point con AirWatch, consulte https://resources.air-watch.com/view/vb7zp7wwhpw756m2pfxy .

Implementación del proxy de túnel para AirWatch

La implementación del proxy de túnel protege el tráfico de red entre un dispositivo de usuario final y un sitio web a través de la aplicación móvil VMware Browser desde AirWatch.

La aplicación móvil crea una conexión HTTPS segura con el servidor del proxy de túnel y protege los datos confidenciales. Para utilizar una aplicación interna con el proxy de AirWatch Tunnel, asegúrese de que el SDK de AirWatch esté insertado en su aplicación, lo que le proporcionará capacidades de tunelización con este componente.

Figura 4-4. Implementación del proxy de túnel

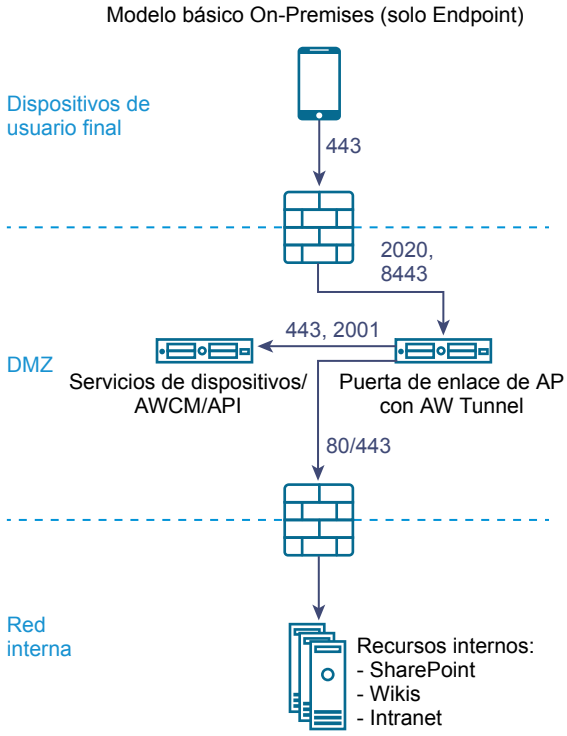


Implementación de túnel por aplicación con AirWatch

La implementación de túnel por aplicación permite que tanto las aplicaciones públicas como las internas puedan acceder de forma segura a los recursos corporativos que se encuentran en su red interna protegida.

Utiliza las capacidades por aplicación que ofrecen los sistemas operativos como, por ejemplo, iOS 7+ o Android 5.0+. Estos sistemas operativos permiten que las aplicaciones específicas aprobadas por los administradores de movilidad puedan acceder a los recursos internos individualmente. La ventaja de utilizar esta solución es que no es necesario realizar ningún cambio en el código para las aplicaciones móviles. La compatibilidad con otros sistemas operativos proporciona una experiencia de usuario sencilla y una mayor seguridad en comparación con cualquier otra solución personalizada.

Figura 4-5. Implementación de túnel por aplicación



Configurar el túnel por aplicación y las opciones del proxy en AirWatch

La implementación del proxy de túnel protege el tráfico de red entre un dispositivo de usuario final y un sitio web a través de la aplicación móvil VMware Browser.

Procedimiento

1 En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.

2 En la línea Configuración de servicio perimetral de Configuración general, haga clic en **Mostrar**.

3 Haga clic en el icono de engranaje de **Túnel por aplicación y configuración de proxy**.

4 Cambie de NO a **SÍ** para habilitar el proxy de túnel.

5 Configure los siguientes recursos de las opciones del servicio perimetral.

Opción	Descripción
Identificador	Establecido de forma predeterminada en View. Access Point se puede comunicar con servidores que utilizan el protocolo XML de View, como el servidor de conexión de View, Horizon Air y Horizon Air Hybrid-Mode.
URL del servidor de API	Introduzca la URL del servidor de la API de AirWatch. Por ejemplo, introduzca https://ejemplo.com:<puerto>.
Nombre de usuario del servidor de API	Introduzca el nombre de usuario para iniciar sesión en el servidor API.
Contraseña del servidor de API	Introduzca la contraseña para iniciar sesión en el servidor de API.

Opción	Descripción
Código del grupo de organización	Introduzca la organización del usuario.
Nombre del host del servidor de AirWatch	Introduzca el nombre de host del servidor de AirWatch.

6 Para configurar otras opciones avanzadas, haga clic en **Más**.

Opción	Descripción
Proxy saliente de AirWatch	Cambie de NO a **SÍ** para inicializar el servicio de proxy de túnel.
HOST del proxy saliente	Introduzca el nombre de host en el que se instala el proxy saliente. **NOTA:** No es el proxy de túnel.
PUERTO del proxy saliente	Introduzca el número de puerto del proxy saliente.
Nombre de usuario de proxy saliente	Introduzca el nombre de usuario para iniciar sesión en el proxy saliente.
Contraseña del proxy saliente	Introduzca la contraseña para iniciar sesión en el proxy saliente.
Autenticación NTLM	Cambie de NO a **SÍ** para especificar que la solicitud de proxy saliente necesita autenticación NTLM.
Usar para el proxy de AirWatch Tunnel	Cambie de NO **SÍ** para utilizar este proxy como un proxy saliente para AirWatch Tunnel. Si no está habilitado, Access Point utiliza este proxy para que la llamada API inicial obtenga la configuración de la consola de administración de AirWatch.

7 Haga clic en **Guardar**.

Configurar Access Point con certificados TLS/SSL

5

Debe configurar los certificados TLS/SSL para los dispositivos de Access Point.

NOTA: La configuración de los certificados TLS/SSL en el dispositivo de Access Point se aplica solo a Horizon View, Horizon Air Hybrid-Mode y el proxy inverso de web.

Configurar certificados TLS/SSL para dispositivos de Access Point

La opción TLS/SSL es obligatoria para las conexiones del cliente a los dispositivos de Access Point. Los dispositivos de Access Point para el cliente y los servidores intermedios que terminan las conexiones TLS/SSL necesitan certificados de servidor TLS/SSL.

Los certificados de servidor TLS/SSL los firma una autoridad de certificación (CA). Una autoridad de certificación es una entidad de confianza que garantiza la identidad del certificado y de su creador. Cuando una autoridad de certificación firma un certificado, los usuarios dejan de recibir mensajes en los que se les pide que comprueben el certificado y de esta forma, los dispositivos del cliente ligero pueden conectarse sin necesidad de configuración adicional.

Al implementar un dispositivo de Access Point se genera un certificado de servidor TLS/SSL predeterminado. En entornos de producción, VMware recomienda sustituir el certificado predeterminado lo antes posible. El certificado predeterminado no está firmado por una CA de confianza. Utilice el certificado predeterminado exclusivamente en un entorno que no sea de producción.

Seleccionar el tipo de certificado correcto

Access Point permite el uso de varios tipos de certificado TLS/SSL. Es crucial seleccionar el tipo de certificado correcto para la implementación. Los distintos tipos de certificado tienen un costo diferente, según el número de servidores en los que se puedan utilizar.

Siga las recomendaciones de seguridad de VMware y utilice nombres de dominio plenamente cualificados (FQDN) para sus certificados, independientemente del tipo seleccionado. No utilice un simple nombre de servidor o dirección IP, ni siquiera para comunicaciones dentro de su dominio interno.

Certificado de nombre de servidor único

Es posible generar un certificado con un nombre de sujeto para un servidor específico. Por ejemplo, `dept.ejemplo.com`.

Este tipo de certificado resulta útil si, por ejemplo, solo se necesita un certificado para un dispositivo de Access Point.

Al enviar una solicitud de firma de certificado a una autoridad de certificación, se proporciona el nombre del servidor que se asociará al certificado. Asegúrese de que el dispositivo de Access Point pueda resolver el nombre de servidor que proporcione de manera que coincida con el nombre asociado al certificado.

Nombres alternativos de sujeto

Un nombre alternativo de sujeto (SAN) es un atributo que se puede agregar a un certificado en el momento de su emisión. Este atributo se utiliza para agregar nombres de sujeto (URL) a un certificado, para que pueda validar más de un servidor.

Por ejemplo, se pueden emitir tres certificados para los dispositivos de Access Point que se encuentran detrás de un equilibrador de carga: `ap1.ejemplo.com`, `ap2.ejemplo.com` y `ap3.ejemplo.com`. Al agregar un nombre alternativo del sujeto que representa el nombre de host del equilibrador de carga, como `horizon.ejemplo.com` en este ejemplo, el certificado será válido porque coincidirá con el nombre de host especificado por el cliente.

Certificado comodín

Un certificado comodín se genera para que se pueda utilizar en varios servicios. Por ejemplo: `*.ejemplo.com`.

Un comodín es útil si muchos servidores necesitan un certificado. Si otras aplicaciones de su entorno, además de los dispositivos de Access Point, necesitan certificados TLS/SSL, también puede utilizar un certificado comodín para esos servidores. No obstante, si utiliza un certificado comodín compartido con otros servicios, la seguridad del producto VMware Horizon dependerá también de la seguridad de esos otros servicios.

NOTA: Solo se puede utilizar un certificado comodín en un único nivel de dominio. Por ejemplo, un certificado comodín con el nombre de sujeto `*.ejemplo.com` se puede utilizar para el subdominio `dept.ejemplo.com` pero no para `dept.it.ejemplo.com`.

Los certificados que se importan al dispositivo de Access Point deben ser de confianza para los equipos cliente y se deben poder aplicar también a todas las instancias de Access Point y a cualquier equilibrador de carga, ya sea mediante el uso de comodines o mediante certificados de nombre alternativo del sujeto (SAN).

Convertir archivos de certificado al formato PEM de una línea

Si desea utilizar la APi de REST de Access Point para configurar las opciones del certificado o bien utilizar los scripts de PowerShell, debe convertir el certificado en archivos de formato PEM para la cadena de certificados y la clave privada y, a continuación, pasar los archivos `.pem` a un formato de una línea que incluya caracteres incrustados de nueva línea.

Al configurar Access Point, es posible que necesite convertir tres tipos de certificados.

- Siempre debería instalar y configurar un certificado de servidor TLS/SSL para el dispositivo de Access Point.
- Si piensa utilizar autenticación de tarjeta inteligente, debe instalar y configurar el certificado emisor de autoridad de certificación del certificado que se agregará a la tarjeta inteligente.
- Si piensa utilizar autenticación de tarjeta inteligente, VMware recomienda instalar y configurar un certificado raíz para la autoridad de certificación que firma el certificado del servidor SAML que está instalado en el dispositivo de Access Point.

Con todos estos tipos de certificados debe realizar el mismo procedimiento para convertir el certificado en un archivo de formato PEM que incluya la cadena de certificados. Con los certificados de servidor TLS/SSL y los certificados raíz, también debe convertir cada uno de los archivos en un archivo PEM que incluya la clave privada. A continuación, deberá convertir cada uno de los archivos `.pem` al formato de una línea que se pueda pasar en una cadena JSON a la API de REST de Access Point.

Prerequisitos

- Compruebe que disponga del archivo de certificado. El formato del archivo puede ser PKCS#12 (`.p12` o `.pfx`) o bien Java JKS o JCEKS.
- Familiarícese con la herramienta de línea de comandos `openssl` que utilizará para convertir el certificado. Consulte https://www.openssl.org/docs/apps/openssl.html.
- Si el certificado tiene el formato Java JKS o JCEKS, familiarícese con la herramienta de línea de comandos de Java `keytool` para convertir en primer lugar el certificado al formato `.p12` o `.pks` antes de convertirlo en archivos `.pem`.

Procedimiento

1 Si su certificado tiene el formato Java JKS o JCEKS, utilice `keytool` para pasar el certificado al formato `.p12` o `.pks`.

IMPORTANTE: Durante la conversión, utilice la misma contraseña de origen y destino.

2 Si su certificado tiene el formato PKCS#12 (`.p12` o `.pfx`), o una pasado el certificado al formato PKCS#12, utilice `openssl` para convertir el certificado en archivos `.pem`.

   Por ejemplo, si el nombre del certificado es `mycaservercert.pfx`, los comandos siguientes le permitirán convertir el certificado:

```
openssl pkcs12 –in mycaservercert.pfx –nokeys –out mycaservercert.pem
openssl pkcs12 –in mycaservercert.pfx –nodes –nocerts –out mycaservercert.pem
openssl rsa –in mycaservercertkey.pem –check –out mycaservercertkeyrsa.pem
```

3 Edite `mycaservercert.pem` y elimine las entradas de certificado que no sean necesarias. Debería incluir el certificado de servidor SSL seguido por cualquier certificado intermedio de AC y un certificado raíz de AC.

4 Los siguientes comandos UNIX le permitirán convertir cada uno de los archivos `.pem` en el valor que se pueda pasar en una cadena JSON a la API de REST de Access Point.

```
awk 'NF {sub(/\r/, ""); printf "%s\\n",$0;}' cert–name.pem
```

   En este ejemplo, *`cert–name`*`.pem` es el nombre del archivo de certificado.

   El nuevo formato coloca toda la información del certificado en una sola línea con caracteres incrustados de nueva línea. Si tiene un certificado intermedio, también deberá tener formato de una línea y estar agregado al primer certificado para que ambos estén en la misma línea.

Ahora puede configurar certificados para Access Point si utiliza estos archivos `.pem` con los scripts de PowerShell adjuntos a la entrada de blog "Utilizar PowerShell para implementar VMware Access Point", disponible en https://communities.vmware.com/docs/DOC-30835. También puede crear y utilizar una solicitud JSON para configurar el certificado.

Qué hacer a continuación

Si convirtió un certificado de servidor TLS/SSL, consulte Sustituir el certificado TLS/SSL predeterminado para Access Point. Si desea información sobre certificados de tarjeta inteligente, consulte Configurar certificado o autenticación de tarjeta inteligente en el dispositivo de Access Point.

Sustituir el certificado TLS/SSL predeterminado para Access Point

Para almacenar un certificado de servidor TLS/SSL firmado por una autoridad de certificación de confianza en el dispositivo de Access Point, debe convertir el certificado al formato adecuado y utilizar scripts de PowerShell o la API de REST de Access Point para configurarlo.

En entornos de producción, VMware recomienda encarecidamente sustituir el certificado predeterminado lo antes posible. El certificado de servidor TLS/SSL que se genera al implementar un dispositivo de Access Point no está firmado por una autoridad de certificación de confianza.

IMPORTANTE: Utilice también este procedimiento para reemplazar periódicamente los certificados firmados por una autoridad de certificación de confianza antes de que caduquen, lo que puede ocurrir cada dos años.

Este procedimiento describe cómo utilizar la API de REST para reemplazar el certificado. Una alternativa más sencilla puede ser utilizar los scripts de PowerShell adjuntos a la entrada de blog "Utilizar PowerShell para implementar VMware Access Point", disponible en https://communities.vmware.com/docs/DOC-30835. Si ya se ha implementado el dispositivo de Access Point, al ejecutar el script de nuevo se apagará el dispositivo, se eliminará y se volverá a implementar con la configuración actual que se especifique.

Prerequisitos

- A menos que ya disponga de un certificado de servidor TLS/SSL válido y de su clave privada, deberá obtener un nuevo certificado firmado de una autoridad de certificación. Al generar una solicitud de firma de certificado (CSR) para obtener uno, asegúrese de que se genere también una clave privada. No genere certificados para servidores con un valor de longitud de clave KeyLength inferior a 1024.

  Para generar la CSR, debe conocer el nombre de dominio plenamente cualificado ((FQDN) que utilizarán los dispositivos cliente para conectarse al dispositivo de Access Point y la unidad organizativa, la organización, la población, el estado y el país para completar el nombre del sujeto.
- Convierta los archivos del certificado al formato PEM y los archivos `.pem` al formato de una línea. Consulte Convertir archivos de certificado al formato PEM de una línea.
- Familiarícese con la API de REST de Access Point. Podrá encontrar la especificación para esta API en la siguiente URL en la máquina virtual donde se instaló Access Point: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.

Procedimiento

1 Cree una solicitud JSON para enviar el certificado al dispositivo de Access Point.

```
{
  "privateKeyPem": "string",
  "certChainPem": "string"
}
```

En este ejemplo, los valores *string* son los valores PEM de una línea de JSON que se crearon como se indicó en los requisitos previos.

2 Utilice un cliente REST como por ejemplo, `curl` o `postman`, para utilizar la solicitud JSON para invocar a la API de REST de Access Point y almacenar el certificado y la clave en el dispositivo de Access Point.

En el ejemplo siguiente, se utiliza un comando de `curl`. En el ejemplo, *access-point-appliance.example.com* es el nombre de dominio plenamente cualificado del dispositivo de Access Point y *cert*.json es la solicitud JSON que creó en el paso anterior.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-appliance.example.com:9443/rest/v1/config/certs/ssl < ~/cert.json
```

Qué hacer a continuación

Si la autoridad de certificación que firmó el certificado no es muy conocida, configure los clientes para que confíen en los certificados raíz e intermedio.

Cambiar los protocolos de seguridad y los conjuntos de cifrado que se utilizan para la comunicación TLS o SSL

Aunque no sea necesario cambiar la configuración predeterminada en casi ningún caso, se pueden configurar los protocolos de seguridad y los algoritmos criptográficos que se utilizan para cifrar las comunicaciones entre los clientes y el dispositivo de Access Point.

La configuración predeterminada incluye conjuntos de cifrado que utilizan cifrado AES de 128 o de 256 bits, excepto para los algoritmos DH anónimos, y los ordena según su nivel seguridad. De forma predeterminada, TLS v1.1 y TLS v1.2 están habilitados. TLS v1.0 y SSL v3.0 están deshabilitados.

Prerequisitos

- Familiarícese con la API de REST de Access Point. Podrá encontrar la especificación para esta API en la siguiente URL en la máquina virtual donde se instaló Access Point: `https://access-point-appliance.example.com:9443/rest/swagger.yaml`.
- Familiarícese con las propiedades específicas para configurar los protocolos y los conjuntos de claves de cifrado: `cipherSuites`, `ssl30Enabled`, `tls10Enabled`, `tls11Enabled` y `tls12Enabled`.

Procedimiento

1 Cree una solicitud JSON para especificar los protocolos y los conjuntos de cifrado que se utilizarán.

En el ejemplo siguiente, se muestra la configuración predeterminada.

```
{
"cipherSuites":
"TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA,TLS_RSA_WITH_AES_128_CBC_SHA,SSL_RSA_WITH_RC4_128_SHA",
  "ssl30Enabled": "false",
  "tls10Enabled": "false",
  "tls11Enabled": "true",
  "tls12Enabled": "true"
}
```

2 Utilice un cliente REST como por ejemplo, `curl` o `postman`, para utilizar la solicitud JSON para invocar a la API de REST de Access Point y configurar los protocolos y los conjuntos de cifrado.

En el ejemplo, *access-point-appliance.example.com* es el nombre de dominio plenamente cualificado del dispositivo de Access Point.

```
curl -k -d @- -u 'admin' -H "Content-Type: application/json" -X PUT https://access-point-
appliance.example.com:9443/rest/v1/config/system < ~/ciphers.json
```

ciphers.json es la solicitud JSON que creó en el paso anterior.

Se utilizarán los protocolos y los conjuntos de cifrado que especificó.

Configurar autenticación en la DMZ

6

Al implementar VMware Access Point por primera vez, la autenticación de contraseña de Active Directory se establece en el valor predeterminado. El usuario introduce su nombre de usuario y su contraseña de Active Directory y estas credenciales se envían a un sistema back-end para autenticación.

Puede configurar el servicio Access Point para realizar autenticación de tarjeta inteligente y certificados, autenticación RSA SecurID, autenticación RADIUS y autenticación adaptativa RSA.

NOTA: La autenticación de contraseña con Active Directory es el único método de autenticación que se puede utilizar con una implementación de AirWatch.

Este capítulo cubre los siguientes temas:

- Configurar certificado o autenticación de tarjeta inteligente en el dispositivo de Access Point
- Configurar la autenticación RSA SecurID en Access Point
- Configurar RADIUS para Access Point
- Configurar la autenticación adaptativa RSA en Access Point
- Generar metadatos SAML de Access Point

Configurar certificado o autenticación de tarjeta inteligente en el dispositivo de Access Point

Puede configurar la autenticación mediante certificado x509 en Access Point para permitir a los clientes autenticarse con certificados en sus escritorios o dispositivos móviles o bien utilizar un adaptador de tarjeta inteligente para la autenticación.

La autenticación basada en certificado se fundamenta en lo que el usuario tiene (clave privada o tarjeta inteligente) y en lo que la persona sabe (la contraseña de la clave privada o el PIN de la tarjeta inteligente). La autenticación de tarjeta inteligente proporciona autenticación de dos factores al verificar tanto lo que la persona tiene (la tarjeta inteligente) como lo que sabe (el PIN). Los usuarios finales utilizan tarjetas inteligentes para iniciar la sesión en sistemas operativos de escritorio remoto de View y para acceder a aplicaciones habilitadas para tarjeta inteligente, como aplicaciones de correo electrónico que utilicen el certificado para firmar correo electrónico para demostrar la identidad del remitente.

Con esta función, la autenticación mediante certificado de tarjeta inteligente se realiza en el servicio Access Point. Access Point utiliza una aserción SAML para comunicar información sobre el certificado X.509 del usuario final y el PIN de la tarjeta inteligente al servidor de Horizon.

Puede configurar la comprobación de la revocación del certificado para impedir la autenticación de los usuarios que tengan certificados de usuario revocados. Los certificados se revocan con frecuencia cuando un usuario abandona una organización, pierde una tarjeta inteligente o se traslada de un departamento a otro. Se admite la comprobación de revocación de certificados con listas de revocación de certificados (CRL) y con el protocolo de estado de certificado en línea (OCSP). Una CRL es una lista de certificados revocados publicada por la autoridad de certificación que los emitió. OCSP es un protocolo de validación de certificados que se utiliza para obtener el estado de revocación de un certificado.

Puede configurar tanto CRL como OCSP en la misma configuración de adaptador de autenticación mediante certificado. Cuando se configuran ambos tipos de comprobación de revocación de certificados y la casilla Usar CRL en caso de error de OCSP está habilitada, se comprueba antes con OCSP y, si esto no funciona, la comprobación de revocación de certificados recae en la CRL. La comprobación de revocación no utiliza OCSP si CRL falla.

También se puede configurar la autenticación de manera que Access Point requiera la autenticación de tarjeta inteligente, pero entonces la autenticación también se pasa al servidor, que puede requerir autenticación de Active Directory.

NOTA: Para VMware Identity Manager, la autenticación siempre pasa a través deAccess Point al servicio de VMware Identity Manager. Se puede configurar la autenticación de tarjeta inteligente para que solo se realice en el dispositivo de Access Point si Access Point se utiliza junto con Horizon 7.

Configurar autenticación mediante certificado en Access Point

La autenticación mediante certificado se habilita y configura en la consola de administración de Access Point.

Prerequisitos

- Obtener el certificado raíz y los certificados intermedios de la CA que firmó los certificados presentados por sus usuarios. Consulte Obtener los certificados de la autoridad de certificación
- Compruebe que los metadatos SAML de Access Point se añadieron al proveedor de servicios y que los metadatos SAML del proveedor de servicios se copiaron al dispositivo de Access Point.
- (Opcional) Lista de identificadores de objeto (OID) de directivas de certificados válidas para la autenticación mediante certificado.
- Para comprobar la revocación, la ubicación del archivo de la CRL y la dirección URL del servidor OCSP.
- (Opcional) Ubicación del archivo del certificado de firma de respuesta de OCSP.
- Contenido del formulario de consentimiento, si este se muestra antes de la autenticación.

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la sección Configuración de autenticación de Configuración general, haga clic en **Mostrar**.
3. Haga clic en el engranaje de la línea del certificado X.509.
4. Configure el formulario del certificado X.509.

   Un asterisco indica que el cuadro de texto es obligatorio. El resto de los cuadros de texto son opcionales.

Opción	Descripción
Habilitar el certificado X.509	Cambie de NO a **SÍ** para habilitar la autenticación del certificado.
***Nombre**	Asigne un nombre a este método de autenticación.
Certificados de la CA raíz e intermedios	Haga clic en **Seleccionar** para seleccionar los archivos de certificado que se van a cargar. Puede seleccionar varios certificados de CA raíz e intermedios que estén codificados como DER o PEM.
Tamaño de la caché de CRL	Introduzca el tamaño de la caché de la lista de revocación de certificados. El valor predeterminado es 100
Habilitar la revocación del certificado	Cambie de NO a **SÍ** para habilitar la comprobación de revocación del certificado. La comprobación de la revocación impide la autenticación de los usuarios con certificados de usuario revocados.
Usar CRL desde los certificados	Active esta casilla para usar la lista de revocación de certificados (CRL) publicada por la CA que emitió los certificados para validar el estado de un certificado, es decir, si está revocado o no.
Ubicación de la CRL	Escriba la ruta de archivo del servidor o local desde la que recuperar la CRL.
Habilitar revocación con OCSP	Active la casilla para usar el protocolo de validación de certificados Protocolo de estado de certificados en línea (Online Certificate Status Protocol, OCSP) para obtener el estado de revocación de un certificado.
Usar CRL en caso de error de OCSP	Si configura tanto CRL como OCSP, puede activar esta casilla para recurrir de nuevo a la CRL si la comprobación con OCSP no está disponible.
Enviar el valor de seguridad (nonce) OCSP	Seleccione esta casilla si desea que se envíe en la respuesta el identificador único de la solicitud de OCSP.
URL de OCSP	Si habilitó la revocación con OCSP, escriba la dirección del servidor OCSP para la comprobación de la revocación.
Certificado de firma de quien responde de OCSP	Introduzca la ruta del certificado de OCSP para la persona que responde, */ruta/al/archivo.cer*.
Habilitar el formulario de consentimiento antes de la autenticación	Seleccione esta casilla para que aparezca una página de formulario de consentimiento antes de que los usuarios inicien sesión en su portal de Workspace ONE mediante la autenticación mediante certificado.
Contenido del formulario de consentimiento	Introduzca aquí el texto que se muestra en el formulario de consentimiento.

5. Haga clic en **Guardar**.

Qué hacer a continuación

Si se configuró la autenticación mediante certificado X.509 y el dispositivo de Access Point se configura detrás de un equilibrador de carga, compruebe que Access Point está configurado con pass-through de SSL en el equilibrador de carga y no está configurado para terminar SSL en el equilibrador de carga. Esta configuración garantiza que el protocolo de enlace de SSL se encuentra entre Access Point y el cliente a fin de pasar el certificado a Access Point.

Obtener los certificados de la autoridad de certificación

Se deben obtener todos los certificados de la autoridad de certificación (CA) correspondiente para todos los certificados de usuario de confianza en las tarjetas inteligentes presentadas por usuarios y administradores. Estos certificados incluyen certificados raíz y pueden incluir certificados intermedios si el certificado de la tarjeta inteligente del usuario fue emitida por una autoridad de certificación intermedia.

Si no dispone del certificado raíz o intermedio de la CA que firmó los certificados en las tarjetas inteligentes presentadas por los usuarios y administradores, puede exportar los certificados de un certificado de usuario firmado por la CA o de una tarjeta inteligente que contenga uno. Consulte Obtener el certificado de CA de Windows.

Procedimiento

- Obtenga los certificados de la CA de uno de los siguientes orígenes.
  - Un servidor Microsoft IIS que ejecute Microsoft Certificate Services. Para obtener información sobre cómo instalar Microsoft IIS, emitir certificados y distribuirlos en su organización, consulte el sitio web de Microsoft TechNet.
  - El certificado raíz público de una CA de confianza. Este es el origen más habitual de los certificados raíz en entornos que ya disponen de una estructura de tarjeta inteligente y de un enfoque estándar para la distribución de tarjetas inteligentes y la autenticación.

Obtener el certificado de CA de Windows

Si dispone de un certificado de usuario firmado por una autoridad de certificación o una tarjeta inteligente que contenga uno, y Windows confía en el certificado raíz, podrá exportar este desde Windows. Si el emisor del certificado del usuario es una autoridad de certificación intermedia, se puede exportar el certificado.

Procedimiento

1. Si el certificado del usuario está en una tarjeta inteligente, insértela en el lector y agregue el certificado del usuario a su almacén personal.

   Si el certificado del usuario no aparece en su almacén personal, utilice el software del lector para exportarlo a un archivo. Este archivo se utiliza en el Paso 4 de este procedimiento.
2. En Internet Explorer, seleccione **Herramientas > Opciones de Internet**.
3. En la pestaña **Contenido**, haga clic en **Certificados**.

4 En la pestaña **Personal**, seleccione el certificado que desee utilizar y haga clic en **Ver**.

Si el certificado del usuario no aparece en la lista, haga clic en **Importar** para importarlo manualmente desde un archivo. Después de importar el certificado, podrá seleccionarlo de la lista.

5 En la pestaña **Ruta de certificación**, seleccione el certificado que está más arriba en el árbol y haga clic en **Ver certificado**.

Si el certificado del usuario está firmado como parte de una jerarquía de confianza, el certificado de firma puede estar firmado por otro certificado de mayor nivel. Seleccione el certificado padre (el que realmente firmó el certificado del usuario) como su certificado raíz. En algunos casos, el emisor puede ser una autoridad de certificación intermedia.

6 En la pestaña **Detalles**, haga clic en **Copiar en archivo**.

Aparecerá el **Asistente para la exportación de certificados**.

7 Haga clic en **Siguiente > Siguiente** y escriba un nombre y una ubicación para el archivo que desea exportar.

8 Haga clic en **Siguiente** para guardar el archivo como certificado raíz en la ubicación especificada.

Configurar la autenticación RSA SecurID en Access Point

Una vez que el dispositivo de Access Point está configurado como agente de autenticación en el servidor RSA SecurID, debe agregar la información de configuración de RSA SecurID al dispositivo de Access Point.

Prerequisitos

- Compruebe que el administrador de autenticación RSA (el servidor RSA SecurID) está instalado y configurado correctamente.
- Descargue el archivo comprimido sdconf.rec del servidor RSA SEcurID y extraiga el archivo de configuración.

Procedimiento

1 En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.

2 En la sección Configuración de autenticación de Configuración general, haga clic en **Mostrar**.

3 Haga clic en el engranaje de la línea de RSA SecurID.

4 Configure la página RSA SecurID.

La información utilizada y los archivos generados en el servidor RSA SecurID son necesarios para configurar la página SecurID.

Opción	Acción
Habilitar RSA SecurID	Cambie de NO a **SÍ** para habilitar la autenticación SecurID.
*Nombre	El nombre es securid-auth.

Opción	Acción
*Número de iteraciones	El número de intentos de autenticación permitidos. Este es el número máximo de intentos de inicio de sesión fallidos cuando se usa el token de RSA SecurID. El valor predeterminado es cinco intentos. **NOTA:** Si más de un directorio está configurado e implementa la autenticación RSA SecurID con directorios adicionales, configure la opción **Número de intentos de autenticación permitidos** con el mismo valor para cada configuración de RSA. Si el valor es distinto, se produce un error en la autenticación SecurID.
*Nombre del host externo	Introduzca la dirección IP de la instancia de Access Point. El valor que introduzca debe coincidir con el que utilizó cuando agregó el dispositivo de Access Point como agente de autenticación al servidor RSA SecurID.
*Nombre del host interno	Introduzca el valor asignado a la solicitud **Dirección IP** en el servidor RSA SecurID.
*Configuración del servidor	Haga clic en Cambiar para cargar el archivo de configuración del servidor RSA SecurID. En primer lugar, debe descargar el archivo comprimido dese el servidor RSA SecurID y extraer el archivo de configuración del servidor, que de forma predeterminada se denomina `sdconf.rec`.
*Nombre del sufijo del ID	Introduzca el ID del nombre que hace que View proporcione una experiencia TrueSSO.

Configurar RADIUS para Access Point

Puede configurar Access Point para que los usuarios tengan que utilizar autenticación RADIUS. La información del servidor RADIUS se configura en el dispositivo de Access Point.

El soporte para RADIUS ofrece una amplia gama de opciones de autenticación alternativas en dos fases basadas en token. Dado que las soluciones de autenticación en dos fases como RADIUS funcionan con administradores de autenticación instalados en servidores distintos, el servidor RADIUS debe estar configurado y accesible para el servicio del administrador de identidades

Cuando los usuarios inician sesión y la autenticación RADIUS está habilitada, aparece en el navegador un cuadro de diálogo de inicio de sesión especial. El usuario debe introducir su nombre de usuario y su código de acceso de autenticación RADIUS en el cuadro de diálogo de inicio de sesión. Si el servidor RADIUS envía una comprobación de acceso, Access Point muestra un cuadro de diálogo que solicita un segundo código de acceso. El soporte actual de comprobación de RADIUS se limita a pedir introducción de texto.

Una vez que el usuario introduce las credenciales en el cuadro de diálogo, el servidor RADIUS puede enviar un mensaje de texto SMS o un correo electrónico, o bien texto mediante cualquier otro mecanismo fuera de banda al teléfono móvil del usuario con un código. El usuario puede introducir este texto y código en el cuadro de diálogo de inicio de sesión para completar la autenticación.

Si el servidor RADIUS proporciona la capacidad de importar usuarios de Active Directory, es posible que se solicite a los usuarios finales en primer lugar que proporcionen las credenciales de Active Directory antes de que se les solicite un código de acceso y un nombre de usuario de autenticación RADIUS.

Configurar autenticación RADIUS

En el dispositivo de Access Point, deberá habilitar la autenticación RADIUS, introducir las opciones de configuración del servidor RADIUS y cambiar el tipo de autenticación a autenticación RADIUS.

Prerequisitos

- Compruebe que el servidor que se utilizará como servidor de administración de autenticación tenga el software de RADIUS instalado y configurado. Configure el servidor RADIUS y, a continuación, configure las solicitudes de RADIUS en Access Point. Consulte las guías de configuración de su proveedor de RADIUS si desea obtener más información sobre la configuración del servidor RADIUS.

Es necesaria la siguiente información del servidor RADIUS:

- Dirección IP o nombre DNS del servidor RADIUS.
- Números de puertos de autenticación. El puerto de autenticación suele ser el 1812.
- Tipo de autenticación. Entre los tipos de autenticación se encuentran PAP (Protocolo de autenticación de contraseña), CHAP (Protocolo de autenticación por desafío mutuo), MSCHAP1 y MSCHAP2 (Protocolo de autenticación por desafío mutuo de Microsoft, versiones 1 y 2).
- Secreto compartido de RADIUS que se utiliza para cifrar y descifrar en los mensajes de protocolo de RADIUS.
- Tiempo de espera específico y valores de reintento necesarios para la autenticación RADIUS

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la sección Configuración de autenticación de Configuración general, haga clic en **Mostrar**.
3. Haga clic en el engranaje de la línea de RADIUS.

Opción	Acción
Habilitar RADIUS	Cambie de NO a **SÍ** para habilitar la autenticación RADIUS.
Nombre*	El nombre es radius-auth
Tipo de autenticación*	Introduzca el protocolo de autenticación que es compatible con el servidor RADIUS. Puede ser PAP, CHAP, MSCHAP1 O MSCHAP2.
Secreto compartido*	Introduzca el secreto compartido de RADIUS.
Número de intentos de autenticación permitidos*	Introduzca el número máximo de intentos de inicio de sesión fallidos cuando se utiliza RADIUS para iniciar sesión. El valor predeterminado es tres intentos.

Opción	Acción
Número de intentos del servidor RADIUS*	Introduzca el número total de intentos de reintento. Si el servidor principal no responde, el servicio espera a la hora configurada antes de volver a intentarlo de nuevo.
Tiempo de espera del servidor en segundos*	Introduzca el tiempo de espera del servidor RADIUS en segundos, después del cual se envía un reintento si el servidor RADIUS no responde.
Nombre de host del servidor RADIUS*	Introduzca el nombre de host o la dirección IP del servidor RADIUS.
Puerto de autenticación*	Introduzca el número de puerto de autenticación RADIUS. El puerto suele ser el 1812.
Prefijo de dominio kerberos	(Opcional) La ubicación de la cuenta de usuario se denomina dominio kerberos. Si especifica una cadena de prefijo de dominio kerberos, esta se colocará delante del nombre de usuario cuando el nombre se envíe al servidor RADIUS. Por ejemplo, si el nombre de usuario introducido es jdoe y se especifica el prefijo de dominio kerberos DOMAIN-A\, el nombre de usuario DOMAIN-A\jdoe se envía al servidor RADIUS. Si no configura estos campos, solo se envía el nombre de usuario introducido.
Sufijo de dominio kerberos	(Opcional) Si configura un sufijo de dominio kerberos, la cadena se coloca al final del nombre de usuario. Por ejemplo, si el sufijo es @myco.com, se enviará el nombre de usuario jdoe@myco.com al servidor RADIUS.
Nombre del sufijo del ID	Introduzca el ID del nombre que hace que View proporcione una experiencia True SSO.
Sugerencia de frase de contraseña de la página de inicio de sesión	Introduzca la cadena de texto que se muestra en el mensaje de la página de inicio de sesión del usuario para indicarle que introduzca el código de acceso RADIUS correcto. Por ejemplo, si este campo se configuró con **contraseña de AD primero, y luego con código de acceso de SMS**, el mensaje de la página de inicio de sesión sería **Introduzca primero su contraseña de AD y luego el código de acceso de SMS.** La cadena de texto predeterminada es **código de acceso RADIUS**.
Habilitar el servidor secundario	Cambie de NO a **SÍ** para configurar un servidor RADIUS secundario para alta disponibilidad. Configure la información del servidor secundario tal y como se describe en el paso 3.

4 Haga clic en **Guardar**.

Configurar la autenticación adaptativa RSA en Access Point

La autenticación adaptativa RSA puede implementarse para proporcionar una autenticación multifactor más segura que la que solo utiliza un nombre de usuario y una contraseña en Active Directory. La autenticación adaptativa supervisa y autentica los intentos de inicio de sesión del usuario según las directivas y los niveles de riesgo.

Cuando se habilita la autenticación adaptativa, los indicadores de riesgo especificados en las directivas de riesgo se configuran en la aplicación RSA Policy Management y la configuración de Access Point de la autenticación adaptativa se utiliza para determinar si un usuario se autentica con el nombre de usuario y la contraseña o si se necesita más información para autenticarlo.

Métodos de autenticación compatibles de la autenticación adaptativa RSA

Los métodos de autenticación seguros de la autenticación adaptativa RSA compatibles en Access Point son la autenticación fuera de banda por correo electrónico, teléfono o SMS y mediante preguntas de comprobación. En el servicio, debe habilitar los métodos de la autenticación adaptativa RSA que pueden proporcionarse. Las directivas de la autenticación adaptativa RSA determinan qué método de autenticación secundaria se utiliza.

La autenticación fuera de banda es un proceso que requiere que se envíe verificación adicional junto con el nombre de usuario y la contraseña del usuario. Cuando los usuarios se registran en un servidor con autenticación adaptativa RSA, deben proporcionar una dirección de correo electrónico, un número de teléfono, o ambos, según la configuración del servidor. Cuando se solicite la verificación adicional, el servidor de autenticación adaptativa RSA envía un código de acceso de un solo uso a través del canal proporcionado. Los usuarios introducirán ese código junto con su nombre de usuario y su contraseña.

Las preguntas de comprobación requieren que el usuario conteste una serie de preguntas cuando se registran en el servidor de autenticación adaptativa RSA. Puede configurar el número de preguntas de registro y el número de preguntas de comprobación que aparecerán en la página de inicio de sesión.

Registrar usuarios con el servidor de autenticación adaptativa RSA

Se debe aprovisionar a los usuarios en la base de datos de autenticación adaptativa RSA para utilizar la autenticación adaptativa en el proceso de autenticación. Los usuarios se agregan a la base de datos de la autenticación adaptativa RSA cuando inician sesión por primera vez con su nombre de usuario y su contraseña. En función de cómo configure la autenticación adaptativa RSA en el servicio, se puede pedir a los usuarios que proporcionen su dirección de correo electrónico, su número de teléfono, su número de servicio de mensajes de texto (SMS) o que establezcan respuestas para las preguntas de comprobación.

NOTA: La autenticación adaptativa RSA no permite introducir caracteres internacionales en los nombres de usuario. Si su intención es permitir caracteres multibyte en los nombres de usuario, póngase en contacto con el equipo de soporte técnico de RSA para configurar la autenticación adaptativa RSA y el administrador de esta función.

Configurar la autenticación adaptativa RSA en Access Point

Para configurar en el servicio la autenticación adaptativa RSA, debe habilitarla, seleccionar los métodos de autenticación adaptativa que se van a aplicar y agregar el certificado y la información de la conexión de Active Directory.

Prerequisitos

- Debe configurar correctamente la autenticación adaptativa RSA con los métodos de autenticación que se van a utilizar en la autenticación secundaria.
- Detalles sobre el nombre de usuario SOAP y la dirección del endpoint SOAP.
- Debe tener disponible la información de la configuración y el certificado SSL de Active Directory.

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la sección Configuración de autenticación de Configuración general, haga clic en **Mostrar**.
3. Haga clic en el engranaje de la línea de autenticación adaptativa RSA.
4. Seleccione la configuración adecuada para su entorno.

NOTA: Un asterisco indica que el campo es obligatorio. Los otros campos son opcionales.

Opción	Descripción
Habilitar el adaptador RSA AA	Cambie de NO a **SÍ** para habilitar la autenticación adaptativa RSA.
Nombre*	El nombre es rsaaa-auth.
Endpoint SOAP*	Introduzca la dirección del endpoint SOAP para permitir la integración entre el servicio y el adaptador de autenticación adaptativa RSA.
Nombre de usuario de SOAP*	Introduzca el nombre de usuario y la contraseña que se utilizó para firmar los mensajes SOAP.

Opción	Descripción
Contraseña de SOAP*	Introduzca la contraseña de API de SOAP de autenticación adaptativa RSA.
Dominio RSA	Introduzca la dirección del dominio del servidor de autenticación adaptativa.
Habilitar el correo electrónico de autenticación fuera de banda	Seleccione SÍ para habilitar la autenticación fuera de banda que envía un código de acceso de un solo uso al usuario final mediante un mensaje de correo electrónico.
Habilitar SMS fuera de banda	Seleccione SÍ para habilitar la autenticación fuera de banda que envía un código de acceso de un solo uso al usuario final mediante un mensaje de texto SMS.
Habilitar SecurID	Seleccione SÍ para habilitar SecurID. Se pide a los usuarios que introduzcan el código de acceso y el token de RSA.
Habilitar pregunta secreta	Seleccione SÍ si va a utilizar preguntas de comprobación y de registro para la autenticación.
Número de preguntas de registro*	Introduzca el número de preguntas que el usuario debe configurar cuando se inscriba en el servidor del adaptador de autenticación.
Número de preguntas de comprobación*	Introduzca el número de preguntas de comprobación que los usuarios deben contestar correctamente para iniciar sesión.
Número de intentos de autenticación permitidos*	Introduzca el número de veces que se muestran las preguntas de comprobación a un usuario que intenta iniciar sesión antes de que se produzca un error en la autenticación.
Tipo de directorio*	El único directorio compatible es Active Directory.
Usar SSL	Seleccione SÍ si utiliza SSL para su conexión de directorio. Agregue el certificado SSL de Active Directory en el campo Certificado del directorio.
Host del servidor*	Introduzca el nombre de host de Active Directory.
Puerto de servidor	Introduzca el número de puerto de Active Directory.
Usar ubicación de servicio DNS	Seleccione SÍ si se utiliza la ubicación del servicio DNS en la conexión del directorio.
DN base	Introduzca el DN desde el que deben empezar las búsquedas en cuentas. Por ejemplo, OU=myUnit,DC=myCorp,DC=com.
DN de enlace*	Introduzca la cuenta que puede buscar usuarios. Por ejemplo, CN=binduser,OU=myUnit,DC=myCorp,DC=com
Contraseña de enlace	Introduzca la contraseña de la cuenta de DN de enlace.
Buscar atributo	Introduzca el atributo de cuenta que contiene el nombre de usuario.
Certificado del directorio	Para establecer conexiones SSL seguras, agregue el certificado de servidor del directorio en el cuadro de texto. En el caso de varios servidores, agregue el certificado raíz de la entidad de certificación.
Usar STARTTLS	Cambie de NO a **SÍ** para utilizar STARTTLS.

5 Haga clic en **Guardar**.

Generar metadatos SAML de Access Point

Para establecer la confianza mutua requerida para la autenticación de tarjeta inteligente, es necesario generar metadatos SAML en el dispositivo de Access Point e intercambiarlos con el servidor.

El lenguaje de marcado para confirmaciones de seguridad (Security Assertion Markup Language, SAML) es un estándar basado en XML que se utiliza para describir e intercambiar información de autenticación y autorización entre distintos dominios de seguridad. SAML transmite información sobre los usuarios entre proveedores de identidades y de servicios en documentos XML llamados aserciones SAML. En este caso, Access Point es el proveedor de identidades y el servidor es el proveedor de servicios.

Prerequisitos

- Configure el reloj (UTC) en el dispositivo de Access Point para que tenga la hora correcta. Por ejemplo, abra una ventana de la consola en la máquina virtual de Access Point y seleccione la zona horaria correcta con la ayuda de los botones de flecha. Compruebe también que el nombre del host ESXi esté sincronizado con un servidor NTP y que VMware Tools, que se está ejecutando en la máquina virtual del dispositivo, sincronice la hora de la máquina virtual con la hora del host ESXi.

  IMPORTANTE: Si el reloj del dispositivo de Access Point no coincide con el del host del servidor, es posible que la autenticación de tarjeta inteligente no funcione.

- Obtenga un certificado de firma que se pueda utilizar para firmar los metadatos de Access Point.

  NOTA: VMware recomienda crear y utilizar un certificado de firma SAML si hay más de un dispositivo de Access Point en la configuración. En este caso, se deben configurar todos los dispositivos con el mismo certificado de firma, para que el servidor pueda aceptar aserciones de cualquiera de los dispositivos de Access Point. Con un certificado de firma SAML específico, los metadatos SAML de todos los dispositivos serán los mismos.

- Si aún no lo ha hecho, convierta el certificado de firma SAML en archivos en formato PEM, y convierta los archivos `.pem` a formato de una línea. Consulte Convertir archivos de certificado al formato PEM de una línea.

Procedimiento

1. En la sección de configuración manual de la IU del administrador, haga clic en **Seleccionar**.
2. En la sección Configuración avanzada, haga clic en el icono de engranaje de **Configuración de proveedor de identidades de SAML** .
3. Seleccione la casilla de verificación **Proporcionar certificado**.
4. Para agregar el archivo de clave privada, haga clic en **Seleccionar** y desplácese hasta el archivo de clave privada del certificado.
5. Para agregar el archivo de cadena de certificados, haga clic en **Seleccionar** y desplácese hasta el archivo de cadena de certificados.
6. Haga clic en **Guardar**.

7 En el cuadro de texto Nombre de host, introduzca el nombre de host y descargue la configuración del proveedor de identidades.

Crear un autenticador SAML utilizado por otros proveedores de servicios

Después de generar los metadatos SAML en el dispositivo de Access Point, se pueden copiar en el proveedor de servicios de back-end. La copia de estos datos al proveedor de servicios es parte del proceso de creación de un autenticador SAML para que se pueda utilizar Access Point como proveedor de identidades.

En el caso de servidores Horizon Air Hybrid-mode, consulte las instrucciones específicas en la documentación del producto.

Copiar metadatos SAML del proveedor de servicios en Access Point

Tras crear y habilitar un autenticador SAML para que Access Point se pueda utilizar como proveedor de identidades, puede generar metadatos SAML en dicho sistema back-end y utilizarlos para crear un proveedor de servicios en el dispositivo de Access Point. Este intercambio de datos establece una relación de confianza entre el proveedor de identidades (Access Point) y el proveedor de servicios back-end, como puede ser el servidor de conexión de View.

Prerequisitos

Compruebe que ha creado un autenticador SAML para Access Point en el proveedor de servicios back-end.

Procedimiento

1 Recupere los metadatos SAML del proveedor de servicios, que generalmente se encuentran en un archivo XML.

Si desea obtener instrucciones, consulte la documentación del proveedor de servicios.

Cada proveedor de servicios tiene su propio procedimiento. Por ejemplo, debe abrir un navegador e introducir una URL, como https://*connection-server.example.com*/SAML/metadata/sp.xml

A continuación, podrá utilizar un comando **Guardar como** para guardar la página web en un archivo XML. El contenido de este archivo comienza con el texto siguiente:

```
<md:EntityDescriptor xmlns:md="urn:oasis:names:tc:SAML:2.0:metadata" ...
```

2 En la sección de configuración manual de la IU del administrador de Access Point, haga clic en **Seleccionar**.

3 En la sección Configuración avanzada, haga clic en el icono de engranaje de **Configuración de proveedor de servicios de SAML** .

4 En el cuadro de texto Nombre de proveedor de servicios, introduzca el nombre del proveedor de servicios.

5 En el cuadro de texto XML de metadatos, pegue el archivo de metadatos que creó en el paso 1.

6 Haga clic en **Guardar**.

Access Point y el proveedor de servicios podrán ahora intercambiar información de autorización y autenticación.

Solucionar problemas relacionados con la implementación de Access Point

7

Dispone de varios procedimientos para diagnosticar y solucionar los problemas que pueden surgir al implementar Access Point en su entorno.

Puede utilizar estos procedimientos para investigar las causas de los problemas e intentar corregirlos usted mismo, o bien puede solicitar ayuda al equipo de asistencia técnica de VMware.

Este capítulo cubre los siguientes temas:

- Solucionar errores de implementación
- Recopilar registros del dispositivo de Access Point
- Habilitar el modo de depuración

Solucionar errores de implementación

Es posible que surjan problemas a la hora de implementar Access Point en su entorno. Si esto ocurriera, tiene a su disposición varios procedimientos para diagnosticar y solucionar problemas relacionados con su implementación.

Advertencia de seguridad al ejecutar scripts descargados de Internet

Compruebe que el script de PowerShell es el script que desea ejecutar y, a continuación, desde la consola de PowerShell, ejecute el siguiente comando:

```
unblock-file .\apdeploy.ps1
```

No se encontró el comando ovftool

Compruebe que el software OVF Tool está instalado en su equipo Windows y que se encuentra en la ubicación establecida en el script.

Red no válida en propiedad netmask1

- El mensaje puede indicar netmask0, netmask1 o netmask2. Compruebe que se haya establecido un valor en el archivo .INI para cada una de las tres redes, como netInternet, netManagementNetwork y netBackendNetwork.

- Compruebe que se haya asociado un perfil de protocolo de red de vSphere con todos los nombres de red a los que se haga referencia. Este perfil especifica las opciones de configuración de red, como la máscara de subred IPv4, la puerta de enlace, etc. Asegúrese de que los valores del perfil de protocolo de red asociado sean correctos para cada una de las opciones.

Mensaje de advertencia que indica que el identificador del sistema operativo no es compatible

Este mensaje de advertencia indica que el identificador del sistema operativo especificado SUSE Linux Enterprise Server 12.0 64-bit (id:85) no es compatible con el host seleccionado. Se asignará el siguiente identificador de sistema operativo: Other Linux (64-bit).

Ignore este mensaje de advertencia. Se asignará automáticamente un sistema operativo compatible.

Configurar Access Point para la autenticación RSA SecurID

Añada las siguientes líneas a la sección de Horizon del archivo .INI.

```
authMethods=securid-auth && sp-auth
matchWindowsUserName=true
```

Añada una nueva sección en la parte inferior del archivo .INI.

```
[SecurIDAuth]
serverConfigFile=C:\temp\sdconf.rec
externalHostName=192.168.0.90
internalHostName=192.168.0.90
```

En ambas direcciones IP se debe establecer la dirección IP de Access Point. El archivo sdconf.rec se obtiene de RSA Authentication Manager, que debe estar completamente configurado. Compruebe que está utilizando Access Point 2.5 o una versión posterior y que puede acceder desde Access Point al servidor RSA Authentication Manager a través de la red. Vuelva a ejecutar el comando apdeploy de Powershell para volver a implementar Access Point configurado para RSA SecurID.

El servicio de ubicación no hace referencia a un error de objeto

Este error informa de que el valor target= utilizado por vSphere OVF Tool no es el correcto para su entorno vCenter. En la tabla que se encuentra en https://communities.vmware.com/docs/DOC-30835 puede consultar ejemplos de formato de target utilizados para hacer referencia a un clúster o un host de vCenter. El objeto de nivel superior se especifica de la siguiente forma:

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/
```

El objeto muestra ahora nombres que se pueden utilizar en el siguiente nivel.

```
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/Cluster1/
or
target=vi://administrator@vsphere.local:PASSWORD@192.168.0.21/Datacenter1/host/esxhost1
```

Los nombres de carpetas, hosts y clústers utilizados para target distinguen entre mayúsculas y minúsculas.

Recopilar registros del dispositivo de Access Point

Para obtener un archivo ZIP que contenga registros de su dispositivo de Access Point, introduzca una URL en un navegador.

Utilice la siguiente URL para recopilar registros procedentes de su dispositivo de Access Point.

```
https://access-point-appliance.example.com:9443/rest/v1/monitor/support-archive
```

En este ejemplo, *access-point-appliance.example.com* es el nombre de dominio plenamente cualificado del dispositivo de Access Point.

Estos archivos de registro se recopilan en el directorio `/opt/vmware/gateway/logs` del dispositivo.

En la tabla siguiente, se muestra la descripción de los distintos archivos incluidos en el archivo ZIP.

Tabla 7-1. Archivos que incluyen información del sistema para ayudar a resolver problemas.

Nombre de archivo	Descripción
`df.log`	Incluye información sobre el uso del espacio en disco.
`netstat.log`	Incluye información sobre las conexiones de red.
`ap_config.json`	Incluye la configuración actual de las opciones del dispositivo de Access Point.
`ps.log`	Incluye un listado de procesos.
`ifconfig.log`	Incluye información sobre las interfaces de red.
`free.log`	Incluye información sobre el uso de la memoria.

Tabla 7-2. Archivos de registro para Access Point

Nombre de archivo	Descripción
`esmanager.log`	Incluye los mensajes de registro procedentes del proceso del administrador del servicio perimetral, que realiza una escucha en los puertos 443 y 80.
`authbroker.log`	Incluye los mensajes de registro del proceso AuthBroker, que controla a los adaptadores de autenticación.
`admin.log`	Incluye los mensajes de registro del proceso que proporciona la API de REST de Access Point en el puerto 9443.
`admin-zookeeper.log`	Incluye los mensajes de registro relacionados con el nivel de datos que se utiliza para almacenar la información de la configuración de Access Point.

Tabla 7-2. Archivos de registro para Access Point (Continua)

Nombre de archivo	Descripción
`tunnel.log`	Incluye los mensajes de registro del proceso de túnel que se utiliza como parte del proceso de API de XML.
`bsg.log`	Incluye los mensajes de registro de la puerta de enlace segura de Blast.
`SecurityGateway_*.log`	Incluye los mensajes de registro de la puerta de enlace segura PCoIP.

Los archivos de registro que acaban en "`–std–out.log`" incluyen la información escrita para `stdout` de varios procesos y suelen estar vacíos.

Archivos de registro de Access Point para AirWatch

- `/var/log/airwatch/tunnel/vpnd`

  Los archivos tunnel-init.log y tunnel.log se obtienen de este directorio.

- `/var/log.airwatch/proxy`

  El archivo proxy.log se obtiene de este directorio.

- `/var/log/airwatch/appliance–agent`

  El archivo appliance-agent.log se obtiene de este directorio.

Habilitar el modo de depuración

Puede habilitar el modo de depuración de un dispositivo de Access Point para ver o manipular el estado interno del dispositivo. El modo de depuración le permite probar el caso de implementación en su entorno.

Prerequisitos

- Compruebe que el dispositivo de Access Point no se está utilizando.

  NOTA: Resulta útil recopilar la información de registro en un dispositivo de Access Point que no está en funcionamiento. Los registros se pueden obtener de la forma habitual.

Procedimiento

1. Inicie sesión en el equipo donde está Access Point.
2. Introduzca el siguiente comando en la interfaz de línea de comandos.

   ```
   cd /opt/vmare/gateway/conf
   ```

3. Consulte el archivo de propiedades del registro.

   ```
   vi log4j–esmanager.properties
   ```

4. Localice la siguiente línea en el archivo de propiedades y edítela. Sustituya info por debug.

   ```
   log4j.logger.com.vmware=info,default
   ```

5 Introduzca el comando para cambiar la configuración de registro desde cualquier ruta.

```
supervisorctl restart esmanager
```