

De la teoría a la práctica: Los principales puntos a tener cuenta para migrar a la gestión moderna de Windows 10 usando VMware Workspace ONE

Índice

El auge de la gestión moderna	3
Opciones de migración: adiós a los enfoques basados en los dispositivos, bienvenidas las identidades	4
La transición hacia la gestión moderna de Windows 10	5
Paso 1: Planificación de la migración	6
Definición de las identidades y las tareas de los usuarios de la organización	6
Definición de los requisitos de las distintas identidades y creación de un programa para la migración	6
Establecimiento de la correspondencia entre las opciones de gestión moderna y tradicional.	7
Paso 2: Preparación del terreno para la migración	7
Determinación de los componentes de la arquitectura de Workspace ONE que se van a implementar.	7
Configuración de los grupos	7
Habilitación de la integración con Workspace ONE Intelligent Hub	8
Configuración de los ajustes de privacidad y propiedad de los dispositivos	8
Integración entre el dominio y Azure	8
Configuración de las colecciones de dispositivos	8
Configuración de los perfiles de trabajo	8
Migración de las aplicaciones	8
Migración y asignación de aplicaciones de Windows	9
Configuración de la distribución en la nube y de igual a igual	9
Configuración del catálogo de aplicaciones	10
Configuración de las actualizaciones.	10
Configuración de los requisitos de conformidad.	11
Valores y parámetros de referencia de los objetos de política de grupo (GPO).	11
Cifrado y BitLocker	11
Conformidad, confirmación de estado y restricciones	11
Scripts y sensores	11
Configuración de la incorporación para las entregas directas.	12
Configuración de la supervisión y la automatización.	12
Supervisión mediante informes y paneles de gestión	12
Configuración de la automatización.	12
Paso 3: Implementación y soporte de la migración	13
Opciones de registro.	13
Interacción y soporte durante las operaciones posteriores.	14
Cómo empezar.	15

MÁS INFORMACIÓN

Para obtener más información sobre Workspace ONE, visite <https://www.vmware.com/es/products/workspace-one.html>.

Para conocer Workspace ONE UEM, visite <https://www.vmware.com/es/products/workspace-one/unified-endpoint-management.html>.

El auge de la gestión moderna

La gestión moderna de escritorios de Windows 10 ya no es una opción, sino una necesidad. Los sistemas de gestión tradicionales para parques de escritorios de Windows suelen estar formados por una amalgama de aplicaciones de software, y dan como resultado un entorno caótico y a menudo inestable. Los enfoques tradicionales utilizan múltiples herramientas administrativas para gestionar el ciclo de vida de los ordenadores, con herramientas independientes para tareas de preproducción y creación de imágenes, mantenimiento de controladores, gestión de actualizaciones del sistema operativo, configuración de políticas de cortafuegos, antivirus y cifrado, etc. La solución es un sistema de gestión moderna que distribuya las políticas, los parches y las aplicaciones desde la nube. Este enfoque resuelve los desafíos de la gestión tradicional, introduce herramientas integradas y mejora la seguridad y la visibilidad.

Debido a la aceleración del uso de los escritorios remotos en 2020 y 2021, y a la probable continuación de su uso intensivo en el futuro, la migración a la gestión moderna de Windows 10 es más urgente que nunca. La implementación de una estrategia de gestión y seguridad que priorice la nube es el método moderno de gestionar escritorios de Windows 10. Una solución nativa de nube para la gestión de escritorios de Windows 10 aumenta la eficiencia y la seguridad, a la vez que ahorra tiempo y dinero.

VMware ofrece una solución de teletrabajo para gestionar escritorios de Windows 10: la plataforma VMware Workspace ONE®. Workspace ONE es la única solución integral y nativa de nube para la gestión moderna de Windows 10 que elimina la necesidad de contar con una infraestructura local, puertas de enlace de nube y herramientas de gestión híbrida complejas. El enfoque de arquitectura nativa de nube de la solución reduce las complicadas infraestructuras locales del pasado y mantiene la posibilidad de diseñar estrategias de perímetro seguro. Esto proporciona a cada empresa el control de su arquitectura, y la libera de los quebraderos de cabeza de gestionarla.

La plataforma Workspace ONE le ofrece las características siguientes para migrar dispositivos con Windows 10 a la gestión moderna:

- Consola de administración que unifica la gestión de la movilidad empresarial (VMware Workspace ONE Unified Endpoint Management [UEM]).
- Posibilidad de configurar la supervisión y la automatización de escritorios de Windows 10 (VMware Workspace ONE® Intelligence).
- Área de trabajo digital para los usuarios finales que incluye, entre otros elementos, un catálogo de aplicaciones unificado, un centro de notificaciones y un portal de autoservicio (VMware Workspace ONE® Intelligent Hub). Los usuarios acceden a las aplicaciones y se registran para utilizarlas mediante Intelligent Hub, y reciben notificaciones sobre aplicaciones nuevas, así como alertas sobre sus dispositivos. También pueden obtener dispositivos y aplicaciones mediante un sistema de autoservicio. Desde esta plataforma, los usuarios finales pueden examinar todas sus aplicaciones y servicios corporativos, lo que incluye aplicaciones nativas de Windows 10, aplicaciones virtuales, aplicaciones web y escritorios virtuales. También existen servicios opcionales que se pueden prestar a los usuarios.
- Herramienta de gestión del ciclo de vida de los escritorios que simplifica la transición de la gestión tradicional del ciclo de vida del PC a la gestión moderna con Workspace ONE UEM (VMware Workspace ONE® AirLift).
- Almacén de cientos de aplicaciones de uso común preempaquetadas y preconfiguradas que el equipo de TI puede implementar instantáneamente en el catálogo de Workspace ONE Intelligent Hub de los usuarios finales (Enterprise App Repository, un componente de Workspace ONE UEM). Las aplicaciones del repositorio se mantienen actualizadas y se prueban para las tres últimas compilaciones del sistema operativo, lo que garantiza que puedan instalarse.
- Plataforma que le permite crear flujos de trabajo personalizados para aplicar a los dispositivos acciones relacionadas con los recursos en un orden específico, siguiendo los criterios detallados que se configuren (VMware Freestyle Orchestrator).
- Herramienta de soporte con la que el personal de TI y de soporte técnico puede ver y controlar de forma remota dispositivos Windows directamente desde la consola de Workspace ONE (VMware Workspace ONE® Assist).

- Herramienta automatizada de inteligencia que examina y corrige las experiencias de los usuarios con las aplicaciones, el sistema operativo y el rendimiento (Digital Employee Experience Management [DEEM]). Muestra análisis de los indicadores clave de rendimiento que afectan a la experiencia de los empleados, como los tiempos de inicio y apagado y los eventos de inicio y cierre de sesión. Recopila datos de los dispositivos Windows y se los envía a Workspace ONE Intelligent Hub, que a su vez se los envía a Workspace ONE Intelligence para mostrarlos y poder interactuar con ellos en los paneles de gestión.
- Asistente virtual automatizado con una función de chat con procesamiento de lenguajes naturales (VMware AVA, incluido en Workspace ONE Intelligent Hub). Los usuarios pueden pedir ayuda para encontrar las herramientas adecuadas, solucionar problemas, pedir dispositivos nuevos, abrir incidencias, gestionar sus tareas, etc.
- Función que le permite mantener todos sus dispositivos protegidos con ajustes y configuraciones basados en políticas estándar del sector (Workspace ONE Baselines). Incluye un catálogo de miles de configuraciones de políticas que puede aplicar a sus dispositivos.
- Servicio que le permite configurar dispositivos para su entrega directa a los usuarios nuevos prácticamente sin intervención del equipo de TI ni tiempo de inactividad del usuario (Drop Ship Provisioning for Workspace ONE, una función de Workspace ONE UEM).



FIGURA 1: Integración del control de acceso, la gestión de aplicaciones y la gestión de terminales multiplataforma en una única plataforma con Workspace ONE

El objetivo de este documento es ofrecer orientación y una descripción de las consideraciones clave para la migración de escritorios de Windows 10 a la gestión moderna con Workspace ONE.

Opciones de migración: adiós a los enfoques basados en los dispositivos, bienvenidas las identidades

La gestión tradicional de dispositivos con Windows 10 utiliza un enfoque basado en el dispositivo, lo que hace que se aplique una configuración independientemente de quién use el dispositivo. Este método funcionaba bien cuando casi todos los ordenadores con Windows estaban en una oficina, porque se podía definir una sola actualización y aplicarla eficientemente a cada dispositivo. Sin embargo, el mundo ha cambiado mucho desde entonces.

La falta de flexibilidad inherente al enfoque basado en el dispositivo, en el que una sola actualización afecta a todos los dispositivos al mismo tiempo, ya no es apropiada para los empleados geográficamente dispersos de hoy día, y la convierte en una opción poco recomendable para la migración. La gestión moderna utiliza un enfoque basado en la identidad, que asume que los empleados utilizan sus dispositivos para más de una tarea, y a menudo en más de un contexto. Una identidad, que a veces se denomina caso de uso, es un grupo de personas que utilizan recursos o servicios a los que acceden a través de arquitecturas diseñadas expresamente. Dentro de una misma identidad es posible tener muchas funciones distintas.

Con un enfoque basado en la identidad, es posible ocuparse de grandes grupos de personas similares simultáneamente. Con un enfoque ágil, el proceso de migración comienza centrándose en una identidad dividida en anillos de distribución. El primer anillo contiene un pequeño número de usuarios, y se abordan todas las tareas relacionadas con esa identidad. Después de una implementación correcta en el primer anillo, puede aplicar los cambios a los siguientes anillos de distribución, y culminar la gestión completa de la primera identidad. El uso de los anillos de distribución le permite probar, confirmar, ajustar y adaptar una implementación a lo largo del proceso.

Un enfoque basado en la identidad puede resultarle útil sea cual sea el tamaño de su organización, ya que le permite ir migrando identidades poco a poco desde las soluciones existentes mientras ajusta y mejora los procedimientos a medida que progresa la migración.

Estos son algunos ejemplos de identidades que han elegido diversas organizaciones. Recomendamos utilizar un total de entre tres y seis identidades, que pueden o no coincidir con las de esta lista.

- IdC
- Dispositivos de quiosco
- Dispositivos de tareas administrativas
- Dispositivos de centros de fabricación
- Dispositivos de laboratorios
- Departamentos de alta seguridad

Una parte esencial del enfoque basado en la identidad consiste en comenzar por una identidad estándar en lugar de un caso de uso específico o especializado.

La transición hacia la gestión moderna de Windows 10

Imagine la migración hacia la gestión moderna de escritorios de Windows 10 como una transición, no un cambio repentino. Puede abordar las etapas de la migración de acuerdo con el tiempo, los fondos y el personal de que disponga. La transición de la gestión tradicional a la gestión moderna es distinta para cada organización. La recompensa es incremental: los ahorros de costes y de tiempo se acumulan progresivamente, independientemente de lo rápida que sea la migración.

Los pasos para la migración son estos:

- Paso 1: Planificación de la migración
- Paso 2: Preparación del terreno para la migración
- Paso 3: Implementación y soporte de la migración

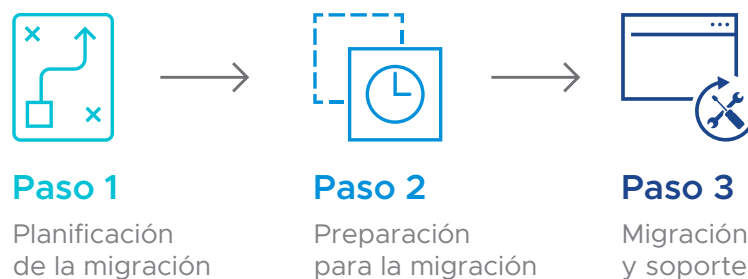


FIGURA 2: Migración a la gestión moderna de Windows 10

Paso 1: Planificación de la migración

Para planificar la migración de su organización a la gestión moderna de escritorios de Windows 10, debe:

- Definir las identidades y las tareas de los usuarios de su organización.
- Definir los requisitos de las distintas identidades.
- Establecer la correspondencia entre las opciones de gestión moderna y tradicional.
- Crear un programa para el proyecto de migración con las dependencias de las tareas.

Definición de las identidades y las tareas de los usuarios de la organización

Definir entre tres y seis identidades es un objetivo razonable. Con un número menor de identidades no tendrá suficientes oportunidades de mejorar el proceso de migración, y con un número mayor complicará la migración y aumentarán los costes.

Cada identidad tiene un conjunto de tareas, y las tareas pueden repetirse para las distintas identidades. Sin embargo, encontrará una desviación entre estas agrupaciones que afecta a la arquitectura y los procedimientos, y que la definirá como una nueva identidad.

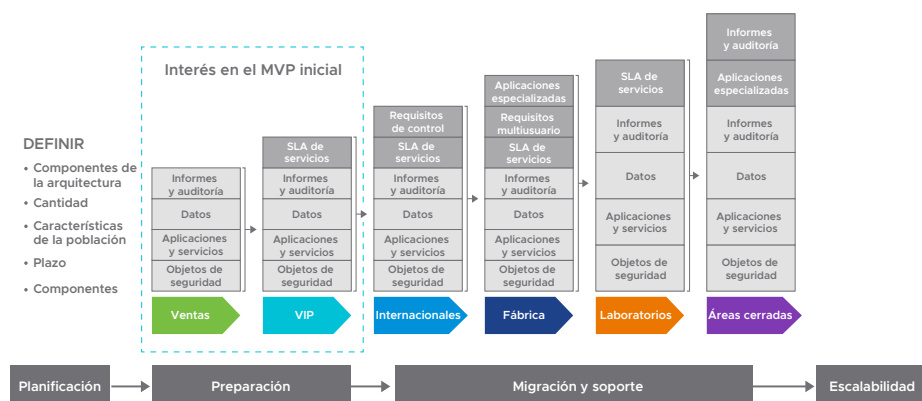


FIGURA 3: Descripción de la migración

Definición de los requisitos de las distintas identidades y creación de un programa para la migración

Cuando haya definido las identidades y las tareas, podrá configurar una lista de los elementos en los que debe trabajar, o *tareas pendientes*. El objetivo es trabajar en *iteraciones*, o bloques de tiempo, de entre dos y tres semanas de duración. Debe calcular las tareas que puede completar en cada iteración y seguir ajustando sus previsiones a medida que avance con el proyecto. Normalmente, cada iteración tiene un tema (que también se conoce como *hito*), que le permite hacer saber a los equipos en los que está trabajando cuáles son las funciones que estarán listas cuando termine la iteración. Este proceso flexible le permite responder mejor a los cambios a medida que se producen. El objetivo es conseguir logros a lo largo del proceso y no esperar hasta el final para ver si el resultado es adecuado para su organización.

Comience por el *producto viable mínimo (MVP)* que necesitaría para gestionar la identidad básica. (Vea un ejemplo en la figura 3). A continuación, debe definir variantes o requisitos incrementales para identidades más complejas. Por ejemplo, en la mayoría de las organizaciones, una identidad podría ser la de los profesionales de ventas o en remoto, que dependen de perfiles de trabajo básicos, como el correo electrónico y la configuración de la red, y de las políticas de protección de datos, y utilizan principalmente aplicaciones de nube y de software como servicio (SaaS). A medida que progrese en las iteraciones, puede incluir requisitos adicionales como los relacionados con perfiles VPN, conformidad estricta, aplicaciones Win32 clásicas, etc.

Establecimiento de la correspondencia entre las opciones de gestión moderna y tradicional.

Cuando establezca la correspondencia entre la gestión moderna y la tradicional, debe tener en cuenta los procesos, los procedimientos, las aplicaciones y las herramientas. No basta con sustituir una herramienta, hay que cambiar la forma en que el equipo de TI interactúa con los usuarios. Lo más probable es que tenga que mover algunos de los datos de sus tipos de herramientas a la nueva plataforma, por ejemplo, para las aplicaciones, así que debe decidir cómo hacerlo. Por ejemplo, Workspace ONE AirLift simplifica la transición desde un sistema de gestión tradicional del ciclo de vida del PC a la gestión moderna con Workspace ONE UEM.

Para la racionalización y migración de *políticas de grupo* a la gestión moderna, Workspace ONE AirLift se comunica con Microsoft Active Directory. Para la racionalización y migración de *aplicaciones* a Workspace ONE UEM, Workspace ONE AirLift interactúa con ConfigMgr.

Paso 2: Preparación del terreno para la migración

Con el fin de prepararse para la migración:

- Determine los componentes de la arquitectura de Workspace ONE que debe implementar.
- Configure los grupos.
- Habilite la integración con VMware Workspace ONE Intelligent Hub.
- Configure los ajustes de privacidad y de propiedad de los dispositivos.
- Efectúe la integración entre el dominio y Azure.
- Configure las colecciones de dispositivos.
- Configure los perfiles de trabajo.
- Migre las aplicaciones.
- Configure las actualizaciones.
- Configure los requisitos de conformidad.
- Configure la incorporación para las entregas directas.
- Configure la supervisión y la automatización.

Trataremos cada uno de estos requisitos brevemente a continuación.

Determinación de los componentes de la arquitectura de Workspace ONE que se van a implementar

Al haber muchos usuarios trabajando de forma remota, lo que incluye usuarios con dispositivos personales, las consideraciones sobre la privacidad son fundamentales. Es preciso respetar las aplicaciones y los datos personales de los usuarios, y proteger las aplicaciones y los datos de la organización.

Para todas sus identidades o casos de uso, haga una lista de las tecnologías existentes, y decida los componentes nuevos de la arquitectura de Workspace ONE que va a integrar primero. La plataforma Workspace ONE le proporciona acceso a diversos productos y funciones, y debe elegir los que desea implementar.

Le recomendamos que implemente Workspace ONE en la mayor medida posible para obtener la mejor experiencia para los usuarios y los administradores.

Configuración de los grupos

Utilice los grupos inteligentes de Workspace ONE para especificar qué plataformas, dispositivos y usuarios reciben una aplicación, una reserva, una política de conformidad, un perfil de trabajo o un aprovisionamiento en concreto. Los grupos inteligentes personalizables proporcionan un mecanismo para la asignación de recursos con arreglo a las necesidades de privacidad y a la propiedad de los dispositivos.

Habilitación de la integración con Workspace ONE Intelligent Hub

Workspace ONE Intelligent Hub es esencial para la experiencia de los usuarios finales. Impleméntelo y contemple la posibilidad de configurar servicios adicionales de Workspace ONE Intelligent Hub, como Custom Branding, People Search y la pestaña Home.

Configuración de los ajustes de privacidad y propiedad de los dispositivos

A los usuarios finales que trabajan en sus propios dispositivos (los usuarios de BYOD) les preocupa especialmente la privacidad de su contenido personal en un dispositivo gestionado por Workspace ONE UEM. Debe garantizar a los empleados que sus datos personales no son objeto de supervisión por parte de la empresa.

Workspace ONE UEM le permite garantizar la privacidad de los datos personales. Puede crear políticas de privacidad personalizadas basándose en el tipo de propiedad del dispositivo.

Integración entre el dominio y Azure

Workspace ONE UEM consigue una buena integración con Microsoft Active Directory (AD) y Microsoft Azure Active Directory (AAD), por lo que dispondrá de una serie de flujos de trabajo de incorporación que se aplican a una amplia gama de casos de uso de Windows 10.

Para migrar cargas de trabajo, debe integrar Workspace ONE AirLift con ConfigMgr y con el dominio de Active Directory.

Configuración de las colecciones de dispositivos

Workspace ONE AirLift conecta las colecciones de dispositivos de ConfigMgr con los grupos inteligentes de Workspace ONE UEM.

Para las identidades principales, migre todas las colecciones de dispositivos a Workspace ONE, de modo que, cuando finalice sus configuraciones, pueda asignárselas a los grupos inteligentes correspondientes.

Configuración de los perfiles de trabajo

La gestión tradicional de Windows utiliza objetos de política de grupo (GPO) para gestionar los dispositivos. En la gestión moderna de Windows de Workspace ONE, el mecanismo principal para gestionar los dispositivos son los perfiles de trabajo. Los perfiles de trabajo son conjuntos de controles implementados en dispositivos individuales. Cada perfil está formado por ajustes, configuraciones y restricciones. Cuando los perfiles de trabajo se combinan con las políticas de conformidad, se aplican reglas y procedimientos corporativos.

Por ejemplo, con Workspace ONE, los usuarios no introducen una contraseña para la red wifi, sino que pueden utilizar dicha red mediante el certificado incluido en el perfil de trabajo. Los usuarios se conectan a la red wifi automáticamente cuando inician sesión, tal como se especifica en su perfil de trabajo.

Del mismo modo, los usuarios se conectan automáticamente a la VPN cuando inician sesión gracias a su perfil de trabajo específico.

Migración de las aplicaciones

La migración de aplicaciones requiere tres pasos principales:

- Migrar las aplicaciones de Windows y asignarlas a identidades o grupos inteligentes.
- Configurar la distribución en la nube y de igual a igual.
- Configurar el catálogo de aplicaciones de Workspace ONE Intelligent Hub.

La arquitectura de distribución de software de Workspace ONE UEM está respaldada por la integración de una red de distribución de contenido (CDN) y de la tecnología de igual a igual. Esto significa que los usuarios finales pueden tener sus aplicaciones instaladas sea cual sea su ubicación, sin necesidad de una infraestructura compleja.

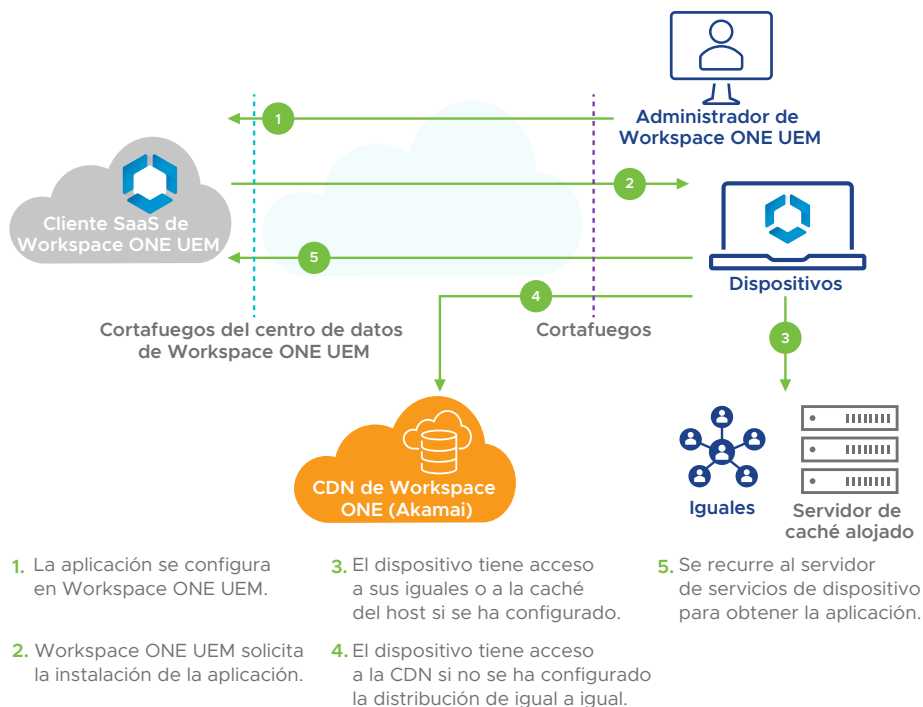


FIGURA 4: Arquitectura de distribución de software de Workspace ONE UEM

Migración y asignación de aplicaciones de Windows

Workspace ONE UEM le permite distribuir la mayoría de los tipos de aplicaciones a los dispositivos con Windows 10: aplicaciones de la Plataforma universal de Windows (UWP), aplicaciones basadas en la nube, aplicaciones remotas o alojadas y aplicaciones clásicas de Windows.

Puede utilizar Workspace ONE AirLift para la migración, y Enterprise App Repository para acelerar la adición de aplicaciones de Windows directamente en Workspace ONE UEM.

Configuración de la distribución en la nube y de igual a igual

Workspace ONE le permite configurar la distribución de aplicaciones en la nube y de igual a igual. Si se suscribe a Workspace ONE utilizando el modelo de SaaS, VMware proporciona una CDN. Con una CDN, los usuarios reciben las aplicaciones y sus actualizaciones automáticamente desde la nube. Cuando un dispositivo que se encuentra en una ubicación geográfica muy alejada solicita la descarga de una aplicación, se le dirige a la red y al nodo de distribución en la nube más cercanos para que la descargue desde ellos. Después de la primera solicitud de descarga, las descargas de la aplicación se almacenan en caché en los nodos de la CDN.

Las organizaciones que disponen de implementaciones locales de Workspace ONE pueden integrarlas con su propia CDN para conseguir las mismas ventajas.

Workspace ONE UEM ofrece el sistema de distribución de igual a igual como método alternativo para implementar aplicaciones de Windows en redes empresariales. La distribución de aplicaciones de igual a igual reduce el tiempo de descarga de las aplicaciones grandes y beneficia a las organizaciones que tienen:

- Múltiples dispositivos en una ubicación de oficinas
- Oficinas en ubicaciones remotas con ancho de banda bajo
- Una estructura de sucursales
- Oficinas con una latencia alta en la CDN y el servidor de servicios de dispositivo

Para estas descargas de igual a igual, Workspace ONE es compatible con Adaptiva, una herramienta de distribución de software de igual a igual, y la caché para sucursales nativa integrada en Windows 10. Puede utilizar la distribución de igual a igual de Workspace ONE o un sistema de distribución de igual a igual asociado a Adaptiva.

Configuración del catálogo de aplicaciones

Asegúrese de configurar Workspace ONE Intelligent Hub para que los usuarios puedan acceder a las aplicaciones migradas.

Configuración de las actualizaciones

Workspace ONE UEM utiliza un modelo de actualización como servicio y envía actualizaciones periódicas del sistema operativo Windows y de las funciones. Las actualizaciones tradicionales de los sistemas operativos siguen un modelo de «borrar y sustituir», pero Workspace ONE UEM aplica las actualizaciones del sistema operativo con frecuencia y de manera dinámica. Por lo tanto, los usuarios finales siempre tienen acceso a las funciones actualizadas del sistema operativo.

Workspace ONE UEM utiliza Windows Update para empresas (WUfB), que está basado en la nube, en lugar de Windows Server Update Services (WSUS). El servicio tradicional WSUS requiere muchos controles detallados y tiene unos costes de almacenamiento elevados porque las actualizaciones se almacenan en el entorno local. Con WUfB, los usuarios descargan las actualizaciones en línea de acuerdo con sus perfiles de trabajo.

Cuando configure WUfB y las políticas de actualización, debe definir los anillos de distribución de las identidades de usuario y las políticas de actualización de cada anillo de distribución. En Workspace ONE se denominan *grupos de asignación*.

Puede crear los grupos de distribución de forma aleatoria para repartir los riesgos entre los grupos de destino, o crear anillos de distribución teniendo en cuenta la importancia de obtener las actualizaciones. Asegúrese de dejar tiempo suficiente para efectuar las pruebas y la validación antes de aplicar las actualizaciones a los anillos esenciales.

El primer anillo de distribución que cree debe ser pequeño y estar compuesto por usuarios que toleren las pruebas preliminares y que sean capaces de proporcionar comentarios técnicos rigurosos, como el grupo de TI. Los siguientes anillos de distribución pueden incluir a la mayoría de los usuarios, siguiendo una estrategia que ponga a prueba las suposiciones obtenidas con los grupos más pequeños. Los últimos anillos de distribución incluirán las excepciones y pequeños colectivos de usuarios atípicos.



FIGURA 5: Implementación de un enfoque de anillos para configurar las actualizaciones

Configuración de los requisitos de conformidad

Para proteger los dispositivos con Windows 10 de su entorno, debe configurar el cifrado y la conformidad.

Valores y parámetros de referencia de los objetos de política de grupo (GPO)

Al adoptar la gestión moderna, pasará a utilizar las políticas de grupo y otras configuraciones basadas en la nube. Una parte importante del uso de las políticas de grupo basadas en la nube comienza por evaluar las políticas actuales y determinar si es preciso trasladarlas a Workspace ONE UEM. Workspace ONE AirLift simplifica la validación y la conversión de las políticas de grupo (GPO) tradicionales actuales en políticas basadas en la gestión de dispositivos móviles.

Si actualmente no tiene políticas de grupo en el dominio o prefiere comenzar desde cero, puede utilizar Workspace ONE Baselines. Workspace ONE Baselines ayuda a mantener protegidos todos sus dispositivos mediante ajustes y configuraciones estándar que se basan en las plantillas Microsoft Windows Desktop Benchmark y Microsoft Windows 10 Security Baseline del Centro para la Seguridad en Internet (CIS). Workspace ONE Baselines utiliza un microservicio basado en la nube que gestiona un catálogo de miles de configuraciones de políticas que pueden aplicarse a los dispositivos. Puede crear valores de referencia o ampliarlos utilizando este catálogo de políticas basadas en archivos de Microsoft ADMX. Estos valores de referencia se basan en los GPO y funcionan de forma similar a estos.

Cifrado y BitLocker

Workspace ONE UEM le permite gestionar el ciclo de vida de cifrado y configurar el cifrado automatizado de los dispositivos con Windows 10. Para ello, debe migrar desde McAfee Management of Native Encryption, configurar un perfil de cifrado de BitLocker y comprobar la configuración de cifrado aplicada.

Conformidad, confirmación de estado y restricciones

Puede utilizar Workspace ONE UEM para establecer la confianza en los usuarios, evaluar la situación de los dispositivos y posibilitar la prevención de pérdida de datos.

Para establecer la confianza en los usuarios, Workspace ONE UEM utiliza funciones de identidad sólidas. Entre ellas se encuentra la autenticación de dos factores, que requiere que un dispositivo registrado, gestionado y conforme emplee dos mecanismos de autenticación.

Para comprobar la situación de los dispositivos, Workspace ONE UEM utiliza su motor de conformidad para evaluarlos, aplicarles políticas de manera local y corregirlos. Esta herramienta de Workspace ONE UEM garantiza que todos los dispositivos respetan las políticas especificadas. Una política puede incluir ajustes de seguridad básicos u otros más esenciales.

La consola de Workspace ONE UEM se utiliza para especificar pasos de notificación de problemas, acciones disciplinarias, periodos de gracia y mensajes.

Para minimizar el riesgo de pérdida de datos, Workspace ONE UEM aprovecha al máximo las funciones nativas de Windows Information Protection. La prevención de pérdida de datos en los dispositivos controla la propagación de datos a la nube.

Scripts y sensores

VMware Freestyle Orchestrator es una plataforma de coordinación de TI sin código que le permite crear flujos de trabajo complejos y personalizados que se aplican a los dispositivos con flexibilidad y rapidez. Puede configurar criterios detallados para organizar las acciones relacionadas con los recursos que se van a aplicar a los dispositivos en un orden específico. Los recursos que puede utilizar en un flujo de trabajo son:

- Aplicaciones (solo internas)
- Condiciones
- Grupos
- Perfiles
- Sensores
- Scripts
- Tratamiento de errores

Configuración de la incorporación para las entregas directas

Workspace ONE le permite distribuir dispositivos con Windows 10 totalmente configurados a los escritorios de los usuarios, de modo que los usuarios nuevos pueden ser productivos inmediatamente. Esta incorporación para las entregas directas libera al equipo de TI de laboriosas tareas de configuración para cada usuario. Y, dado el número cada vez más alto de teletrabajadores, el ahorro de tiempo es considerable.

¿Cómo se efectúan las entregas directas de los dispositivos a los usuarios nuevos?

La función Drop Ship Provisioning for Workspace ONE permite a los fabricantes de equipos originales (OEM) de dispositivos Windows y a los administradores de VMware proporcionar una experiencia de usuario prácticamente sin intervención del equipo de TI ni tiempo de inactividad del usuario. Las configuraciones, los ajustes y las aplicaciones vienen precargados de fábrica. Ahora, en lugar de esperar a que se descarguen las aplicaciones y se apliquen las configuraciones, el usuario se encuentra con un dispositivo listo para utilizarlo al arrancarlo por primera vez. Y si el equipo de TI efectúa posteriormente una restauración o recuperación del dispositivo, la funcionalidad de restauración automatizada permite conservar las aplicaciones y la gestión, lo que minimiza el tiempo de inactividad.

Configuración de la supervisión y la automatización

Workspace ONE Intelligence le permite configurar la supervisión y automatización de los escritorios de Windows 10 y se integra con Workspace ONE UEM para proporcionar visibilidad unificada y datos en tiempo real.

Supervisión mediante informes y paneles de gestión

Workspace ONE Intelligence es un servicio que agrega y correlaciona datos de múltiples orígenes para proporcionar visibilidad de todo el entorno de Windows a través de informes y paneles de gestión. Puede utilizar los informes para obtener información y los paneles de gestión para visualizar datos y garantizar la conformidad de los dispositivos.

Configuración de la automatización

La automatización de Workspace ONE Intelligence utiliza parámetros para activar un flujo de trabajo. El flujo de trabajo se puede personalizar para que actúe cuando se presenten escenarios específicos en un entorno de Workspace ONE.

A continuación se enumeran algunos ejemplos del uso de la automatización de Workspace ONE Intelligence:

- **Estado de la batería:** puede automatizar la detección de los dispositivos con Windows 10 cuya batería no esté en condiciones óptimas. Los dispositivos Windows que no pueden funcionar una jornada laboral completa sin cargarse provocan interrupciones y reducen la movilidad y la productividad de los empleados. La automatización de la sustitución de las baterías puede ayudarle a mejorar la experiencia del empleado, aumentar la productividad y maximizar vida útil de los dispositivos.
- **Corrección de parches:** puede automatizar la corrección de parches para los escritorios de Windows 10 con Workspace ONE Intelligence. Es posible crear un panel de gestión en Workspace ONE Intelligence que muestre todos los dispositivos que actualmente carecen de una actualización esencial de Windows. También es posible crear una automatización que notifique a los usuarios cuándo deben actualizar sus dispositivos. La combinación de las funciones de gestión de dispositivos con Workspace ONE UEM permite a los administradores de TI aprobar la implementación de parches e informar sobre ella.
- **Automatización basada en sensores:** los sensores le permiten satisfacer de manera flexible los requisitos de conformidad de InfoSec, ya que puede consultar cualquier parámetro del sistema, desde el hardware al software, y hacer que esté disponible para la generación de informes y la corrección automatizada. Por ejemplo, con los scripts de sensores, los administradores pueden consultar la versión de las aplicaciones, el estado de cifrado, los valores de las claves del registro y otros datos que deseen, y utilizar la automatización de Intelligence para solucionar discrepancias de conformidad.

Paso 3: Implementación y soporte de la migración

Ahora que ha planificado la migración y se cumplen los requisitos, puede migrar los escritorios de Windows 10 de su organización, etapa por etapa, e identidad por identidad, según lo programado.

Su primera identidad debe ser un pequeño grupo que pueda tolerar su curva de aprendizaje para la migración. Basándose en su experiencia con este primer grupo, puede ajustar y modificar el proceso, y continuar con la siguiente identidad. Cuando llegue al último 20 % de los usuarios, tendrá una metodología comprobada.

Workspace ONE proporciona mecanismos para apoyar la actividad laboral de los usuarios finales, lo que incluye el soporte remoto y el acceso a las aplicaciones.

Opciones de registro

La inclusión de los escritorios de Windows 10 en la gestión moderna de Workspace ONE se denomina *registro*. Si un dispositivo es totalmente nuevo, efectúe una entrega directa. Si un dispositivo ya existe, instale Workspace ONE Intelligent Hub.

Puede adaptar el siguiente árbol de decisiones a su organización para que le ayude a determinar las opciones de registro para los escritorios de Windows 10. Los posibles flujos de trabajo de incorporación de este árbol de decisiones son los siguientes:

- **Aprovisionamiento mediante entrega directa:** los fabricantes de equipos originales de dispositivos Windows y los administradores de VMware pueden proporcionar una experiencia prácticamente sin intervención del equipo de TI ni tiempo de inactividad del usuario. Las configuraciones, los ajustes y las aplicaciones vienen precargados de fábrica. En lugar de esperar a que se descarguen las aplicaciones y se apliquen las configuraciones, puede tener un dispositivo listo para utilizarlo al arrancarlo por primera vez.
- **Registro en Microsoft Azure Active Directory:** Workspace ONE UEM se integra con Azure AD y proporciona una completa selección de flujos de trabajo de incorporación, incluidos Autopilot y el registro durante la experiencia de uso inmediato.
- **Registro basado en agentes:** utiliza VMware Workspace ONE Intelligent Hub para Windows 10, que permite a los usuarios finales registrar sus propios dispositivos, lo que les proporciona flexibilidad y control, y reduce la sobrecarga del equipo de TI.
- **Registro basado en la línea de comandos:** proporciona la máxima flexibilidad de administración mediante el uso de parámetros en los comandos. Permite automatizar el registro utilizando las herramientas PCLM o el dominio existentes.

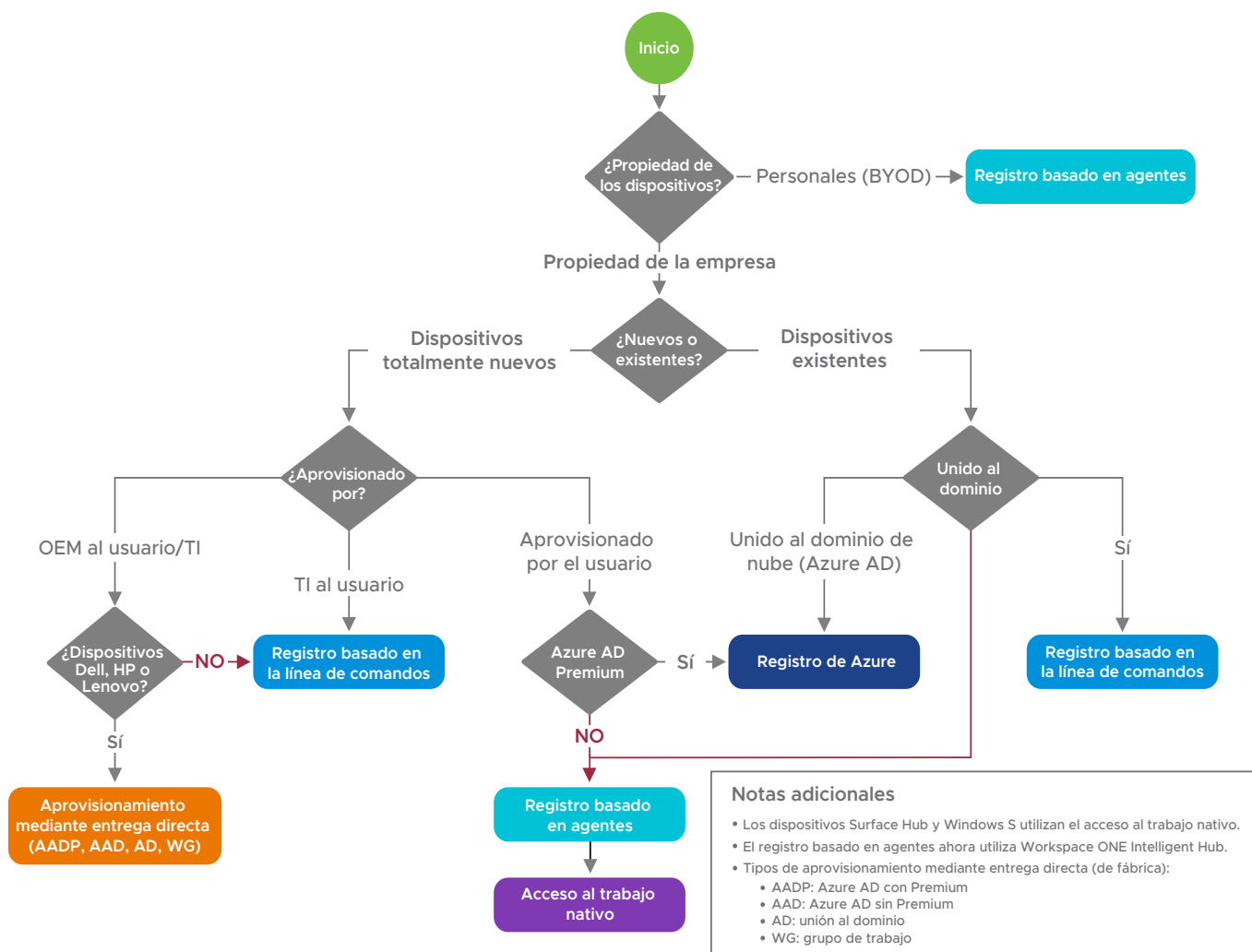


FIGURA 6: Árbol de decisiones para la incorporación de Windows 10

Interacción y soporte durante las operaciones posteriores

Workspace ONE Intelligent Hub

Workspace ONE Intelligent Hub es una pieza fundamental para que continúe la implicación entre los usuarios y el equipo de TI. Es un catálogo centralizado de aplicaciones y notificaciones empresariales, así como un portal que permite a los empleados interactuar con el equipo de TI y realizar operaciones en la modalidad de autoservicio con sus dispositivos y aplicaciones.

Con VMware AVA, que forma parte de Workspace ONE Intelligent Hub, los usuarios pueden interactuar con una función de chat con procesamiento de lenguajes naturales para obtener ayuda al buscar las herramientas adecuadas, solucionar problemas, pedir dispositivos nuevos, abrir incidencias, gestionar sus tareas, etc.

Soporte remoto con Workspace ONE Assist

Workspace ONE Assist permite ver o controlar de forma remota los dispositivos de los usuarios directamente desde la consola de Workspace ONE, y mantener la privacidad y la confianza de los empleados.

Soporte proactivo con Digital Employee Experience Management

Digital Employee Experience Management (DEEM) le permite dar soporte proactivo a los usuarios de Windows 10 mostrando análisis de los indicadores clave de rendimiento. DEEM mejora las posibilidades de dar soporte a los escritorios de Windows 10.

MÁS INFORMACIÓN

- Visite [VMware TechZone](#)
- Vea las dos partes de la sesión de VMworld para clientes sobre la gestión que prioriza la nube:
 - [Pasos reales para la gestión que prioriza la nube \(parte 1 de 2\)](#)
 - [Pasos prácticos para la gestión que prioriza la nube \(parte 2 de 2\)](#)

Cómo empezar

La migración a la gestión moderna de escritorios de Windows 10 no puede hacerse de la noche a la mañana, es un proceso. Los planes que le llevarán a implementar la migración son fundamentales, por lo que debe tomarse su tiempo para diseñarlos y después para ejecutarlos metódicamente.

Workspace ONE lleva la gestión de Windows 10 y la experiencia y las operaciones de soporte de los empleados al siguiente nivel. Para obtener más información sobre el modo en que la gestión moderna nativa de nube con Workspace ONE simplifica las operaciones, refuerza la seguridad y proporciona experiencias de uso inmediato a los empleados en todas partes, vea el [laboratorio práctico de Workspace ONE](#).



VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com
C/ Rafael Botí, 26 - 2.ª planta, 28023 Madrid, España. Tel. +34 914125000 Fax +34 914125001 www.vmware.es

Copyright © 2021 VMware, Inc. Todos los derechos reservados. Este producto está protegido por las leyes de derechos de autor y de propiedad intelectual de Estados Unidos e internacionales. Los productos de VMware están cubiertos por una o varias de las patentes enumeradas en vmware.com/go/patents. VMware es una marca comercial o marca registrada de VMware Inc. o sus filiales en Estados Unidos o en otras jurisdicciones. Las demás marcas y nombres mencionados en este documento pueden ser marcas comerciales de sus respectivas empresas. N.º artículo: FY21-6168-VMW-WIN10-MOD-MGMT-WKSP1-WP-A4-WEB-20210120_ES 2/21