Quest

Dispositivo de administración de sistemas KACE® 11.1

Notas de la versión

Índice

Notas de la versión 11.1 del dispositivo de administración de sistemas KACE® de Quest®

En este documento, se proporciona información acerca de la versión 11.1 de KACE Systems Management Appliance.

Acerca del dispositivo de administración de sistemas KACE 11.1

KACE Systems Management Appliance es un dispositivo virtual diseñado para automatizar la administración de dispositivos, la implementación de aplicaciones, la aplicación de parches, la administración de activos y la administración de tickets de la mesa de servicios. Para obtener más información acerca de la serie KACE Systems Management Appliance, visite https://www.quest.com/products/kace-systems-management-appliance/. Esta versión contiene una serie de nuevas características, problemas resueltos y mejoras de seguridad.

NOTA: Este es el único documento traducido para esta versión; sin embargo, las variantes localizadas no incluyen información sobre los problemas ya resueltos, las mejoras y los problemas conocidos. Otras guías, como la *Guía para el administrador* y la ayuda en el producto, no están localizadas en este momento; además, se incluyen los documentos de la versión 10.2.

Nuevas características

Esta versión de KACE Systems Management Appliance incluye las siguientes características.

Comunicaciones del dispositivo

- **Adiciones de la bandeja del sistema del agente de KACE**: Se agregaron más funcionalidades al ícono del agente en la bandeja del sistema, como los vínculos de apertura. Los administradores del sistema pueden especificar hasta diez vínculos que aparecen en el nuevo elemento de menú **Accesos directos**. Este elemento de menú solo aparece cuando se especifican uno o más vínculos en la configuración de comunicación del agente, en la sección Accesos directos del ícono de estado del agente.

  Se admiten vínculos de identificador uniforme de recursos (URI) estándar, como las direcciones URL de HTTP, SSH y FTP. Al hacer clic en este vínculo, el sistema inicia la aplicación asociada al recurso seleccionado. Por ejemplo, cuando hace clic en un vínculo de tipo HTTP, el sistema lo abre en el navegador predeterminado.
- **Inventario de Hyper-V**: La información de inventario y los comandos de dispositivos relacionados se agregaron en esta versión para el Administrador de máquina virtual y los Datos de MS Hyper-V para dispositivos administrados por un agente. En los detalles del inventario, se incluye una lista de máquinas

virtuales y hosts de Hyper-V para inventariar. Esto es similar a la función de inventario de VMware creada en la versión 10.0.

- **Actualizaciones compatibles con el sistema operativo**: El dispositivo ahora es compatible con las siguientes versiones de SO en dispositivos administrados por un agente:
  - MS Windows 10 20H2
  - MS Windows Server 2019 20H2
  - macOS 11.0
    - Cuando se conecta a **Consola de usuario** mediante HTTPS desde un sistema macOS 11.0, el dispositivo no puede determinar el identificador único (KUID) del agente asociado a ese sistema. Esto afecta a la lista *Mis dispositivos* y a la instalación de la Biblioteca de software. La causa raíz de este problema es el nuevo requisito de macOS 11.0 en el que el usuario debe aprobar todos los valores de confianza del certificado. Este problema también hace que la siguiente entrada aparezca en `konea.log` en el agente:

      ```
      |ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot |
      SecTrustSettingsSetTrustSettings failed|{"err":"La autorización se denegó
      debido a que no era posible interactuar con el usuario."}
      ```

    - El dispositivo no admite la aplicación del parche del sistema operativo para esta versión. La aplicación de parches está disponible. Los parches a nivel de SO para dispositivos macOS 11.0 están disponibles con KACE Cloud Mobile Device Manager (MDM), si tiene una suscripción.

Aplicación de parche

- **Actualizaciones del paquete de Linux**: El dispositivo ahora le permite automatizar el proceso de instalación y administración de actualizaciones del paquete de Linux, lo que mantiene actualizado el SO Linux en los dispositivos SUSE, Ubuntu, CentOS, Raspbian y Red Hat Linux administrados. Estas actualizaciones mejoran el rendimiento general de sus dispositivos con Linux administrados y los protegen de posibles vulnerabilidades.

  Utilice esta función para crear programas de actualización que le permitan detectar actualizaciones de paquetes o detectar y actualizar todos los paquetes que correspondan. Puede revisar la lista de actualizaciones de paquetes disponibles después de una acción de programa solo de detección, para cada variante de Linux.

  El proceso de actualización se basa en la suposición de que sus dispositivos Linux administrados apuntan a los repositorios de paquetes adecuados. Solo se identifican los paquetes que incluyen actualizaciones de seguridad. El dispositivo no intenta detectar o actualizar todos los paquetes ni todo el SO a la última versión.

  NOTA: Raspbian Linux no distingue entre las actualizaciones regulares y de seguridad. La detección y actualización de paquetes para dispositivos administrados de Raspbian da como resultado la instalación de todos los paquetes actualizados en esos dispositivos.

- **Integración en el nuevo catálogo de actualizaciones de hardware de Dell**: A partir de esta versión, el dispositivo utiliza una nueva versión del catálogo de hardware de Dell. El proceso de detección e implementación de actualizaciones de hardware es muy similar al utilizado para aplicar parches en el dispositivo. Comience por crear actualizaciones de programas para detectar, implementar o detectar e implementar actualizaciones de hardware. Puede revisar la lista de las actualizaciones de Dell disponibles en la página del catálogo. En esta página, se enumeran las actualizaciones de los archivos de firma que existen en el dispositivo.
  - Esta función requiere la última versión del agente de KACE para que se ejecute en dispositivos Dell administrados.
  - Los datos existentes con relación a las actualizaciones de hardware de Dell, como el historial de programas, no se migran desde versiones anteriores del dispositivo.
  - Los informes de usuario asociados a las actualizaciones de hardware de Dell y creados con una versión anterior del dispositivo no se migran a la versión 11.1.

Infraestructura

- **Oval para Linux y Mac**: En esta versión, el dispositivo extiende la compatibilidad de Oval más allá de solo al MS Windows existente mediante la selección más grande y óptima del mundo de datos de CVE.
- **Alertas de renovación de licencias**: Cuando el mantenimiento del dispositivo expira, algunas características, como la compatibilidad con la aplicación de parches, ya no estarán disponibles. Esto provoca que aparezca una alerta de error en el Panel de inicio. Para renovar su licencia, visite https://support.quest.com/contact-us/renewals.

Mesa de servicio

- **Jerarquía de categorías de tickets de la mesa de servicio**: Se mejoró la Consola del administrador para permitirle definir categorías y subcategorías más optimizadas para la mesa de servicio. Puede crear y editar nodos de categorías y subcategorías de tickets mediante un widget de árbol. La vista de árbol le permite comprender y administrar mejor las relaciones entre las categorías. Puede agregar fácilmente nuevos nodos de categoría, cambiarles el nombre, eliminarlos u ordenarlos, según sea necesario. También hay una función de búsqueda disponible para localizar rápidamente una categoría o subcategoría específica.
- **Capacidad para especificar el prefijo del ticket de la mesa de servicio**: A partir de esta versión, puede utilizar un prefijo diferente para cada cola a fin de organizar su flujo de trabajo de la mesa de servicio y asociarlo a las categorías correspondientes, como `HELP:` para la mesa de servicio o `HDREQ:` para solicitudes de hardware y software.
- **Compatibilidad para el servicio GCC High de Microsoft 365**: Sus credenciales OAuth de MS Office 365 ahora le permiten especificar su tipo de inquilino y dirección URL de punto de punto de conexión de Azure AD a fin de adquirir tokens para la nube nacional asociada a su entorno. Cuando seleccione un mensaje de correo electrónico entrante de OAuth sobre Office 365 de mesa de servicio, puede apuntar a un servicio API de Microsoft 365 correspondiente, como GCC de Microsoft 365 y GCC High de Microsoft 365, entre otros. En particular, GCC High de Microsoft 365 se utiliza en entornos de alta seguridad.

Mejoras

La siguiente es una lista de las mejoras implementadas en esta versión.

Mejora	Id. del problema
Windows Installer now preserves the `NoHooks userinit` registry setting during upgrade.	K1A-2393
Managed Installation can continue if the Agent disconnects.	K1A-2392
KACE Agent no verifies the Konea tunnel and alerts the server if broken.	K1A-2384
The user is alerted when reboot is pending and patching operations are skipped as a result.	K1A-2381
11.1 KACE macOS agents use PKG installer file rather than DMG disk image.	K1A-2374
API access can now be restricted through the *Access Control List Details* page.	K1-30596
This version includes the ability to sort by custom ticket fields in KACE GO.	K1-30562

Mejora	Id. del problema
SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local `admin` user.	K1-30246
This version includes an option to reject SAML users who do not already have an account on the appliance.	K1-30211
Approval Status column is added to the *Quarantine* list and *Quarantine Detail* pages.	K1-30105
In the *General Settings* page, an option is added to indicate interest in participation in a future Beta program.	K1-30071
The appliance now includes the ability to select an Azure AD *GCC High account* during the creation of credentials for a Office365 OAuth account, and to set the URL endpoint for a .us domain.	K1-22281
In the email notification text editor, the **$** button now allows insertion of tokens.	K1-22082
Added the ability to select a *single-tenant* Azure AD account type during the creation of credentials for a Office365 OAuth account.	K1-21914
User's manager can now be reset to *Unassigned* either manually through the **Consola del administrador**, or during LDAP import with an empty manager mapped field.	K1-19328
Discovery schedules for devices associated with an Active Directory server, now include a new option for enabling the appliance to use a secure port for LDAP communication, **Use Secure LDAP (LDAPS)**. This check box is available in the *Active Directory* section on the *Discovery Schedule Detail* page, when you select **Active Directory** as the *Discovery Type*.	N/A
Access Control List restrictions can be now applied based on sub-domains. You can specify the sub-domain name on the *Access Control List* page, in the *IP Address/ Doomain* column of the *Allow List*.	N/A

Problemas resueltos

La siguiente es una lista de los problemas resueltos en esta versión.

Resolved Service Desk issues

Problema resuelto	Id. del problema
Creating a Service Desk process template that included a separator could result in an error when used from the User Portal.	K1-30698
Time Closed, *Time Stalled* and *Time Opened* are not updated for a parent ticket with approvals.	K1-30685
When copying text from a Word application to a ticket, the formatting could not be retained.	K1-30545

Problema resuelto	Id. del problema
When duplicating a process, the ticket template was not duplicated.	K1-30460
Tickets with very long summary fields could result in an error when the *Tickets* list page loads.	K1-23726
Default ticket template is not set when creating a new ticket by email.	K1-23422
Unexpected rendering behavior (scrolling) could be seen when viewing ticket details when multiple categories and sub-categories are present.	K1-22645
In the Service Desk list view, *Time Open* and *Time Opened* are renamed to *Time Since Last Opened* and *Last Opened*, respectively.	K1-22630
Emails sent with display names with a comma or multi-language character to a Service Desk queue through POP3 was not handled correctly, in some cases.	K1-22610
Image was broken using several variables in email templates.	K1-21347
Email On Event ticket notification emails were formatted differently than Custom Ticket Rule emails.	K1-21198
Default value was not displayed on ticket detail page for drop-down fields with *Always Required* option.	K1-21187
Service Desk: Token emails from Gmail to Gmail leaved behind empty spaces.	K1-21186
When a ticket is submitted by email with embedded dark colors, the text was hidden if the **Consola del administrador** is also set to a dark theme.	K1-21147
Process parent ticket did not close if child tickets were closed from *Tickets* list view.	K1-21143
Service Desk email notifications broke if templates exceeded character limits.	K1-21118
Advanced Search: Filters did not work as expected when using Unassigned Owner.	K1-21116
Advanced Search in *Tickets* list: Filters did not work as expected when using *Status* and *Process Status*.	K1-21107
Populating a Service Desk ticket multi-selection custom field with double quotes in the select value resulted in unexpected behavior.	K1-21094
Ticket attachment links sent in email notifications did not work as expected in some cases.	K1-19964

Resolved KACE Agent issues

Problema resuelto	Id. del problema
CentOS receives all updates with the Linux Update feature. The security filter is not available for the Linux Package Upgrades page.	K1A-3810

Problema resuelto	Id. del problema
KACE Agent 11.0 failed to download file from HTTPS source, impacting use of replication shares that are accessed through the HTTPS protocol.	K1A-2330
Client certificate install operation could timeout on newly provisioned Windows devices, preventing the agent from receiving any commands from the appliance until a reconnect event happened.	K1A-2329
VMM managed Hyper-V host was not added to appliance during VMM inventory when the Agent is installed on some Hyper-V hosts.	K1A-2328
Replication did work when password had an '@' symbol.	K1A-2326
macOS 11.0 (Big Sur): Installing KACE Agent with the Agent Status icon enabled resulted in warnings during installation.	K1A-2318
`konea.exe` and `clientidentifier.exe` could crash in some environments.	K1A-2291
Recurring Alert messages kept spawning new Windows on endpoint.	K1A-2289
Wake-on-LAN (WoL) through relay did not display error when the relay agent selected was down.	K1A-2285
Tokens were treated as invalid by agents (error: Agent token signed by another server) if the appliance database became out of sync with the file system.	K1-30642
SNMP inventory data from Dell servers could cause inventory to fail.	K1-30615
In the **Consola de administración del sistema**, on the *Agent Token Detail* page, *Organization* is represented with its ID instead of name.	K1-29969
Offline KScripts did not run when scheduled for *Run on the* instance/day of week.	K1-21173
MSI Policy wizard script could fail to set the registry value correctly.	K1-21049
Scripting option *Allow run without a logged-in user* cleared still allowed script to run.	K1-19576
SMB URLs did not properly handle passwords with special characters.	K1-17342

Resolved Inventory issues

Problema resuelto	Id. del problema
SNMP inventory mistakenly identified non-hex strings as hex strings, causing incorrect values in some cases.	K1-30668
Dell Warranty retrieval errors were not logged to the new `dell_warranty_log` error file.	K1-30531
Overdue Service Desk widgets included tickets that were not yet overdue.	K1-30480

Problema resuelto	Id. del problema
In the **Quarantine** list page, it was not possible to view the details of a quarantined device.	K1-24508
Viewing script logs from the *Device Detail* page displayed blank logs.	K1-21349
Reset Tries button in *Windows Feature Updates Status* on *Device Detail* page did not always work.	K1-21172
Gateway IP Address was not an available column on the *Devices* list page.	K1-21131
Machine deletion could lead to software installation counts being inaccurate.	K1-20437
No history was tracked when Smart Label was edited.	K1-17612

Other resolved issues

Problema resuelto	Id. del problema
The *Windows Feature Update Summary* page did not correctly list all updates, in some cases.	K1-30887
Knowledge Base articles with multiple labels could be hidden for users.	K1-30671
LDAP Import: Scheduled imports set to *None* could still run automatically.	K1-30666
Compliance by Patch and *Compliance by Machine* widgets sometimes did not display correct values.	K1-30630
Images did not appear correctly in knowledge base articles, in some cases.	K1-30565
Emails with multiple CC's sent to a Service Desk queue through a POP3 server could not be handled correctly.	K1-30533
File attachments of type .eml or .msg were missing from tickets submitted by email.	K1-30527
Managed Installation with **Override default installation** configured would show **Default installation** set after saving.	K1-30481
An error could be seen while creating custom view on the *Quarantine* page in the **Consola de administración del sistema**.	K1-29978
Do not associate file Managed Installation option was not displayed correctly after saving.	K1-29927
In some cases, the network settings for the proxy settings were not honored by the Credential manager when using an Office365 OAuth account.	K1-29063
Access to the **Consola del administrador** could be disrupted when changing an organization's virtual IP address or host name.	K1-25452

Problema resuelto	Id. del problema
Email sent to Service Desk queues that use a multi-part MIME format could fail to parse correctly.	K1-22656
When a non-administrative queue owner attempts to retrieve the list of Service desk tickets using the API, tickets they did not submit could be omitted from the results.	K1-22653
SFTP- and FTP-specific *Offboard Backup Transfer Settings* fields containing backslashes caused offboard backup failure.	K1-22608
The *Object History* page sometimes failed to load when it contained Windows Feature Update data.	K1-21575
Agent upstream tunnel client certificate validation failed when an aging konea certificate was archived.	K1-21354
In KACE GO it was not possible to accept barcode searches that have embedded spaces or new line characters.	K1-21195
SAML LDAP attribute mapping option could cause authentication failures.	K1-21193
Asset import did not change Assignee information.	K1-21185
Code can now be saved in the *Notes* field of KScripts.	K1-21184
Monitoring: Create Ticket in Profile configuration did not select proper queue ID.	K1-21175
Search on *Device Issues* page did not function as expected.	K1-21169
SAML: Editing SP Metadata for `NameIDFormat` did not save changes.	K1-21139
Unexpected behavior observed when trying to map and update *Manager* field using SAML.	K1-21102
Default role for new users did not always honor the role chosen in *Settings*.	K1-21082
Alternate location for Managed Installation was not used behind a replication share.	K1-21016
Location was unassigned on asset when a new or previously removed device connects.	K1-20468
The **Generate Self-Signed Certificate** button was incorrectly enabled before the configuration information was saved in the SSL wizard.	K1-18300

Problemas conocidos

Los siguientes problemas son conocidos en el momento de esta publicación.

Problema conocido	Id. del problema
KACE Agent for SUSE 11.1 requires `libxslt` to be installed in order to install. This is a newly introduced dependency.	K1A-3813
Disk Usage history is not recorded by a macOS KACE Agent of an APFS file system.	K1A-3805
The appliance reports the MS Windows 10 build number 20H2 through its technical release version of 2009.	K1A-3803
Dell Updates: Custom View does not report any results when Smart Label is a criteria.	K1-31860
Email attachments in `.eml` and `.msg` file format are marked as *discarded* if subject contains slashes '/'.	K1-31786
Linux package upgrades: *Deploy All* can push some updates that change system configuration which requires manual reconfiguration, such as on Ubuntu 18.04LTS (Desktop version with UI).	K1-31770
KACE GO: Non-admin queue owners cannot to set ticket device/asset to arbitrary device.	K1-31764
Windows Feature Update (WFU) schedule fails when using a deployment type of *Detect and Stage* type and the Agent version is 10.2.	K1-31743
Wake-on-LAN (WoL) options are not present in the **Choose Action** menu on the *Device Detail* page for supported devices.	K1-31729
Duplicating patch schedule from list of schedules does not work as expected.	K1-31714
Duplicating Dell Updates schedule from list of schedules does not work as expected.	K1-31713
Users with no queue permissions cannot see tickets they are CC-ed on.	K1-31710
Downloading status count is not displayed in *Patch Schedules* list page.	K1-31066
Managed Installation Detail page incorrectly shows that PKG files cannot be used.	K1-30820
Patching step with reboot in *Task Chain* shows Failed status.	K1-30812
Patch schedule with On-Demand Deploy ends Task Chain task when staging is completed.	K1-30811
Patch schedule information is not showing correctly after disabling a patch schedule.	K1-30733
Schedule information is not showing correctly after disabling a Linux package upgrade schedule.	K1-30725
Pasting an image into a knowledge base article causes other pasted images to reset alignment and justification.	K1-30721

Problema conocido	Id. del problema
Package download process incorrectly updates offline *Last Modified* instead of *Last Update* status.	K1-30588
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268

Requisitos del sistema

La versión mínima requerida para instalar KACE Systems Management Appliance 11.1 es 11.0. Si su dispositivo ejecuta una versión anterior, deberá actualizarla a la versión indicada antes de continuar con la instalación.

La versión mínima requerida para actualizar el agente de KACE es la 10.2. Recomendamos ejecutar la última versión del agente con KACE Systems Management Appliance 11.1.

NOTA: El paquete RPM del agente de KACE se puede instalar en dispositivos SUSE Linux administrados solo cuando se instala el paquete `libxslt-tools` antes del paquete del agente.

Para comprobar el número de versión del dispositivo, inicie sesión en **Consola del administrador** y haga clic en **¿Necesita ayuda?** En el panel de ayuda que aparece en la parte inferior, haga clic en el botón "**i**" en un círculo.

Antes de actualizar o instalar la versión 11.1, verifique que su sistema cumpla con los requisitos mínimos. Estos requisitos están disponibles en las especificaciones técnicas de KACE Systems Management Appliance.

- Para dispositivos virtuales: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/.
- Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/.

Licencia de producto

Si actualmente posee una licencia de producto para KACE Systems Management Appliance, no se requiere una licencia adicional.

Si es la primera vez que utiliza KACE Systems Management Appliance, consulte la guía de configuración del dispositivo para ver los detalles de licencias del producto. Vaya a Más recursos para ver la guía adecuada.

NOTA: Las licencias del producto para la versión 11.1 se pueden usar solamente en KACE Systems Management Appliance de versión 11.1 o posterior. Las licencias de la versión 11.1 no se pueden utilizar en dispositivos de versiones anteriores, como la versión 10.0.

Instrucciones de instalación

Puede aplicar esta versión mediante una actualización anunciada o mediante la carga y aplicación manual de un archivo de actualización. Para obtener instrucciones, consulte los siguientes temas:

- Preparación para la actualización
- Actualización del servidor de KACE Systems Management Appliance mediante una actualización anunciada
- Carga y ejecución manual de una actualización
- Tareas posteriores a la actualización

NOTA: Para garantizar la precisión de la detección del software y los recuentos de instalación para dispositivos con un software particular, comenzando en la versión 7.0 de KACE Systems Management Appliance, el catálogo de software se reinstala con cada actualización.

Preparación para la actualización

Antes de actualizar el servidor de KACE Systems Management Appliance, siga estas recomendaciones:

- **Verifique la versión del servidor de KACE Systems Management Appliance**:

  La versión mínima requerida para instalar KACE Systems Management Appliance 11.1 es 11.0. Si su dispositivo ejecuta una versión anterior, deberá actualizarla a la versión indicada antes de continuar con la instalación.

  Para comprobar el número de versión del dispositivo, inicie sesión en **Consola del administrador** y haga clic en **¿Necesita ayuda?** En el panel de ayuda que aparece en la parte inferior, haga clic en el botón "**i**" en un círculo.

- **Verifique la versión del agente de KACE**.

  La versión mínima requerida para actualizar el agente de KACE es la 10.2. Recomendamos ejecutar la última versión del agente con KACE Systems Management Appliance 11.1.

  NOTA: El paquete RPM del agente de KACE se puede instalar en dispositivos SUSE Linux administrados solo cuando se instala el paquete `libxslt-tools` antes del paquete del agente.

- **Realice una copia de seguridad antes de empezar**.

  Realice una copia de seguridad de la base de datos y los archivos. A continuación, guárdela en una ubicación que no esté en el servidor de KACE Systems Management Appliance por si tiene que acudir a ella más adelante. Para obtener instrucciones sobre cómo realizar una copia de seguridad de la base de datos y los archivos, consulte la **Guía para el administrador**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.

- **Dispositivos instalados antes de la versión 7.0**.

  En el caso de los dispositivos instalados inicialmente antes de la versión 7.0 para los cuales no se haya recreado la imagen (dispositivos físicos) o que no se hayan reinstalado (de manera virtual), Quest Software recomienda encarecidamente exportar, volver a crear (una imagen o instalación de una máquina virtual desde un archivo OVF) y volver a importar la base de datos antes de actualizar a la versión 11.1. Para obtener más información, visite https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance.

  Si la versión de su dispositivo no corresponde a la más actualizada, se incluyeron consejos útiles acerca de la actualización en el siguiente artículo: https://support.quest.com/kace-systems-management-

appliance/kb/155574/upgrading-a-kace-systems-management-appliance-that-is-multiple-versions-behind-upgrade-path-6-x-to-10-0-.

Hay muchas razones por las que debe recrear la imagen del dispositivo. Por ejemplo, la nueva disposición del disco ofrece una mejor compatibilidad con la versión 11.1. También cuenta con seguridad y rendimiento superiores.

Para determinar si su sistema se beneficiaría de dicha actualización, puede usar un archivo `KBIN` para determinar la antigüedad exacta de su dispositivo y su diseño de disco. Para descargar el `KBIN`, visite https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report.

- **Asegúrese de que el puerto 52231 esté disponible**.

  Antes de cualquier actualización `.kbin`, el puerto 52231 debe estar disponible para que se pueda acceder a la página de la consola de actualización de KACE. Si la actualización se inicia sin que este puerto esté disponible, no podrá supervisar el progreso de la actualización. Quest KACE recomienda permitir el tráfico al dispositivo a través del puerto 52231 desde un sistema confiable y monitorear la actualización desde la consola de actualización. Sin acceso a la consola de actualización, la actualización redirige a una página inaccesible que aparece en el navegador como tiempo de espera. Esto puede hacer que una persona crea que la actualización bloqueó el sistema, lo que provoca que se reinicie el equipo cuando, en realidad, la actualización aún está en curso. Si no está seguro acerca del progreso de la actualización, comuníquese con el equipo de soporte de KACE y **no reinicie el dispositivo**.

Actualización del servidor de KACE Systems Management Appliance mediante una actualización anunciada

Puede actualizar el servidor de KACE Systems Management Appliance mediante una actualización anunciada en la página *Panel* o en la página *Actualizaciones del dispositivo* de la **Consola del administrador**.

PRECAUCIÓN: Nunca reinicie el servidor de KACE Systems Management Appliance de forma manual durante una actualización.

1. Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la **Guía para el administrador**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.
2. Vaya al *Panel de control* del dispositivo:
   - **Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.**
   - **Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://KACE_SMA_hostname/system` o seleccione Sistema en la lista desplegable de la esquina superior derecha de la página y luego haga clic en Ajustes.**
3. En la barra de navegación de la izquierda, haga clic en **Actualizaciones del dispositivo** para mostrar la página *Actualizaciones del dispositivo*.
4. Haga clic en **Comprobar actualizaciones**.

   Aparecen los resultados de la comprobación en el registro.
5. Cuando haya una actualización disponible, haga clic en **Actualizar**.

IMPORTANTE: Puede que algunos navegadores parezcan congelarse durante los primero diez minutos en que se desempaqueta y verifica la actualización. No salga de la página, no actualice la página ni haga clic en cualquiera de los botones del navegador en la página durante este tiempo, ya que estas acciones interrumpen el proceso. Después de que se desempaqueta y se verifica la actualización, aparece la página de *Registros*. No reinicie manualmente el dispositivo en cualquier momento durante el proceso de actualización.

Se aplica la versión 11.1 y se reinicia el servidor de KACE Systems Management Appliance. El progreso aparece en la ventana del navegador y en la **Consola del administrador**.

6. Cuando finalice la actualización del servidor, actualice todos sus agentes a la versión 11.1.

Carga y ejecución manual de una actualización

Si cuenta con un archivo de actualización de Quest, puede cargar ese archivo manualmente para actualizar el servidor de KACE Systems Management Appliance.

PRECAUCIÓN: Nunca reinicie el servidor de KACE Systems Management Appliance de forma manual durante una actualización.

1. Realice una copia de respaldo de la base de datos y los archivos. Para ver las instrucciones, consulte la **Guía para el administrador**, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/.
2. Con sus credenciales de inicio de sesión de cliente, inicie sesión en el sitio web de Quest en https://support.quest.com/kace-systems-management-appliance/download-new-releases, descargue el archivo `.kbin` del servidor de KACE Systems Management Appliance para la versión 11.1 GA (disponibilidad general) y guárdelo localmente.
3. En la barra de navegación de la izquierda, haga clic en **Actualizaciones del dispositivo** para mostrar la página *Actualizaciones del dispositivo*.
4. En la sección *Actualizar manualmente*:
    a. Haga clic en **Examinar** o en **Elegir archivo** y ubique el archivo de actualización.
    b. Haga clic en **Actualizar** y luego haga clic en **Sí** para confirmar.

    Se aplica la versión 11.1 y se reinicia el servidor de KACE Systems Management Appliance. El progreso aparece en la ventana del navegador y en la **Consola del administrador**.
5. Cuando finalice la actualización del servidor, actualice todos sus agentes a la versión 11.1.

Tareas posteriores a la actualización

Luego de la actualización, verifique que esta haya sido exitosa y verifique la configuración, según sea necesario.

Verificación de finalización correcta

Para verificar que la actualización se haya realizado correctamente, vea el número de la versión de KACE Systems Management Appliance.

1. Vaya al *Panel de control* del dispositivo:
    - **Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.**
    - **Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://KACE_SMA_hostname/system` o seleccione Sistema en la lista desplegable de la esquina superior derecha de la página y luego haga clic en Ajustes.**
2. Para comprobar la versión actual, haga clic en **¿Necesita Ayuda?** en la esquina superior derecha de la página y, en el panel de ayuda que aparece, en la parte inferior, haga clic en el botón **i** en un círculo.

Verificación de ajustes de seguridad

Para mejorar la seguridad, el acceso a la base de datos a través de HTTP y FTP está deshabilitado durante la actualización. Si utiliza estos métodos para acceder a los archivos de la base de datos, cambie los ajustes de seguridad luego de la actualización, según sea necesario.

1. Vaya al *Panel de control* del dispositivo:
   - **Si el componente Organización no está habilitado en el dispositivo, haga clic en Ajustes.**
   - **Si el componente Organización sí está habilitado en el dispositivo: Inicie sesión en la Consola de administración del sistema del dispositivo: `http://KACE_SMA_hostname/system` o seleccione Sistema en la lista desplegable de la esquina superior derecha de la página y luego haga clic en Ajustes.**
2. En la barra de navegación de la izquierda, haga clic en **Ajustes de seguridad** para mostrar la página *Ajustes de seguridad*.
3. En la sección superior de la página, modifique los siguientes ajustes:
   - **Habilitar archivos de copia de seguridad seguros**: desactive esta casilla de verificación para habilitar que los usuarios accedan a los archivos de copia de seguridad de la base de datos a través de una HTTP sin autenticación.
   - **Habilitar acceso a la base de datos**: seleccione esta casilla de verificación para habilitar que los usuarios accedan a la base de datos a través del puerto 3306.
   - **Habilitar copia de seguridad a través del FTP**: seleccione esta casilla de verificación para habilitar que los usuarios accedan a los archivos de copia de seguridad de la base de datos a través de un FTP.

   PRECAUCIÓN: No se recomienda la modificación de estos ajustes, ya que disminuye la seguridad de la base de datos.
4. Haga clic en **Guardar**.
5. **Solo actualizaciones KBIN**. Fortalezca el acceso al dispositivo con la contraseña raíz (2FA).
   a. En la Consola de administración del sistema, haga clic en **Ajustes** > **Soporte**.
   b. En la página de *Soporte*, en *Herramientas para la solución de problemas*, haga clic en **Autenticación de dos factores**.
   c. En la página *Autenticación de dos factores*, haga clic en **Reemplazar clave secreta**.
   d. Registre los tokens y coloque esta información en un lugar seguro.

Más recursos

Podrá encontrar información adicional a través de los siguientes recursos:

- Documentación del producto en línea (https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents)
  - **Especificaciones técnicas**: información sobre los requisitos mínimos para instalar o actualizar a la última versión del producto.

    Para dispositivos virtuales: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/.

Para KACE como servicio: vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/.

- **Guías de configuración**: instrucciones para configurar dispositivos virtuales. Vaya a https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents para ver la documentación de la última versión.
- **Guía para el administrador**: instrucciones para usar el dispositivo. Vaya a https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/ para ver la documentación de la última versión.

Globalización

Esta sección contiene información acerca de la instalación y el funcionamiento de este producto en configuraciones que no están en idioma inglés, como las que necesitan los clientes de fuera de los Estado Unidos. Esta sección no reemplaza la información acerca de plataformas y configuraciones admitidas que se encuentra en otras secciones de la documentación del producto.

Esta versión es compatible con Unicode y admite cualquier conjunto de caracteres. En esta versión, todos los componentes del producto deben estar configurados para utilizar la misma codificación de caracteres, o una compatible, y deben estar instalados para que utilicen el mismo idioma y las mismas opciones regionales. Esta versión está destinada a brindar soporte a las operaciones en las siguientes regiones: América del Norte, Europa Occidental y América Latina, Europa Central y del Este, Lejano Oriente, Japón.

La versión está localizada en los siguientes idiomas: Francés, alemán, japonés, portugués (Brasil), español.

Acerca de nosotros

Quest crea soluciones de software que hacen reales los beneficios de las nuevas tecnologías en un panorama de TI cada vez más complejo. Desde administración de bases de datos y de sistemas hasta administración de Active Directory y Office 365 y resistencia a la seguridad cibernética, Quest ayuda a los clientes a resolver su próximo desafío de TI ahora. En todo el mundo, más de 130 000 empresas y el 95 % de la lista Fortune 500 confían en Quest para disfrutar de administración y monitoreo proactivos en la próxima iniciativa empresarial, encontrar la siguiente solución para los desafíos complejos de Microsoft y mantenerse a la vanguardia ante la próxima amenaza. Quest Software. Donde convergen el futuro y el presente. Para obtener más información, visite www.quest.com.

Recursos del soporte técnico

El soporte técnico se encuentra disponible para los clientes de Quest con un contrato válido de mantenimiento y para los clientes que poseen versiones de prueba. Puede acceder al portal del Soporte de Quest en https://support.quest.com.

El portal de soporte proporciona herramientas de autoayuda que puede utilizar para resolver problemas de forma rápida e independiente, las 24 horas al día, los 365 días del año. El portal de soporte le permite:

- Enviar y gestionar una solicitud de servicio
- Consultar los artículos de la base de conocimientos
- Suscribirse a las notificaciones de productos
- Descargar documentación del software y técnica
- Ver videos de procedimientos
- Participar en debates de la comunidad
- Chatear en línea con ingenieros de soporte
- Ver servicios para ayudarlo con su producto

Avisos legales

Leyenda

PRECAUCIÓN: Un ícono de PRECAUCIÓN indica la posibilidad de daños al equipo o pérdida de datos si no se siguen las instrucciones.

IMPORTANTE, NOTA, SUGERENCIA, MÓVIL o VIDEO: Un ícono de información indica información de soporte.

Notas de la versión del dispositivo de administración de sistemas KACE

Actualizado en: abril del 2021

Versión del software: 11.1