Quest

KACE® Systemverwaltungs-Appliance 11.0

Versionshinweise

Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 11.0 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 11.0.

Über die KACE Systems Management Appliance 11.0

KACE Systems Management Appliance ist eine virtuelle Appliance, die zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset-Managements und der Service Desk-Ticketverwaltung entwickelt wurde. Weitere Informationen zur KACE Systems Management Appliance Serie finden Sie unter https://www.quest.com/products/kace-systems-management-appliance/. Diese Version enthält eine Reihe neuer Funktionen, behobener Probleme und Sicherheitsverbesserungen.

HINWEIS: Dies ist das einzige Dokument, das für diese Version übersetzt wird. Andere Handbücher wie das *Administratorhandbuch* und die produktinterne Hilfe wurden bisher nicht lokalisiert, und die Version 10.2 ist in dieser Produktversion enthalten.

Neue Funktionen und Erweiterungen

Diese Version der KACE Systems Management Appliance beinhaltet die folgenden Funktionen und Erweiterungen.

Patchen:

- **Windows-Bereitstellung nach Bedarf für Patches**: Die Appliance unterstützt einen neuen Patch-Zeitplan, mit dem Endbenutzer über ein Taskleistensymbol eine Bereitstellungsaktion auslösen können.
- **Sicherheits-Dashboard**: Ein neues *Sicherheits*- Dashboard ermöglicht ein wesentlich einfacheres Verständnis des Patch-Status der Geräte im Inventar.
- **Patch-Zeitplanassistent und Patch-Ergebnisse**: Diese Version enthält einen neuen Workflow zum Erstellen von Patch-Zeitplänen und zeigt die Patching-Ergebnisse so an, dass sie einfacher zu verstehen sind.

Gerätesicherheit

- **Verbesserungen bei der Gerätesicherheit**: In dieser Version werden Sicherheitsverbesserungen hinzugefügt, wie z. B. Quarantänemaßnahmen für Agenten, um mehr Optionen für die Sicherung der Kommunikationskanäle bereitzustellen, einschließlich der automatischen Zuweisung zu Organisationen auf der Grundlage von Token.
    - Die Appliance kann jetzt zwischen den Agenten unterscheiden, die extern (außerhalb der Firewall) verbunden sind, und denen, die eine interne Verbindung herstellen. Zusätzlich zur bereits eingestellten Verbindung zu Port 443 überwacht die Appliance für Agentenverbindungen auch Port 52230. Mithilfe einer aufgeteilten DNS-Konfiguration und der Konfiguration der Firewall zwecks

Weiterleitung des externen Ports 443 an Port 52230 auf der Appliance können Sie Agenten als interne oder externe Agenten identifizieren.

Um die Appliance dem Internet zugänglich zu machen und die Sicherheit zu maximieren, kann über Port 52230 kein Zugriff auf die Weboberfläche der Appliance erfolgen. Wenn Sie externen Zugriff auf die Web-Schnittstelle der Appliance haben möchten, konfigurieren Sie 443 auf 52230 Port nicht zur Weiterleitung auf der Firewall.
Weitere Informationen finden Sie in diesem Knowledge Base-Artikel: https://go.kace.com/to/k1000-external-agent-port.

- **Allgemeine Serversicherheits-Verbesserungen**: Die Appliance verfügt in dieser Version über mehrere Sicherheitsverbesserungen. Die Härtung der Benutzeroberfläche von Appliances zusammen mit dem Tunneling und der Quarantäne von Agenten ermöglicht eine wesentlich sicherere Bereitstellung innerhalb oder außerhalb der entmilitarisierten Zone (DMZ).

KACE GO App

- **Ticketgenehmigung**: Sie können jetzt Service Desk-Tickets in der KACE GO App genehmigen.
- **HTML-Editor**: Ein HTML-Editor wird zu den Ticketfeldern *Zusammenfassung*, *Auflösung*, und *Kommentare* hinzugefügt, um die Lesbarkeit der eingegebenen Inhalte mithilfe allgemeiner Formatierungstags zu verbessern.

Administratorkonsole

- **Eingebettete Videos**: Ab dieser Version können Sie mithilfe des Ausblendmenüs alle verfügbaren Schulungsvideos durchsuchen, die mit der aktuellen Seite verknüpft sind. Sie können ein Video im Hilfebereich, in einem kleineren Fenster außerhalb der Seite oder auf der Knowledge Base-Seite des Ziels wiedergeben, auf der das Video gehostet wird.
- **Verbesserte Navigation auf der linken Seite**: Wenn Sie ein Element im linken Fensterbereich auswählen, wird jetzt nur das Menü erweitert, ohne die Seite zu öffnen, die dem obersten Element zugeordnet ist. Sie können zum besseren Verständnis auch mehrere übergeordnete Menüs gleichzeitig erweitern.
- **Benutzerdefinierte Logos**: Vom Kunden bereitgestellte Appliance-Logos können jetzt in der Administratorkonsole und der Systemadministrationskonsole definiert werden.
- **Hintergrundfarbe für ein benutzerdefiniertes Anmeldeportal**: Die Hintergrundfarbe des Anmeldeportals kann jetzt für alle Benutzeroberflächen angepasst werden.

  HINWEIS: Die Farbauswahl wird in Internet Explorer 11 nicht unterstützt.

- **Automatische Auswahl der Organisation beim Anmelden**: Auf jede unternehmensspezifische Administratorkonsole und Benutzerkonsole kann direkt über die virtuelle IP- oder Hostnamenkonfiguration zugegriffen werden. Dadurch können Benutzer die Auswahl der Organisation bei der Anmeldung umgehen.

Service Desk

- **Verbesserungen von Ticketvorlagen**: Den Service Desk-Ticketvorlagen wird ein neues Layout wird hinzugefügt, damit Sie den Inhalt des Tickets besser organisieren können, wenn die Vorlage Felder in variabler Höhe enthält. Sie können den Inhalt des Tickets auch mithilfe eines Trennzeichens in separate Abschnitte aufteilen.
- **Eingebettete Bilder und Screenshots in Ticketfeldern**: Sie können jetzt Bilder und Screenshots in die Felder *Zusammenfassung* und *Kommentare* aufnehmen, um Probleme im Zusammenhang mit Tickets besser zu kommunizieren.
- **Verknüpfung „Nimm dieses Ticket“**: Die Listenseite *Tickets* verfügt über eine neue Steuerung, mit der Sie sich schnell ein Ticket zuweisen können.
- **Verbesserungen von Prozesstickets**: Sie können für eine vorhandene Prozessvorlage ein Prozessticket schnell per E-Mail erstellen, indem Sie den Namen der Prozessvorlage im Feld *Betreff* angeben. Sie können auch festlegen, dass Ticketprozesse nach einem bestimmten wiederkehrenden Zeitplan beginnen.

HINWEIS: In früheren Versionen konnten Sie mit Ticketarchivierungsplänen die Option *Keine* als Zeitplanoption auswählen. Jene Option wird in dieser Version entfernt. Wenn Sie zuvor Zeitpläne für die Ticketarchivierung mit dieser Option verwendet haben, werden diese nach dem Upgrade automatisch aktualisiert und täglich ausgeführt.

Weitere Funktionen

- **Updates für den Anmeldeinformationen-Manager**: LDAP-Labelkonfigurationen können jetzt den Anmeldeinformationen-Manager zum Speichern und Freigeben von Anmeldeinformationen verwenden.
- **Skripte können zu Kategorien hinzugefügt werden**: Jedes Skript kann nach einer zugewiesenen benutzerdefinierten Kategorie sortiert oder gefiltert werden.
- **Neue VMware-Widgets auf dem Bestandsaufnahme-Dashboard**: Die folgenden Widgets werden zum *Bestandsaufnahme*-Dashboard hinzugefügt: VMware Device Counts, VMware ESXi Version Counts, VMware Device Reports, and VMware ESXi Device By Status.
- **Neue OS-Unterstützung**: Diese Version unterstützt MacOS 10.16 und CentOS.

HINWEIS: *Charlie Root*-E-Mails, die von der Appliance generiert wurden, enthielten keine nützlichen Informationen und führten oft zu Verwirrung. Aus diesem Grund werden diese E-Mails nicht mehr generiert und an den Administrator gesendet.

Enhancements

The following is a list of enhancements implemented in this release.

Enhancement	Issue ID
It was not possible to allow Credentials specific access through Roles.	K1-20924
FTP/SFTP offboard backup improved performance and Public Key Authentication for SFTP.	ESMP-7444
Managed OS widget in Dashboard did not display version number.	ESMP-6448
Customize User Fields is now accessible through the *Choose Action* menu on the *Users* list page.	ESMP-6113
It was not possible to reset history settings to default values.	ESMP-5916
Agentless support for vSphere 7.0 is added in this release.	ESMEC-3557

Behobene Probleme

TIm Anschluss finden Sie eine Liste mit Problemen, die in dieser Version behoben wurden.

Behobenes Problem	ID des Problems
Offline appliance could not to run patch detects with `version-check` failed errors.	K1-21171
Workspace ONE Discovery/Inventory did not respect user domain provided in the credentials.	K1-21145

Behobenes Problem	ID des Problems
Windows Feature Update could report that it was not applicable because user locale is set as non-English.	K1-21101
Unknown user rejection email was not be sent in some cases.	K1-21081
POP3: Failure to process one email could prevent further emails from being processed.	K1-21077
Reset tries in the Windows Feature Update Catalog Detail page did not work as expected.	K1-21074
Ticket load time performance was sometimes degraded with many associated child tickets.	K1-21073
Replication Share Inventory did not run after regular agent inventory in some cases.	K1-21070
When using Office 365 with `OAuth`, an Invalid header value detected message could be seen when the display name contains Unicode characters.	K1-21066
Some Dell Updates did not appear in the list of available updates in the Administrator Console, even though they did exist on the appliance.	K1-21053
Service Desk Templates: Conditional Logic involving Owner and null usage did not work as expected.	K1-21050
Windows Feature Update could fail on lower specification systems if any of the individual steps during the update itself exceeded the global agent process time out set in the appliance.	K1-21048
Hyperlink to archived/merged tickets was sometimes incorrect, causing an error.	K1-21043
Re-enabling appliance backups could give an incorrect error message.	K1-21041
An email sent to a Service Desk queue with multiple addresses in the *To* line could produce unexpected results.	K1-21036
The ` ` character was not decoded correctly in Gmail messages when using `OAuth`.	K1-21035
MSG files uploaded to Attachment type Asset Fields open in browser instead of downloading.	K1-21033
Windows Feature Update payload files for unsubscribed locales could be incorrectly downloaded.	K1-21031
Asset Import schedule creation or modification inserted blank/duplicate rows in `IM_CRON`.	K1-21026
SFTP full path was not retained when editing an existing asset import schedule.	K1-21015

Behobenes Problem	ID des Problems
With multiple NICs, using Add to SDA Boot Action on a device sometimes did not work as expected.	K1-21011
K1000 Discovery Completed email is missing the schedule name in the body.	K1-21010
The *Patch Schedule* page did not prompt the user to save when clicking **Run Now**, after changing the device label.	K1-21009
An error page appeared while trying to save a blank Mac profile without a configuration.	K1-21004
When creating a new Organization, incorrect date for *Last updated* was displayed.	K1-21003
The appliance generated spurious `Charlie Root` emails which did not contain useful information.	K1-21001
Adding the `related_tickets` shaping option to fetch ticket list API call did not work as expected	K1-20994
Windows Feature Update schedule sometimes had incorrect Build section if no Windows Feature Update signatures were downloaded.	K1-20985
LDAP labels could not be applied at login for Security Assertion Markup Language (SAML) accounts.	K1-20978
An error displayed while using description as a Smart Label criteria on the *Patch Catalog* list page.	K1-20975
Dell Warranty not updated when `PARENT_SERVICE_TAG` was null.	K1-20972
The *Smart Labels* list page was missing the *View By* filter.	K1-20968
Primary Device is not automatically set when a user submits a ticket.	K1-20966
The *Manage Associated Labels* dialog box search only had "begins with" type searching.	K1-20963
When Access Control List blocked access to the Administrator Console, SAML did not work for the User Portal.	K1-20958
Comment appended to Service Desk parent ticket on last child close was missing the ticket ID.	K1-20954
Using a custom date time format for monitoring failed when microseconds were part of the timestamp.	K1-20952
Kbot script task of creating a message window displayed the snooze option that was not used.	K1-20946
SDA Deployment Time was missing the UTC offset.	K1-20931

Behobenes Problem	ID des Problems
Microsoft Surface devices were being classified incorrectly as virtual devices.	K1-20929
It was not possible to hide the *Location* field on *License* Asset Type	K1-20923
Default CC was not added to `CC_List`, resulting in ticket not showing in the ticket list.	K1-20922
AirWatch/Workspace ONE: auto-provisioning duplicated devices without a MAC address.	K1-20915
Sending email to ticket that queue owner did not own prevented them from being added to the CC list.	K1-20899
`RegistryValue`-related custom inventory rule was not evaluated correctly for numeric values that exceeded max unsigned integer value.	K1-20893
When setting ticket *Due Date* to *Always Required*, the default option did not force the date to be selected.	K1-20890
Using the *Download Status* did not list patches with multiple files when not all of them were applicable.	K1-20869
Managed Installation (MI) sort by date (*Created* or *Modified*) incorrectly sorted by the first digit only.	K1-20801
It was not possible to add or delete a manual label if a device did not have an associated asset.	K1-20776
IP Address sorting was not working as expected on the *Devices* list page.	K1-20756
Custom ticket fields: Setting the user type to *Always Required* did not prevent the ticket from being saved.	K1-20755
Operating system name was missing in tracked history while selecting OS on the *Replication* list page.	K1-20711
Link was missing for the Patch Schedule name on the *Object History* list page.	K1-20706
Replication sometimes failed to copy all files when the replicating Agent runs on a Mac OS or Linux.	K1-20691
Asset History check boxes could clear when canceling and saving.	K1-20684
Scheduled Report emailed empty files when the reports temporary directory was too large.	K1-20675
Export All on the *Devices* list page *Choose Action* menu ran out of memory with a large number of devices.	K1-20672
Single select field with quote wrapped items including commas were split by the comma in KACE GO, preventing tickets from being saved.	K1-20668

Behobenes Problem	ID des Problems
On the *Queue Detail* page, under *Archive Preferences*, the **Run Now** button allowed multiple clicks, causing unexpected results.	K1-20658
Archive purge never occurred if *Archive schedule* was set to *None*.	K1-20657
If inventory contains an emoji character (for example, in a file name), the appliance failed to parse the inventory properly.	K1-20649
Fields exported from the *Devices* list page did not include all options.	K1-20631
The `RegistryValueReturn` custom inventory rule was not evaluated correctly for values under `HKCurrentUser` on non-English OS.	K1-20622
Single sign-on with Azure AD could cause synchronization failures.	K1-20585
The *Assets by Location* widget showed inaccurate percentages.	K1-20565
Unwanted history was tracked in the *Relay Machine* field while trying to create or modify any agentless devices.	K1-20486
Custom User fields with a *Required* flag were not handled properly during LDAP import.	K1-20389
Organization LDAP Filter test could fail due to improper variable or wildcard substitution.	K1-20333
Under *Asset History Configuration*, clearing the boxes related to *Connection* and **Disconnection** did not prevent those entries from being logged.	K1-20307
A date in a Provisioning schedule name could result in an error when accessing the *Search Scripting Logs* tab.	K1-20256
The *Device* detail page performance could be affected (or the page may fail to load) due to a large number of associated asset history records.	K1-19881
The *Last Update* column on the *Patch Schedule* list page did not sort correctly.	K1-19777
The KACE Agent could not extract zip files larger than 5 GB, created using the MS Windows Explorer's built in ZIP mechanism.	K1-17274
Scripts created through the MSI policy wizard did not work for software inside a ZIP file.	K1-17264
Asset History: Clearing field selections did not clean up the `ASSET_HISTORY` table.	ESMP-7504
If 2FA was enabled on the appliance, *Import Managed Installations* could not work as expected.	ESMP-7120
KACE Cloud Mobile Device Manager was not passing the correct license value if the device was not enrolled.	ESMEC-3838

Behobenes Problem	ID des Problems
KACE Cloud Mobile Device Manager/KACE hybrid agent would get stuck if the agentless record is deleted during agentless provisioning.	ESMEC-3837
The KACE menu application did not load the correct system locale when locale changed.	ESMEC-3765
Multiple `explorer.exe` processes on Windows caused launch in active desktop and launch in sessions to misbehave.	ESMEC-3529
`GET` calls to obtain work item associated to a ticket sometimes did not work as expected.	ESMAS-4891
Using the API, administrators can now move tickets to another queue.	ESMAS-4888
In KACE GO app, when a device or machine is a required field, this did not appear when a user created a ticket, resulting in the `Missing required field` error.	ESMAS-4843
Moving parent ticket to a new process type bypassed approvals.	ESMAS-4758
Bold formatting did work in HTML editor (such as response templates or ticket entries) in some browsers and operating systems.	ESMAS-4619
Rolling back product suite patches could sometimes remove only one of the available components such as on Office 2016.	ESMAM-2722

Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

Bekanntes Problem	ID des Problems
Asset Import does not change Assignee information.	K1-21185
Inserting code snippets or other unexpected characters in a script's note may cause an error.	K1-21184
User Custom Fields may not be listed in the Column selector drop-down in the *Users* list page.	K1-21179
Offline KScripts do not run when scheduled for *Run on the* instance/day of week.	K1-21173
The **Reset Tries** button in the *Windows Feature Update Status* section on the *Device Detail* page may not work.	K1-21172
Parent ticket appears to be in process when child tickets are closed from *Tickets* list view.	K1-21143
Response Templates marked public are only editable by the creator.	K1-21130

Bekanntes Problem	ID des Problems
Unexpected behavior observed when trying to map and update the Manager field using SAML.	K1-21102
POP3 and IMAP cannot use self-signed certificates for inbound email.	K1-21086
Invalid filters (Smart Labels) can be saved, resulting in Smart Labels that never populate.	K1-20268
An error may be seen while creating custom view on the *Quarantine* page in the Systemverwaltungskonsole.	ESMP-7825
On the *Agent Tokens* list page, in the **Choose Action** menu, selecting **Create Report** does not work as expected.	ESMP-7799
In the Systemverwaltungskonsole, the *Agent Token Detail* page displays the organization ID instead of the name.	ESMP-7793
Device links on the *Agent Command Queue* and *Agent Task Status* pages may not function as expected.	ESMP-7774
Do not associate file Managed Installation option does not display correctly after saving.	ESMP-7753
Token Usage by Machine record is not updated when machine changes token or is removed from list.	ESMP-7588
Recurring alert messages keep spawning new windows on the device.	ESMEC-3913
Wake-on-LAN (WoL) through relay does not display error when the relay agent selected is down.	ESMEC-3898
Monitoring can fail with error in the Mac OS 11 system log because it has multi-line entries in `system.log`.	ESMEC-3883
Existing Patch Schedule name is allowed when duplicating the schedule.	ESMAM-2863
In KACE GO, any ticket attachments past the fifth on a single comment are not saved correctly.	ESMAS-5006

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 11.0 ist 10.2. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Für ein Upgrade des KACE Agenten ist mindestens Version 9.0 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE Systems Management Appliance 11.0.

Um die Versionsnummer der Appliance zu überprüfen melden Sie sich bei der Administratorkonsole an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

Vergewissern Sie sich vor der Aktualisierung auf Version 11.0, dass das System die Mindestanforderungen erfüllt. Diese Anforderungen werden in den technischen Daten der KACE Systems Management Appliance erläutert.

- Virtuelle Appliances: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-virtual-appliances/.
- KACE als Dienst: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-kace-as-a-service/.

Produktlizenzierung

Falls Sie derzeit eine KACE Systems Management Appliance Produktlizenz besitzen, ist keine zusätzliche Lizenz erforderlich.

Wenn Sie die KACE Systems Management Appliance zum ersten Mal verwenden, finden Sie ausführliche Informationen zur Produktlizenzierung im Handbuch zur Appliance-Einrichtung. Das entsprechende Handbuch finden Sie unter Weitere Ressourcen.

HINWEIS: Produktlizenzen für Version 11.0 können nur für KACE Systems Management Appliance mit Version 11.0 oder höher verwendet werden. Lizenzen für Version 11.0 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 9.0 ausgeführt werden.

Installationsanweisungen

Sie können diese Version mit einer mitgeteilten Aktualisierung oder durch das manuelle Hochladen und Anwenden einer Aktualisierungsdatei anwenden. Anweisungen hierzu finden Sie in den Abschnitten zu den folgenden Themen:

- Aktualisierung vorbereiten
- Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung
- Eine Aktualisierung manuell hochladen und anwenden
- Aufgaben nach der Aktualisierung

HINWEIS: Um die Genauigkeit der Softwareerkennung und Installationszahlen für Geräte mit einer bestimmten Software ab Version 7.0 sicherzustellen, wird der Softwarekatalog bei jedem Upgrade neu installiert.

Aktualisierung vorbereiten

Befolgen Sie vor der Aktualisierung Ihres KACE Systems Management Appliance Servers die folgenden Empfehlungen:

- **Überprüfen Sie die Serverversion Ihrer KACE Systems Management Appliance**:

  Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 11.0 ist 10.2. Wenn auf Ihrer Appliance eine frühere Version ausgeführt wird, müssen Sie eine Aktualisierung auf die angegebene Version durchführen, bevor Sie die Installation fortsetzen können.

Um die Versionsnummer der Appliance zu überprüfen melden Sie sich bei der Administratorkonsole an und klicken Sie auf **Hilfe**. Klicken Sie auf der angezeigten Hilfefeld auf die umkreiste Schaltfläche „**i**“.

- **Überprüfen Sie die KACE Agentenversion**.

  Für ein Upgrade des KACE Agenten ist mindestens Version 9.0 erforderlich. Wir empfehlen die Ausführung der neuesten Agentversion mit KACE Systems Management Appliance 11.0.

- **Führen Sie eine Sicherung durch, bevor Sie beginnen**.

  Sichern Sie Ihre Datenbank und Ihre Dateien und legen Sie diese für spätere Zwecke an einem Speicherort außerhalb des KACE Systems Management Appliance Servers ab. Anweisungen zur Sicherung Ihrer Datenbank und Ihrer Dateien finden Sie im Administratorhandbuch, https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/.

- **Vor Version 7.0 installierte Appliances**.

  Bei Appliances, die ursprünglich vor Version 7.0 installiert wurden und für die noch kein neues Image (physische Appliances) erstellt wurde oder die noch nicht neu installiert wurden (virtuell), empfiehlt Quest Software dringend, die Datenbank zu exportieren, neu zu erstellen (über ein Image oder die Installation einer virtuellen Maschine über eine OVF-Datei) und vor der Aktualisierung auf Version 11.0 neu zu importieren. Weitere Informationen hierzu finden Sie unter https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance.

  Wenn Ihre Appliance-Version mehrere Versionen umfasst, finden Sie im folgenden Artikel nützliche Tipps zur Aktualisierung: 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-.

  Die Appliance über ein Image neu zu erstellen bietet zahlreiche Vorteile. Das neue Laufwerk-Layout bietet beispielsweise eine verbesserte Kompatibilität mit Version 11.0. Zudem profitieren Sie von Verbesserungen bei Sicherheit und Leistung.

  Um festzustellen, ob Ihr System von einer solchen Aktualisierung profitieren würde, können Sie eine `KBIN`-Datei verwenden, um das genaue Alter Ihrer Appliance und das Festplattenlayout zu bestimmen. `KBIN` können Sie unter https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report herunterladen.

- **Stellen Sie sicher, dass Port 52231 verfügbar ist**.

  Vor einem `.kbin`-Upgrade muss Port 52231 verfügbar sein, damit die Seite KACE Upgrade-Konsole zugänglich ist. Wenn das Upgrade initiiert wird, ohne diesen Port verfügbar zu machen, können Sie den Fortschritt des Upgrades nicht verfolgen. Quest KACE empfiehlt dringend, Datenverkehr von einem vertrauenswürdigen System über Port 52231 zuzulassen und das Upgrade von der Upgrade-Konsole aus zu überwachen. Ohne Zugriff auf die Upgrade-Konsole wird das Upgrade zu einer Seite umgeleitet, auf die nicht zugegriffen werden kann, was im Browser als Timeout angezeigt wird. Dies kann den Anschein vermitteln, dass das Upgrade das System zum Absturz gebracht hat, woraufhin häufig der Kasten neu gestartet wird, obwohl das Upgrade noch ausgeführt wird. Wenn Sie sich nicht sicher sind, wie weit das Upgrade fortgeschritten ist, wenden Sie sich an den KACE-Support und **starten Sie die Appliance nicht neu**.

Aktualisieren des KACE Systems Management Appliance Servers mit einer beworbenen Aktualisierung

Sie können den KACE Systems Management Appliance mithilfe einer Aktualisierung aktualisieren, die auf der Seite *Dashboard* oder *Appliance-Aktualisierungen* der Administratorkonsole zur Verfügung gestellt wird.

VORSICHT: Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE Systems Management Appliance Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im Administratorhandbuch (https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/).
2. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Klicken Sie auf **Überprüfen**, ob aktuelle Versionen verfügbar sind.

   Die Ergebnisse der Überprüfung werden im Protokoll angezeigt.
5. Wenn eine Aktualisierung verfügbar ist, klicken Sie auf **Aktualisieren**.

   WICHTIG: Während der ersten 10 Minuten stürzen einige Browser scheinbar ab, während die Aktualisierung entpackt und überprüft wird. Verlassen oder aktualisieren Sie die Seite während dieses Zeitraums nicht und klicken Sie nicht auf Browserschaltflächen auf der Seite, da diese Aktionen den Vorgang unterbrechen würden. Nachdem die Aktualisierung entpackt und überprüft wurde, wird die Seite *Protokolle* angezeigt. Starten Sie die Appliance während des Aktualisierungsvorgangs nicht manuell neu.

   Die Version 11.0 wird angewandt und der KACE Systems Management Appliance Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.
6. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 11.0.

Eine Aktualisierung manuell hochladen und anwenden

Wenn Sie eine Aktualisierungsdatei von Quest erhalten haben, können Sie diese manuell hochladen, um den KACE Systems Management Appliance Server zu aktualisieren.

VORSICHT: Während einer Aktualisierung dürfen Sie keinen manuellen Neustart des KACE Systems Management Appliance Servers durchführen.

1. Sichern Sie Ihre Datenbank und die entsprechenden Dateien. Anweisungen hierzu finden Sie im Administratorhandbuch (https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/).
2. Melden Sie sich mit Ihren Kundenanmeldeinformationen auf der Quest Website an: https://support.quest.com/kace-systems-management-appliance/download-new-releases. Laden Sie die `KBIN`-Datei des KACE Systems Management Appliance Servers für die allgemein verfügbare Version 11.0 GA (general availability, Allgemeine Verfügbarkeit) herunter und speichern Sie sie lokal.
3. Klicken Sie auf der linken Navigationsleiste auf **Appliance-Aktualisierungen**, um die Seite *Appliance-Aktualisierungen* anzuzeigen.
4. Im Abschnitt *Manuell aktualisieren*:
   a. Klicken Sie auf **Durchsuchen** oder auf **Datei auswählen** und suchen Sie nach der Aktualisierungsdatei.
   b. Klicken Sie auf **Aktualisieren** und zur Bestätigung auf **Ja**.

Die Version 11.0 wird angewandt und der KACE Systems Management Appliance Server wird neu gestartet. Der Bearbeitungsstatus wird im Browserfenster und in der Administratorkonsole angezeigt.

5. Wenn das Server-Upgrade abgeschlossen ist, aktualisieren Sie alle Agenten auf Version 11.0.

Aufgaben nach der Aktualisierung

Überprüfen Sie im Anschluss an die Aktualisierung, ob diese erfolgreich war und die richtigen Einstellungen festgelegt sind.

Erfolgreichen Abschluss überprüfen

Überprüfen Sie den erfolgreichen Abschluss, indem Sie die KACE Systems Management Appliance Versionsnummer kontrollieren.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.
2. Um die aktuelle Version zu überprüfen, klicken Sie oben rechts auf der Seite auf **Hilfe**, und klicken Sie anschließend im angezeigten Hilfefeld unten auf die umkreiste Schaltfläche **i**.

Sicherheitseinstellungen überprüfen

Zur Erhöhung der Sicherheit wird während der Aktualisierung der Datenbankzugriff per HTTP und FTP deaktiviert. Wenn Sie mithilfe dieser Methoden auf Datenbankdateien zugreifen, ändern Sie die Sicherheitseinstellungen nach der Aktualisierung entsprechend.

1. Navigieren Sie zur *Systemsteuerung* der Appliance:
   - Wenn die Organisationskomponente auf der Appliance nicht aktiviert ist, klicken Sie auf **Einstellungen**.
   - Wenn die Organisationskomponente auf der Appliance aktiviert ist: Melden Sie sich an der Systemverwaltungskonsole der Appliance an: `http://`KACE_SMA_hostname`/system`. Oder wählen Sie rechts oben auf der Seite aus der Dropdown-Liste die Option **System** aus und klicken Sie dann auf **Einstellungen**.
2. Klicken Sie auf der linken Navigationsleiste auf **Sicherheitseinstellungen**, um die Seite *Sicherheitseinstellungen* anzuzeigen.
3. Ändern Sie im oberen Bereich der Seite die folgenden Einstellungen:
   - **Aktivieren von „Sicherungsdateien sichern“**: Deaktivieren Sie dieses Kontrollkästchen, damit Benutzer per HTTP ohne Authentifizierung auf Datenbanksicherungsdateien zugreifen können.
   - **Datenbankzugriff aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer über Port 3306 auf die Datenbank zugreifen können.
   - **Sicherung über FTP aktivieren**: Aktivieren Sie dieses Kontrollkästchen, damit Benutzer per FTP auf Datenbanksicherungsdateien zugreifen können.

VORSICHT: Die Änderung dieser Einstellungen verringert die Sicherheit der Datenbank und wird aus diesem Grund nicht empfohlen.

4. Klicken Sie auf **Speichern**.
5. **Nur KBIN-Upgrades**. Erschweren Sie den Zugriff auf Root-Kennwort (2FA) für die Appliance.
    a. Klicken Sie in der Systemverwaltungskonsole auf **Einstellungen** > **Support**.
    b. Klicken Sie auf der Seite *Support* unter *Problembehebungstools* auf **Zweifaktor-Authentifizierung**.
    c. Klicken Sie auf der Seite *System unterstützt Zweifaktor-Authentifizierung* auf **Geheimen Schlüssel ersetzen**.
    d. Notieren Sie die Token und bewahren Sie diese Informationen an einem sicheren Ort auf.

Weitere Ressourcen

Zusätzliche Informationen erhalten Sie in den folgenden Ressourcen:

- Online-Produktdokumentation (https://support.quest.com/kace-systems-management-appliance/11.0/technical-documents)
    - **Technische Daten**: Informationen zu den Mindestanforderungen bei der Installation der bzw. Aktualisierung auf die aktuelle Version des Produkts.

      Virtuelle Appliances: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-virtual-appliances/.
      KACE als Dienst: Weitere Informationen finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/technical-specifications-for-kace-as-a-service/.
    - **Einrichtungshandbücher**: Anweisungen zum Einrichten virtueller Appliances. Die Dokumentation der neuesten Version finden Sie unter https://support.quest.com/kace-systems-management-appliance/11.0/technical-documents.
    - **Administratorhandbuch**: Anweisungen zur Verwendung der Appliance. Die Dokumentation der neuesten Version finden Sie unter https://support.quest.com/technical-documents/kace-systems-management-appliance/11.0-common-documents/administrator-guide/.

Globalisierung

Dieser Abschnitt enthält Informationen zum Installieren und Verwenden dieses Produkts in nicht englischsprachigen Konfigurationen (beispielsweise für Kunden außerhalb Nordamerikas). Dieser Abschnitt ersetzt nicht die anderen Angaben zu unterstützten Plattformen und Konfigurationen in der Produktdokumentation.

Diese Version ist für Unicode aktiviert und unterstützt alle Zeichensätze. In dieser Version sollten alle Produktkomponenten für die Verwendung derselben oder kompatibler Zeichenkodierungen konfiguriert und so installiert werden, dass sie dieselben Gebietsschema- und Regionsoptionen verwenden. Diese Version unterstützt die Verwendung in folgenden Regionen: Nordamerika, Westeuropa und Lateinamerika, Mittel- und Osteuropa, Fernost (Asien), Japan.

Diese Version wurde für die folgenden Sprachen lokalisiert: Französisch, Deutsch, Japanisch, Portugiesisch (Brasilien), Spanisch.

Über uns

Quest entwickelt Softwarelösungen, die sich die Vorteile neuer Technologien bei einer immer komplexer werdenden IT-Infrastruktur zu Nutze machen. Von der Datenbank- und Systemverwaltung über Active Directory- und Office 365-Verwaltung bis hin zur Erhöhung der Widerstandskraft gegen Cyberrisiken unterstützt Quest Kunden bereits jetzt bei der Bewältigung ihrer nächsten IT-Herausforderung. Weltweit verlassen sich mehr als 130.000 Unternehmen und 95 % der Fortune 500-Unternehmen auf Quest, um proaktive Verwaltung und Überwachung für die nächste Unternehmensinitiative bereitzustellen, die nächste Lösung für komplexe Microsoft-Herausforderungen zu finden, und der nächsten Bedrohung immer einen Schritt voraus zu sein. Quest Software. Wo die Zukunft auf die Gegenwart trifft. Weitere Informationen hierzu finden Sie unter www.quest.com.

Ressourcen für den technischen Support

Der technische Support steht Quest Kunden mit gültigem Servicevertrag sowie Kunden mit Testversionen zur Verfügung. Auf das Quest Support Portal können Sie unter https://support.quest.com/de-de/ zugreifen.

Im Support-Portal finden Sie Tools zur Selbsthilfe, mit denen Probleme rund um die Uhr schnell und selbständig gelöst werden können. Das Support-Portal bietet folgende Möglichkeiten:

- Einreichen und Verwalten einer Serviceanfrage
- Anzeigen von Knowledge Base-Artikeln
- Registrieren für Produktbenachrichtigungen
- Herunterladen von Software und technischer Dokumentation
- Anzeigen von Anleitungsvideos
- Teilnehmen an Community-Diskussionen
- Online Chatten mit Supporttechnikern
- Anzeigen von Services, die Sie bei Ihrem Produkt unterstützen können

Rechtliche Hinweise

© 2020 Quest Software Inc. ALL RIGHTS RESERVED.

This guide contains proprietary information protected by copyright. The software described in this guide is furnished under a software license or nondisclosure agreement. This software may be used or copied only in accordance with the terms of the applicable agreement. No part of this guide may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Quest Software Inc.

The information in this document is provided in connection with Quest Software products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Quest Software products. EXCEPT AS SET FORTH IN THE TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT, QUEST SOFTWARE ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL QUEST SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF QUEST SOFTWARE HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Quest Software makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Quest Software does not make any commitment to update the information contained in this document.

If you have any questions regarding your potential use of this material, contact:

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

Refer to our Web site (https://www.quest.com) for regional and international office information.

Patente

Quest Software ist stolz auf seine fortschrittliche Technologie. Für dieses Produkt können Patente bzw. Patentanmeldungen bestehen. Aktuelle Informationen zum bestehenden Patentschutz für dieses Produkt finden Sie auf unserer Website unter https://www.quest.com/legal.

Trademarks

Quest, the Quest logo, Join the Innovation, and KACE are trademarks and registered trademarks of Quest Software Inc. For a complete list of Quest marks, visit https://www.quest.com/legal/trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legende

VORSICHT: Das Symbol VORSICHT weist auf eine mögliche Beschädigung von Hardware oder den möglichen Verlust von Daten hin, wenn die Anweisungen nicht befolgt werden.

WICHTIG, HINWEIS, TIPP, MOBIL oder VIDEO: Ein Informationssymbol weist auf ergänzende Informationen hin.

KACE Systems Management Appliance – Versionshinweise

Letzte Überarbeitung: Oktober 2020

Software-Version: 11.0