KACE® Systemverwaltungs-Appliance 12.0

Versionshinweise

Inhaltsverzeichnis

Quest® KACE® Systems Management Appliance 12.0 – Versionshinweise

Dieses Dokument enthält Informationen zur KACE Systems Management Appliance Version 12.0.

Über die KACE Systems Management Appliance 12.0

KACE Systems Management Appliance wurde zur Automatisierung der Geräteverwaltung, der Anwendungsbereitstellung, des Patchings, des Asset-Managements und der Service Desk-Ticketverwaltung entwickelt. 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.

Neue Funktionen

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

Infrastruktur

- **Support für Azure und AWS S3 Speicher**: Sie können die Appliance jetzt so konfigurieren, dass sie cloudbasierte Offboard-Backups wie die Microsoft Azure Blob und Amazon S3 Speicher verwendet. Hierfür ist ein Konto für MS Azure oder Amazon S3 Speicher erforderlich.
- **Möglichkeit zur Änderung des Admin-Benutzernamens**: Wenn Ihre Umgebung mehrere Appliances umfasst, können Sie für Compliance mit Ihren Sicherheitsrichtlinien regelmäßige administrative Änderungen vereinfachen und beschleunigen. Der Name des Standard-Administratorkontos kann leicht geändert werden. Seien Sie jedoch vorsichtig, wenn Sie den Benutzernamen und das Kennwort des Administratorkontos ändern. Die Anmeldenamen und Kennwörter für das `admin`-Konto auf allen

verknüpften Appliances und Organisationen müssen gleich sein, wenn Sie über die Dropdown-Liste in der Ecke oben rechts zwischen diesen wechseln möchten.

- **Verbesserte Administratoren-Sicherheit**: Das lokale `admin`-Konto kann jetzt bei Bedarf deaktiviert oder umbenannt werden.
- **Ändern der Standardkonfigurations-Kennwörter**: Ab dieser Version können Sie die Kennwörter der Standard-Dienstkonten wie beispielsweise `konfig`/`konfig` und `netdiag`/`netdiag` leicht ändern.
- **Verbesserte Skalierbarkeit**: Mit der Appliance können Sie jetzt bis zu 50.000 Geräte mit der Standardkonfiguration verwalten.
- **FreeBSD 12.2**: FreeBSD, das im Lieferumfang der Appliance enthalten ist, wurde auf Version 12.2 aktualisiert, die eine Reihe von Sicherheitsempfehlungen umsetzt.
- **LDAP/SAML für die System-Verwaltungskonsole**: Die LDAP-Unterstützung wurde nun auf die **Systemverwaltungskonsole** erweitert. Sie ermöglicht einem Benutzer, über ein LDAP-Profil auf die **Systemverwaltungskonsole** zuzugreifen und als Administrator mit vollständigen Lese-/Schreibberechtigungen auf die **Administratorkonsole** der einzelnen Organisationen zuzugreifen.
- **Verbesserte Assistenten für Ersteinrichtung**: Mit dem Assistenten für die *Ersteinrichtung* können Sie nun die Gerätedaten aus einem Backup wiederherstellen und die Netzwerkkonfiguration nach Bedarf neu einstellen.
- **Möglichkeit zum Ausschließen von Netzwerkeinstellungen von einem Wiederherstellungsjob**: Backup-, Wiederherstellungs- und Migrationsprozesse werden häufig in mehreren Umgebungen ausgeführt, z. B. in Test- und Entwicklungsumgebungen. Es ist häufig erforderlich, dass Ziel- und Zielgeräte online bleiben. Der Wiederherstellungsvorgang hat jetzt die Möglichkeit, Netzwerkeinstellungen auszuschließen, sodass der Geräteadministrator ausgewählte Geräte online halten kann.
- **Support für Nutanix**: Die Appliance kann jetzt auf Nutanix gehostet werden. Beachten Sie, dass der Support für Nutanix für Gasttools unter FreeBSD derzeit nicht unterstützt wird, sodass bestimmte Nutanix-Funktionen wie VSS (Snapshot), Self-Service Restore und VM Mobility nicht verfügbar sind.

Gerätekommunikation

- **Nativer CPU-Agent der M1-Serie für macOS**: Ab dieser Version kann der KACE Agent nativ auf Apple Silicon(M1)-Chips ausgeführt werden.

Service Desk

- **Vorschlagen von Artikeln aus der Knowledge Base bei der Ticketerstellung**: Während Sie ein Ticket beim Service Desk erstellen, wird eine Liste mit empfohlenen Artikeln aus der Knowledge Base basierend auf den im Ticket bereitgestellten Informationen angezeigt.

  Ticket Import Tool: Die Appliance verfügt jetzt über eine benutzerdefinierte Mapping-Funktion zum Import von Tickets aus externen Systemen. So können Sie Ihre Tickets problemlos von einem anderen System migrieren.

Verbesserungen

Nachfolgend finden Sie eine Liste von in dieser Version implementierter Verbesserungen.

HINWEIS: Die Appliance-API unterstützt jetzt API-Clients, die bei der Kommunikation mit der Appliance `x-kace-api-version`- und `x-kace-csrf-token`-Header verwenden. Ältere Clients, die `x-dell-api-version` und `x-dell-csrf-token` verwenden, werden jedoch weiterhin unterstützt, solange sie den `x-dell-api-version`-Anforderungsheader in der Anmeldeanforderung enthalten. Bitte beachten Sie, dass die Kommunikationsmethode mit den alten Dell-Headern mittlerweile veraltet ist und in einer zukünftigen Version entfernt werden wird.

Verbesserung	ID des Problems
KACE Agent is supported natively for macOS devices with Apple silicon chip.	K1A-3783
KACE Agent system tray shortcuts now support a list of default KACE specific replacement variables.	K1A-707
KACE Agent only supports 64-bit Linux operating systems for RHEL, Ubuntu, SUSE, and CentOS.	K1-31940
Patch status now changes to *Active* if a previously superseded patch is no longer superseded.	K1-31917
Global Administrator role is added to the **Systemverwaltungskonsole**.	K1-31910
Last inventory processing time for each device is now available on the *Device Details* page.	K1-31828
Samba-enabled boxes now have a method of disabling guest access.	K1-30808
10.x KACE Agents no longer connect to the KACE Systems Management Appliance Server. All agents must be upgraded prior to upgrading the appliance to version 12.0. See .	K1-30178
Changes to ticket rules are now logged in object settings history.	K1-22114

Behobene Probleme

Dieser Abschnitt enthält die in dieser Version behobenen Probleme:

- Behobene Service-Desk-Probleme
- Behobene KACE-Agent-Probleme
- Behobene Inventarprobleme
- Behobene Sicherheitsprobleme
- Sonstige behobene Probleme

Behobene Service-Desk-Probleme

Im Anschluss finden Sie eine Liste mit Service-Desk-Problemen, die in dieser Version behoben wurden.

Behobene Service-Desk-Probleme

Behobenes Problem	ID des Problems
Requiring 2FA (two-factor authentication) for the **Administratorkonsole** could cause unexpected behavior with ticket creation from the **Benutzerkonsole**.	K1-32102
In the Service Desk *Tickets* list page, sorting by category did not behave as expected.	K1-31939

Behobenes Problem	ID des Problems
System message in ticket process comment could display HTML content.	K1-31938
Conditional Logic did not behave as expected with check boxes.	K1-31928
In Service Desk *Ticket Templates*, Conditional Logic did not work as expected for the *Category* field.	K1-31907
Error message could be seen when converting a ticket to a process.	K1-31893
When using the text editor and adding a link with the option to open it on a new tab did not behave as expected.	K1-31886
In a queue with SMTP inbound email, any emails from users with a comma in the display name showed up in the ticket as deleted users.	K1-31874
Changing screen label for Service Desk queue to include apostrophe caused the label to include ASCII code.	K1-31830
Child ticket submitter was set to parent ticket's submitter instead of the logged-in user when creating a ticket using a process.	K1-31797
Accented letters in the subject of an email sent to a Service Desk queue were replaced with question marks '?'.	K1-31784
When adding an image during ticket creation, the image was not always saved, as expected.	K1-31779
Users with no queue permissions were not able to see tickets they are copied on.	K1-31710
A double space in an email sometimes did not appear as expected in a Service Desk ticket.	K1-30843
Queue Email notifications were not working for approvers if they were not also ticket owners.	K1-30815
Pasting an image into a Knowledge Base article caused other pasted images to reset alignment and justification.	K1-30721
Ticket Archive: *Owners Only* comments were not visible after a ticket was archived	K1-30652
Service Desk Custom View was inaccurate for *All Queues* if permissions were limited in one of the queues.	K1-30608
Ticket ID could not be found in a search using the *All Queues* view.	K1-30606
User Download did not show in the user portal when restricting by device label.	K1-20682
Ticket was not added to process ticket table on using **Save and Create Child** button from the process child ticket.	K1-19052

Behobene KACE-Agent-Probleme

Im Anschluss finden Sie eine Liste mit KACE-Agent-Problemen, die in dieser Version behoben wurden.

Behobene KACE-Agent-Probleme

Behobenes Problem	ID des Problems
Agent alert message was seen for skipped tasks with no way of preventing or permanently hiding them. This will be reintroduced in a future version as an optional feature.	K1A-3871
Offline scripts with the **Also run once at next client checkin** option selected failed to run.	K1A-3843
KACE Agent could fail to run Powershell scripts during inventory if script execution policy is disabled by default on non-English OS.	K1A-3842
KACE Agent returned `Core.0` as part of the OS name on CentOS.	K1A-3841
KACE Agent Client Certificate handshake failed when another Konea certificate was imported by an external tool.	K1A-3840
macOS KACE Agent was instructed to download bad path when triggered to run with command only during Software Catalog-based managed installation.	K1A-3815
Windows 10 20H2 and 21H1 were reported by their display version instead of the technical version of 2009.	K1A-3803
An expected reboot could cause a patching task to enter an error state.	K1A-467

Behobene Inventarprobleme

Im Anschluss finden Sie eine Liste mit Inventarproblemen, die in dieser Version behoben wurden.

Behobene Inventarprobleme

Behobenes Problem	ID des Problems
Age column on the *Quarantine* list page did not sort correctly.	K1-30818
In rare situations, machine deletion could fail and produce unexpected results.	K1-30770
Quarantine record is hidden from the organization if the device is moved to another organization.	K1-29987
Performance degradation seen on the *Software Detail* page when the software was associated with large number of devices.	K1-20576

Behobene Sicherheitsprobleme

Im Anschluss finden Sie eine Liste mit Sicherheitsproblemen, die in dieser Version behoben wurden.

Behobene Sicherheitsprobleme

Behobenes Problem	ID des Problems
Downloading and *Paused* columns on the *Patch Schedules* list page were not showing expected data.	K1-31926
Dell Updates: *Custom View* did not report any results when Smart Label was a criteria.	K1-31860
All Linux machines in inventory (including v.11.0 KACE Agents) were included in the *Linux Package Upgrade Schedules* list before a schedule is run.	K1-31836
Windows Feature Update Catalog Installed, *Missing*, and *Error* counts did match the device list results.	K1-31819
Windows Feature Update *Detect, Stage and On-demand Deploy* schedule was not processing the correct output when files were not staged on the agent machine.	K1-31766
Permission was denied when a read-only user attempted to **Show Labels** on the *Patch Catalog* and *Dell Update Catalog* list pages.	K1-31750
Duplicating a patch schedule from a list of schedules did not work as expected.	K1-31714
Duplicating a Dell Update schedule from list of schedules did not work as expected.	K1-31713
Performance could degrade when doing an *Advanced Search* on the *Patch Catalog* list page.	K1-29975

Sonstige behobene Probleme

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

Sonstige behobene Probleme

Behobenes Problem	ID des Problems
Reset Tries button was disabled on *Device Details* page for patches and Dell Updates.	K1-31900
Extra rows could be seen when CSV reports were created.	K1-31885
Built-in report *Label Associations* did not work as expected	K1-31884
Patch Smart Labels with the *Operating System* field set to *Mac* did not include "Big Sur".	K1-31871

Behobenes Problem	ID des Problems
Performance issues were seen for agent connections after server restart for large deployments.	K1-31864
Windows Feature Update task displayed as successful when still running in a task chain.	K1-31794
For KACE GO, non-administrative queue owners could not set ticket device/asset to arbitrary device.	K1-31764
Duplicating ticket with custom field could fail from the User Portal.	K1-30856
Dashboard's *Managed Operating Systems Widget* results could be inaccurate.	K1-30813
Patching step with reboot in *Task Chain* incorrectly showed failed status.	K1-30812
During LDAP Import, *Additional Emails* could get overwritten if not mapped.	K1-30713
Package download process incorrectly updated offline last modified instead of last update status.	K1-30588
Importing LDAP users could unintentionally block attributes from mapping, that the administrator specifically listed under *Attributes to retrieve*.	K1-30083
Wizard report for *Asset - License* could return incorrect results.	K1-21350
License asset *Custom View* and *Advanced Search* could prevent some columns from displaying values.	K1-21342
Reporting: Special characters in the ticket *Title*, *Summary*, and *Comments* showed up incorrectly in report.	K1-21140
Read Only Administrators could not export assets.	K1-21096
It was not possible to manually update the *Additional Emails* field.	K1-21084
User *Custom Field* label was not used in column selector drop-down on the *Users* list page.	K1-20763
Edit Report wizard that uses Asset Subtype could display duplicate entries.	K1-20415
Advanced Search in the *Assets* list page could cause columns to be hidden, which also affected export.	K1-20059

Bekannte Probleme

Die folgenden Problem sind zum Zeitpunkt dieser Freigabe bekannt.

HINWEIS: Inventur von Agentless Ubuntu 21.04 Geräten schlägt für Benutzer mit einer nicht standardmäßigen Shell für den Dash fehl.

Bekanntes Problem	ID des Problems
When accessing user portal Downloads items, the preselected device is not the current device when using Firefox and SSL.	K1A-3874
KMenu utility does not work on Windows 7 and Windows Server 2008 R2 unless .NET framework 4.5 is installed.	K1A-3864
The Scripting API fails to create or update an existing script.	K1-32195
Approver, Category CC user unable to add comment through email if queue submitter is restricted.	K1-32173
In the *Devices* list, export of CSV fails when the Client Version column is sorted.	K1-32164
Duplicating replication share configuration allows same replication device to be saved.	K1-32128
Asset import preview shows asset IDs instead of the name of the asset.	K1-32090
ZFS-mounted file system is not represented correctly with Agentless inventory. This primarily affects FreeBSD.	K1-31824

Systemanforderungen

Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 12.0 ist 11.1. 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 von KACE Agent ist mindestens Version 11.0 erforderlich. Wir empfehlen, immer dieselbe Version des Agenten und der KACE Systemverwaltungs-Appliance zu verwenden.

Ab Version 12.0 der Appliance müssen frühere Versionen von KACE Agent, wie z. B. 11.1, speziell für Ihre Appliance-Version signiert werden. Wenn Sie beispielsweise KACE Agent 11.1 mit der Version 12.0 der Appliance verwenden, müssen Sie die KACE Agent 11.1 KBIN-Datei, mit der der Appliance-Schlüssel 12.0 signiert ist, abrufen und installieren. Sie können signierte KACE Agent KBIN-Dateien von der Seite KACE Systemverwaltungs-Appliance *Software Downloads* herunterladen.

HINWEIS: Das KACE Agent RPM-Paket kann nur auf verwalteten SUSE Linux-Geräten installiert werden, wenn das `libxslt-tools`-Paket vor dem Agenten-Paket installiert wird.

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 12.0, 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/12.0-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/12.0-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 12.0 können nur für KACE Systems Management Appliance mit Version 12.0 oder höher verwendet werden. Lizenzen für Version 12.0 können nicht auf Appliances verwendet werden, auf denen ältere Versionen wie etwa Version 11.0 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:

- **WICHTIG: Aktivieren von Booten aus Legacy-BIOS**:

  Während eines Upgrades kann ein Problem beim Booten aus der UEFI BIOS ausgelöst werden. Um dies zu verhindern, müssen Sie sicherstellen, dass das Booten aus Legacy-BIOS aktiviert ist. Das Gerät muss vor dem Umschalten ausgeschaltet werden. Stellen Sie außerdem bei ESX-basierten virtuellen Maschinen sicher, dass die Hardwareversion 13 oder höher ist.

  Vor der Anwendung des Appliance-Upgrades müssen Sie sicherstellen, dass der Cache Ihres Browsers leer ist und dass Port 52231 von Ihrem Browser auf die Appliance verfügbar ist. Benutzer, die von zu

Hause aus arbeiten, müssen möglicherweise ihre Unternehmens-Firewall so konfigurieren, dass sie die Kommunikation über Port 52231 zulässt.

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

  Die mindestens erforderliche Version für die Installation von KACE Systems Management Appliance 12.0 ist 11.1. 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 Agent-Version**.

  Für ein Upgrade von KACE Agent ist mindestens Version 11.0 erforderlich. Wir empfehlen, immer dieselbe Version des Agenten und der KACE Systemverwaltungs-Appliance zu verwenden.

  Ab Version 12.0 der Appliance müssen frühere Versionen von KACE Agent, wie z. B. 11.1, speziell für Ihre Appliance-Version signiert werden. Wenn Sie beispielsweise KACE Agent 11.1 mit der Version 12.0 der Appliance verwenden, müssen Sie die KACE Agent 11.1 KBIN-Datei, mit der der Appliance-Schlüssel 12.0 signiert ist, abrufen und installieren. Sie können signierte KACE Agent KBIN-Dateien von der Seite KACE Systemverwaltungs-Appliance *Software Downloads* herunterladen.

  HINWEIS: Das KACE Agent RPM-Paket kann nur auf verwalteten SUSE Linux-Geräten installiert werden, wenn das `libxslt-tools`-Paket vor dem Agenten-Paket installiert wird.

- **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/12.0-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 12.0 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 12.0. 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/12.0-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 12.0 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 12.0.

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/12.0-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 12.0 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 12.0 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 12.0.

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/12.0/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/12.0-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/12.0-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/12.0/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/12.0-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

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: September 2021

Software-Version: 12.0