

Quest®



KACE®システム管理アプライアンス11.1

リリースノート



目次

Quest® KACE®システム管理 アプライアンス11.1リリースノート.....	3
KACEシステム管理アプライアンス11.1について.....	3
新機能.....	3
拡張機能.....	5
解決済みの問題.....	6
既知の問題.....	10
システム要件.....	12
製品ライセンス.....	12
インストール手順.....	12
更新の準備.....	13
アドバタイズされたアップデートを使用した KACE システム管理アプライアンスサーバの アップデート.....	14
アップデートの手動によるアップロードと適用.....	14
アップデート後のタスク.....	15
正常に完了していることの確認.....	15
セキュリティ設定の確認.....	16
追加のリソース.....	16
グローバリゼーション.....	17
当社について.....	17
テクニカルサポートのリソース.....	17
法的情報.....	18

Quest® KACE®システム管理 アプライアンス11.1リリースノート

このドキュメントは、KACE システム管理アプライアンスバージョン 11.1 に関する情報が記載されています。

KACEシステム管理アプライアンス11.1について

KACE システム管理アプライアンスは、デバイスの管理、アプリケーションの展開、パッチ適用、資産管理、サービスデスクチケット管理などを自動化するための、仮想アプライアンスです。KACE システム管理アプライアンスシリーズの詳細については、<https://www.quest.com/products/kace-systems-management-appliance/>をご覧ください。このリリースには、多くの新機能が搭載されており、問題が修正され、セキュリティが強化されています。



注: これは、このリリースで翻訳されている唯一の文書ですが、ローカライズされたタイプには、問題解決、拡張機能、既知の問題に関する情報は含まれません。管理者ガイドや製品内のヘルプなど、その他のガイドは現時点ではローカライズされていません。バージョン 10.2 の文書が含まれています。

新機能

このリリースの KACE システム管理アプライアンスは、以下の機能を備えています。

デバイス通信

- **KACE エージェントシステムトレイの追加:** リンクを開くなど、システムトレイのエージェントアイコンにその他の機能が追加されました。システム管理者は、新しいショートカットメニュー項目に表示されるリンクを最大 10 個まで指定できます。このメニュー項目は、エージェントステータスアイコンのショートカットセクションで 1 つ以上のリンクが指定されている場合にのみ表示されます。

HTTP、SSH、FTP URL などの標準の統一資源位置指定子 (URI) リンクをサポートしています。このリンクをクリックすると、システムが選択したリソースに関連付けられたアプリケーションが起動します。たとえば、HTTP タイプのリンクをクリックすると、システムはデフォルトのブラウザでリンクを開きます。

- **Hyper-V インベントリ:** このリリースでは、エージェント管理対象デバイスの仮想マシンマネージャと MS Hyper-V データ用に、インベントリ情報と関連デバイスのコマンドが追加されました。インベントリ

の詳細情報には、仮想マシンとインベントリへの Hyper-V ホストの一覧などがあります。これは、バージョン 10.0 で作成された VMware インベントリ機能に似ています。

- **オペレーティングシステムサポートの更新**：アプライアンスは、エージェント管理デバイスで次の OS バージョンをサポートするようになりました。
 - MS Windows 10 20H2
 - MS Windows Server 2019 20H2
 - macOS 11.0
 - macOS 11.0 システムから HTTPS を使用してユーザーコンソールに接続する場合、アプライアンスは、そのシステムに関連付けられているエージェントの一意識別子 (KUID) を決定できません。これは、マイデバイスリストおよびソフトウェアライブラリのインストールに影響します。この問題の根本的な原因は、すべての証明書の信頼設定をユーザーが承認する必要があるという macOS 11.0 の新しい要件のためです。この問題により、エージェントの konea.log に、次のエントリが表示されることもあります。

```
[ERROR|ssl_darwin.go:107:AddCertAsTrustedRoot | SecTrustSettingsSetTrustSettings failed|{"err":"The authorization was denied since no user interaction was possible."}]
```
 - アプライアンスは、このバージョンのオペレーティングシステムのパッチ適用をサポートしていません。アプリケーションへのパッチ適用が使用可能です。macOS 11.0 デバイスの OS レベルのパッチ適用は、サブスクリプションがある場合、KACE Cloud モバイルデバイスマネージャ (MDM) で使用できます。

パッチ適用

- **Linux パッケージのアップグレード**：アプライアンスで、Linux パッケージのアップグレードのインストールおよび管理プロセスを自動化できるようになりました。これにより、管理対象の Linux RedHat、SUSE、Ubuntu、CentOS、Raspbian デバイスの Linux OS を最新の状態に維持できます。これらのアップグレードにより、管理対象の Linux デバイスの全体的なパフォーマンスが向上し、潜在的な脆弱性から保護されます。

この機能を使用すれば、パッケージのアップグレードを検出したり、適用可能なすべてのパッケージを検出してアップグレードを行ったりする、アップグレードスケジュールを作成できます。Linux フレーバーごとに検出のみのスケジュールアクションの後に、使用可能なパッケージのアップグレードの一覧を確認できます。

アップグレードプロセスは、管理対象の Linux デバイスが適切なパッケージリポジトリを参照していることを前提としています。セキュリティ更新を含むパッケージのみが識別されます。アプライアンスは、すべてのパッケージを検出またはアップグレードしようしたり、OS 全体を最新バージョンにアップグレードしようとしたりはしません。

i **注**: Raspbian Linux では、定期的な更新とセキュリティ更新は区別されません。管理対象の Raspbian デバイスのパッケージを検出してアップグレードすると、それらのデバイスにすべての更新済みパッケージがインストールされます。

- **新しい Dell ハードウェア更新カタログとの統合**：このリリース以降、アプライアンスは新しいバージョンの Dell ハードウェアカタログを使用します。ハードウェア更新を検出して展開するプロセスは、デバイスのパッチ適用に使用されるプロセスと非常に似ています。まず、ハードウェア更新を検出、展開、または検出して展開するためのスケジュール更新を作成します。カタログページで、利用可能な Dell アップデートの一覧を確認できます。このページには、アプライアンスに存在するシグニチャファイルの更新が一覧表示されます。
 - この機能を使用するには、管理対象の Dell デバイスで実行する KACE Agent の最新バージョンが必要です。
 - スケジュール履歴などの Dell ハードウェア更新に関連する既存のデータは、アプライアンスの以前のバージョンからは移行されません。
 - Dell ハードウェア更新に関連付けられ、旧バージョンのアプライアンスで作成されたユーザーレポートは、バージョン 11.1 には移行されません。

インフラストラクチャ

- **Linux and Mac 向け Oval** : このリリースでアプライアンスは、世界最大かつ最高の CVE データを使用して、これまで MS Windows のみだった Oval サポートを拡張します。
- **ライセンス更新のアラート** : アプライアンスのメンテナンスの期限が切れると、パッチ適用サポートなど一部の機能が使用できなくなります。これにより、ホームダッシュボードにエラーアラートが表示されます。ライセンスを更新するには、<https://support.quest.com/contact-us/renewals> にアクセスしてください。

サービスデスク

- **サービスデスクチケットのカテゴリ階層** : 管理者コンソールが改善され、サービスデスクのカテゴリおよびサブカテゴリの設定を効率化できるようになりました。ツリーウィジェットを使用して、チケットカテゴリおよびサブカテゴリノードを作成および編集できます。ツリービューを使用すると、カテゴリ間の関係をよりよく理解して管理できます。必要に応じて、新しいカテゴリノードの追加、名前の変更、削除、並べ替えを簡単に行うことができます。検索機能を使用して、特定のカテゴリまたはサブカテゴリをすばやく検索することもできます。
- **サービスデスクチケットのプレフィックスを指定する機能** : このリリース以降、各キューに異なるプレフィックスを使用してサービスデスクのワークフローを整理し、ヘルプデスクに対する HELP: やハードウェアとソフトウェアの要求に対する HDREQ: などの適切なカテゴリに関連付けることができます。
- **Microsoft 365 GCC High サービスのサポート** : MS Office 365 OAuth 認証情報では、Azure AD テナントタイプとエンドポイント URL を指定して、お使いの環境に関連付けられたナショナルクラウドのトークンを取得できるようになりました。インバウンドサービスデスクの E メールに Office 365 OAuth を選択すると、Microsoft 365 GCC、Microsoft 365 GCC High など、該当する Microsoft 365 API サービスを参照できます。特に、Microsoft 365 GCC High は、高セキュリティ環境で使用されます。

拡張機能

以下は、このリリースに実装されている拡張機能の一覧です。

拡張機能	問題 ID
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
SAML-enabled systems can now be locked down to allow access only to SAML-authenticated users and the local admin user.	K1-30246

拡張機能	問題 ID
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 管理者コンソール , 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/Domain column of the Allow List.	N/A

解決済みの問題

以下の問題は、このリリースで解決されています。

Resolved Service Desk issues

解決済みの問題	問題 ID
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
When duplicating a process, the ticket template was not duplicated.	K1-30460

解決済みの問題**問題 ID**

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 管理者コンソール 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**解決済みの問題****問題 ID**

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

解決済みの問題	問題 ID
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 システム管理コンソール, 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

解決済みの問題	問題 ID
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
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

解決済みの問題**問題 ID**

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**解決済みの問題****問題 ID**

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 システム管理コンソール.	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 管理者コンソール could be disrupted when changing an organization's virtual IP address or host name.	K1-25452
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

解決済みの問題	問題 ID
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

既知の問題

このリリースの時点で以下の問題の存在が認識されています。

既知の問題	問題 ID
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

既知の問題	問題 ID
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
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

システム要件

KACE システム管理アプライアンス 11.1 をインストールするために必要な最小バージョンは 11.0 です。使用しているアプライアンスで以前のバージョンが実行されている場合、リストされているバージョンにアップデートしてから、インストールに進む必要があります。

KACE エージェントをアップグレードするために必要な最小バージョンは 10.2 です。KACE システム管理アプライアンス 11.1 で最新のエージェントバージョンを実行することをお勧めします。



注: KACE Agent RPM パッケージは、エージェントパッケージの前に libxslt-tools パッケージがインストールされている場合のみ、管理対象の SUSE Linux デバイスにインストールできます。

アプライアンスのバージョン番号を確認するには、管理者コンソールにログインして、サポートが必要な場合をクリックします。表示されるヘルプパネルの下部で、丸で囲まれた i ボタンをクリックします。

バージョン 11.1 にアップグレードまたはインストールする前に、お使いのシステムが最小要件を満たしていることを確認してください。これらの要件は、KACE システム管理アプライアンスの技術仕様で確認できます。

- 仮想アプライアンスの場合：<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/> に移動します。
- サービスとしての K1000 の場合：<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/> に移動します。

製品ライセンス

現在 KACE システム管理アプライアンスの製品ライセンスをお持ちの場合、追加のライセンスは必要ありません。

初めて KACE システム管理アプライアンスを使用している場合は、アプライアンスセットアップガイドで製品ライセンスの詳細を確認してください。[追加のリソース](#)に移動して、適切なガイドを確認します。



注: バージョン 11.1 の製品ライセンスは、バージョン 11.1 以降を実行する KACE システム管理アプライアンスでのみ使用できます。バージョン 11.1 のライセンスは、10.0 など以前のバージョンのアプライアンスを実行するアプライアンスでは使用できません。

インストール手順

このバージョンを適用するには、アドバタイズされたアップデートを使用するか、アップデートファイルを手動でアップロードして適用します。手順については、以下のトピックを参照してください。

- [更新の準備](#)
- [アドバタイズされたアップデートを使用した KACE システム管理アプライアンスサーバのアップデート](#)
- [アップデートの手動によるアップロードと適用](#)
- [アップデート後のタスク](#)



注: 特定のソフトウェアを実行しているデバイスのソフトウェア検出とインストール数の正確性を確保するため、KACE システム管理アプライアンス 7.0 リリースから、ソフトウェアカタログがアップグレードごとに再インストールされます。

更新の準備

KACE システム管理アプライアンスサーバをアップデートする前に、次の推奨事項に従ってください。

- **KACE システム管理アプライアンスサーバのバージョンの確認：**

KACE システム管理アプライアンス 11.1 をインストールするために必要な最小バージョンは 11.0 です。使用しているアプライアンスで以前のバージョンが実行されている場合、リストされているバージョンにアップデートしてから、インストールに進む必要があります。

アプライアンスのバージョン番号を確認するには、管理者コンソールにログインして、サポートが必要な場合をクリックします。表示されるヘルプパネルの下部で、丸で囲まれた **i** ボタンをクリックします。

- **KACE エージェントのバージョンの確認。**

KACE エージェントをアップグレードするために必要な最小バージョンは 10.2 です。KACE システム管理アプライアンス 11.1 で最新のエージェントバージョンを実行することをお勧めします。

i | **注:** KACE Agent RPM パッケージは、エージェントパッケージの前に libxslt-tools パッケージがインストールされている場合にのみ、管理対象の SUSE Linux デバイスにインストールできます。

- **開始前のバックアップ：**

データベースとファイルをバックアップして、将来参照できるようにバックアップを KACE システム管理アプライアンスサーバ以外の場所に保存します。データベースとファイルのバックアップの詳細については、『管理者ガイド』（<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>）を参照してください。

- **バージョン 7.0 より前にインストールされたアプライアンス。**

Quest Software では、バージョン 7.0 より前に最初にインストールされたアプライアンスのイメージ再作成（物理アプライアンス）または再インストール（仮想）を行わない場合、バージョン 11.1 にアップグレードする前に、データベースのエクスポート、再作成（OVF ファイルからのイメージまたは仮想マシンのインストール）、および再インポートを行うことを強くお勧めします。詳細については、「<https://support.quest.com/kace-systems-management-appliance/kb/111810/how-to-re-image-the-k1000-appliance>」を参照してください。

お使いのアプライアンスのバージョンがかなり古い場合は、次の記事にアップグレードに関する役立つヒントが記載されています。<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->

アプライアンスのイメージを再作成する理由は多数あります。たとえば、新しいディスクレイアウトでは、バージョン 11.1 との互換性が向上しています。また、セキュリティとパフォーマンスも向上しています。

システムがこのようなアップグレードのメリットを受けるかどうかを判断するには、KBIN ファイルを使用して、アプライアンスの正確な使用年数とディスクレイアウトを特定します。KBIN をダウンロードするには、「<https://support.quest.com/kace-systems-management-appliance/kb/210267/how-to-run-the-kace-systems-management-appliance-configuration-report>」にアクセスしてください。

- **ポート 52231 が使用可能であることの確認。**

.kbin をアップグレードする前に、ポート 52231 を使用して、KACE アップグレードコンソール ページにアクセスできるようにする必要があります。このポートを使用可能にせずにアップグレードが開始された場合、アップグレードの進行状況を監視することはできません。Quest KACE では、信頼できるシステムからポート 52231 を介したアプライアンスへのトラフィックを許可し、アップグレードコンソールからアップグレードを監視することを強く推奨します。アップグレードコンソールにアクセスしない場合、アップグレードはタイムアウトしたとして、ブラウザに表示されるアクセスできないページにリダイレクトされます。これにより、ユーザーはアップグレードによりシステムがクラッシュしたと判断して、ボックスを再起動することになりますが、実際にはアップグレードはまだ進行中です。アップグレードの進行状況が不明な場合、KACE サポートに連絡してください。また、アプライアンスを再起動しないでください。

アドバタイズされたアップデートを使用した KACE システム管理アプライアンスサーバのアップデート

管理者コンソールのダッシュボードページまたはアプライアンスの更新ページで、アドバタイズされたアップデートを使用して KACE システム管理アプライアンスサーバをアップデートできます。

注意: アップデート中、KACE システム管理アプライアンスサーバを手動で再起動しないでください。

1. データベースとファイルをバックアップします。詳細については、**管理者ガイド** (<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>) を参照してください。
2. アプライアンスのコントロールパネルに移動します。
 - アプライアンスで組織コンポーネントが有効化されていない場合は、**設定** をクリックします。
 - アプライアンスで組織コンポーネントが有効化されている場合、アプライアンスの**システム管理コンソール** にログインします。(http://KACE_SMA_hostname/system) にログインするか、ページの右上隅にあるドロップダウンリストから **システム** を選択し、**設定** をクリックします。
3. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、アプライアンスの更新ページを表示します。
4. **更新の確認** をクリックします。

確認の結果がログに表示されます。
5. 更新プログラムが使用可能な場合は、**更新** をクリックします。

重要: 最初の 10 分間、アップデートが解凍および検証されている間、一部のブラウザはフリーズしたように見える場合があります。この間に、ページからの移動やページのリフレッシュ、またはページでブラウザのボタンをクリックすると、これらのアクションによって処理が中断されるため、この間はこれらの操作を実行しないようにしてください。アップデートの解凍と検証の後、ログページが表示されます。アップデートプロセス中のいずれの時点でも、アプライアンスを手動で再起動しないでください。

バージョン 11.1 が適用され、KACE システム管理アプライアンスサーバが再起動します。ブラウザウィンドウと管理者コンソールに進捗が表示されます。

6. サーバのアップグレードが完了したら、すべてのエージェントをバージョン 11.1 にアップグレードします。

アップデートの手動によるアップロードと適用

Quest でアップデートファイルが公開されている場合は、そのファイルを手動でアップロードして、KACE システム管理アプライアンスサーバを更新できます。

注意: アップデート中、KACE システム管理アプライアンスサーバを手動で再起動しないでください。

1. データベースとファイルをバックアップします。詳細については、**管理者ガイド** (<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/>) を参照してください。
2. ログイン資格情報を使用して、Quest Web サイト (<https://support.quest.com/kace-systems-management-appliance/download-new-releases>) にログインし、KACE システム管理アプライアンスサーバの .kbin ファイル (11.1 GA (一般向け) リリース用) をダウンロードして、ローカルに保存します。
3. 左側のナビゲーションバーで、**アプライアンスの更新** をクリックして、**アプライアンスの更新** ページを表示します。
4. 手動によるアップデート セクションで次の操作を実行します。
 - a. **参照** または **ファイルを選択** をクリックして、アップデートファイルを見つけます。
 - b. **アップデート** をクリックし、**はい** をクリックして確認します。バージョン 11.1 が適用され、KACE システム管理アプライアンスサーバが再起動します。ブラウザウィンドウと管理者コンソールに進捗が表示されます。
5. サーバのアップグレードが完了したら、すべてのエージェントをバージョン 11.1 にアップグレードします。

アップデート後のタスク

アップデートが終わったら、アップデートが成功していることを確認し、必要に応じて設定を確認します。

正常に完了していることの確認

KACE システム管理アプライアンスのバージョン番号を表示して、正常に完了していることを確認します。

1. アプライアンスの **コントロールパネル** に移動します。
 - アプライアンスで組織コンポーネントが有効化されていない場合は、**設定** をクリックします。
 - アプライアンスで組織コンポーネントが有効化されている場合、アプライアンスの **システム管理コンソール** にログインします。 (http://KACE_SMA_hostname/system) にログインするか、ページの右上隅にあるドロップダウンリストから **システム** を選択し、**設定** をクリックします。
2. 現在のバージョンを検証するには、ページの右上隅にある **サポートが必要な場合** をクリックし、表示されるヘルプパネルの下部で、丸で囲まれた **i** ボタンをクリックします。

セキュリティ設定の確認

セキュリティを強化するため、アップデート中は HTTP および FTP 経由のデータベースアクセスが無効になります。データベースファイルへのアクセスにこれらの方法を使用している場合は、アップデートの後、必要に応じてセキュリティ設定を変更します。

1. アプライアンスのコントロールパネルに移動します。
 - アプライアンスで組織コンポーネントが有効化されていない場合は、設定 をクリックします。
 - アプライアンスで組織コンポーネントが有効化されている場合、アプライアンスのシステム管理コンソールにログインします。(http://KACE_SMA_hostname/system) にログインするか、ページの右上隅にあるドロップダウンリストから システム を選択し、設定 をクリックします。
2. 左のナビゲーションバーで セキュリティ設定 をクリックして、セキュリティ設定 ページを表示します。
3. ページの上部で、次の設定を変更します。
 - **セキュアバックアップファイルの有効化**：このチェックボックスをオフにすると、ユーザーは、HTTP を使用して認証なしにデータベースバックアップファイルにアクセスできるようになります。
 - **データベースアクセスの有効化**：このチェックボックスをオンにすると、ユーザーは、ポート 3306 経由でデータベースにアクセスできるようになります。
 - **FTP 経由のバックアップの有効化**：このチェックボックスをオンにすると、ユーザーは、FTP を使用してデータベースバックアップファイルにアクセスできるようになります。

注意: これらの設定を変更するとデータベースのセキュリティが低下するため、推奨されません。
4. 保存 をクリックします。
5. **KBINアップグレードの場合のみ**。アプライアンスへのルートパスワード (2FA) アクセスの難度を上げます。
 - a. システム管理コンソールで、設定 > サポート の順にクリックします。
 - b. サポート ページのトラブルシューティングツール で、**2要素認証** をクリックします。
 - c. 2要素認証をサポート ページで、**シークレットキーの置き換え** をクリックします。
 - d. トークンに関する記録を作成し、この情報を安全な場所に保管します。

追加のリソース

次の場所から、その他の情報を利用できます。

- オンライン製品ドキュメント (<https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents>)
 - 技術仕様：製品のインストールや、最新バージョンへのアップグレードに必要な最小要件に関する情報が記載されています。
- 仮想アプライアンスの場合：<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-virtual-appliances/> に移動します。

サービスとしてのKACEの場合：<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/technical-specifications-for-kace-as-a-service/> に移動します。

- セットアップガイド：仮想アプライアンスのセットアップに関する説明が記載されています。<https://support.quest.com/kace-systems-management-appliance/11.1/technical-documents> に移動して、最新リリースのマニュアルを参照します。
- 管理者ガイド：アプライアンスの使い方に関する説明が記載されています。<https://support.quest.com/technical-documents/kace-systems-management-appliance/11.1-common-documents/administrator-guide/> に移動して、最新リリースのマニュアルを参照します。

グローバル化

本項には、この製品を英語以外の構成でインストールして運用するための情報（北米以外のお客様が必要とする情報など）を記載しています。本項は、製品マニュアルの他の場所に記載されているサポート対象プラットフォームや設定に関する資料の代わりとなるものではありません。

このリリースはユニコード対応であり、すべての文字コードをサポートしています。このリリースでは、すべての製品コンポーネントを、同じまたは互換性のある文字エンコードを使用するように設定する必要があり、また同じロケールと地域オプションでインストールする必要があります。このリリースは、次の地域での運用をサポートすることを目的としています。北米、西ヨーロッパ、ラテンアメリカ、中央および東ヨーロッパ、極東アジア、日本。

このリリースは、次の言語のローカライズ版が用意されています。フランス語、ドイツ語、日本語、ポルトガル語（ブラジル）、スペイン語。

当社について

Quest は、複雑化する IT 環境において、新しいテクノロジーの利点を現実のものにするソフトウェアソリューションを生み出しています。データベースとシステム管理から Active Directory と Office 365 の管理、サイバーセキュリティの回復力まで、Quest はお客様の次の IT の課題を今すぐ解決できるように支援します。世界中で、130,000 社以上の企業と Fortune 500 企業の 95% が、次の企業イニシアチブのプロアクティブな管理と監視を実施し、複雑なマイクロソフトの課題に対応する次のソリューションを見つけ、次の脅威に先んじるために、Quest を頼りにしています。Quest Software。今「次」に備える。詳細に関しては、「www.quest.com」を参照してください。

テクニカルサポートのリソース

Quest の有効なメンテナンス契約をお持ちのお客様、および試用版をお持ちのお客様は、テクニカルサポートをご利用いただけます。Quest サポート ポータルは、<https://support.quest.com> からアクセスできます。

サポートポータルは、問題を迅速に自身で解決するのに使用できるセルフヘルプツールを提供しており、毎日24時間アクセスできます。このサイトでは、以下の操作を実行できます。

- サービスリクエストの送信と管理
- サポート技術情報記事の表示
- 製品情報への登録
- ソフトウェアと技術文書のダウンロード
- 説明ビデオの再生
- コミュニティの討論への参加
- サポートエンジニアとのオンラインチャット
- 製品のサポートサービスの表示

法的情報

© 2021 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.

特許

Quest Software の先進技術は、当社の誇りです。この製品には特許および出願中の特許が適用される場合があります。この製品に該当する特許の最新情報については、当社の Web サイト <https://www.quest.com/legal> をご覧ください。

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.

凡例



注意: 注意アイコンは、指示に従わなかった場合に、ハードウェアの損傷やデータ損失につながる可能性があることを示します。



重要、注、ヒント、モバイル、またはビデオ: 情報アイコンは、補足情報を表しています。

KACEシステム管理アプライアンスリリースノート

更新日 - 2021 年 4 月

ソフトウェアバージョン - 11.1