KACE® Systems Management Appliance 10.0

Setup Guide for Azure Platforms

Table of Contents

Setting up the appliance

Before you begin

Before you set up the appliance, there are a number of preliminary actions you need to take.

1. Ensure that you have a subscription to Microsoft Azure. When you install your virtual KACE SMA, the appliance will run as a virtual machine in the Azure cloud. For more information about the Azure cloud platform, or to sign up, see http://azure.microsoft.com/en-us/.
2. Purchase a license for a Microsoft Azure virtual KACE SMA from Quest sales at https://www.quest.com/company/contact-us.aspx.
3. Ensure that your network and firewall settings allow outbound access to KACE SMA on port 443. This port is used for appliance web-based consoles and Agent communications over HTTPS. It should also be open on devices, including desktops and servers, that have the KACE SMA Agent software installed.

Feature exceptions

All functionality of the KACE SMA Administrator Console can be configured to be used within the cloud. However, some features require direct access to your network, which is established using a site-to-site VPN connection. VPN connections leverage the shared network, and a single VPN connection usually is sufficient to enable the functionality for a single company. In some cases, however, additional VPN connections might be necessary, and dedicated network bandwidth might be required. For more information, see Using VPN connections and network resources.

Administrator Console features that require a VPN connection

The following Administrator Console features require a VPN connection:

- Server monitoring using Agentless device management.
- Wake On LAN, Network Discovery (including IP Scan, Active Directory® scan, and NMAP scan), KACE SMA Agent provisioning from the appliance (see Provisioning the KACE SMA Agent to managed devices).

  

  These features do not require a VPN when Agent relay is used.

- Importing and exporting resources (file sharing is blocked by the cloud firewall).
- FTP access to backup files (FTP access is blocked by the cloud firewall).

- Application packages and script dependencies must be uploaded using HTTP. Large package uploads could timeout on slower network connections. Packages larger than 2 GB must be distributed using an alternate download location from an internal file server.
- LDAP user and device labels.
- LDAP user authentication.
- LDAP user import.
- Active Directory single sign on for the Administrator Console and User Console.

User Console feature exceptions

The User Console is the interface that makes software library and Service Desk features available to end users. The following User Console feature is not supported in the cloud:

- Automatic software installations from the User Console (downloads are supported).

Create a KACE SMA virtual machine in Azure

This topic describes the process of creating a virtual machine (VM) in Microsoft Azure to serve as your KACE Systems Management Appliance (SMA) using a VM template available from the Azure Marketplace.

Ensure that you have a valid Azure subscription. When you install your virtual KACE SMA, the appliance will run as a virtual machine in the Azure cloud. For more information about the Azure cloud platform, or to sign up, see http://azure.microsoft.com/en-us/.

1. Log in to https://azuremarketplace.microsoft.com/ using your Azure subscription credentials.
2. In the Search field, type KACE Systems Management Appliance.
3. Open the KACE Systems Management Appliance application.
4. Review the information on the Plans + Pricing section to find out about recommended virtual machine resource requirements.
5. Click GET IT NOW.
6. Click Create.

   The Create Virtual Machine page appears, consisting of several tabs. Some of these tabs contain options that are required to configure a KACE SMA VM.

   

   The Azure interface changes frequently. Some options may not match precisely. For the latest details about this page, visit https://docs.microsoft.com/en-us/azure/.
7. On the Create Virtual Machine page, on the Basics tab, provide the following information.

Option	Description
Subscription	Specify the name of your Azure subscription.
Resource group	Create a resource group or use an existing one for this virtual machine.
Virtual machine name	Type the name of the virtual machine you are about to create.
Image	This option displays the selected KACE Systems Management Appliance image.
Size	a. Click Change Size. b. On the Select a VM size page that appears, select a configuration from the recommended VM sizes, as required.
Authentication type	Provide the authentication details for the administrator account on the virtual machine. Administrator account credentials will not be used to access the appliance. However, this information is mandatory for any virtual machine you create in Azure, and you need to specify it. a. Select Password. b. In the Username field, type the user name of the virtual machine administrator. c. In the Password field, type the password of administrator account.

8. Leave all other options as is, and click Next.
9. On the Discs tab, click OS disk type and select Premium SSD. This is the recommended minimum for the appliance.
10. Leave all other options as is, and click Next.
11. On the Networking tab, configure the following options:

Option	Description
Virtual Network	Select an existing virtual network or create a new one.
Subnet	Select existing subnet or define a new one.
IP	Use a public IP address if you want to communicate with the KACE SMA from outside the virtual network.

When you upgrade the appliance, to track the upgrade status in the browser, you must open port 52231. Close this port when the upgrade is successfully applied.

12. Leave all other options on this and any remaining tabs as is, and click Next until you reach the Review tab.
13. On the Review tab, click Create.

    While the VM deploys, a progress bar appears in the browser. When complete, a notification appears briefly, and an overview with details for your VM appears in Azure.

Configure the appliance

Use the Initial Setup wizard to configure the appliance, and to log in to the Administrator Console.

Your browser setting determines the language displayed in the Administrator Console the first time you log in. For information about changing the language settings, go to the appliance Administrator Guide: Accessing the Administrator Guide and online Help.

1. Obtain the fully qualified DNS name of the virtual machine running the appliance software in Azure.
   a. In Azure, select the virtual machine, and go to Overview settings.
   b. On the Overview page, click Configure and set a DNS name for the KACE SMA. For example, my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com.

   For more information about these settings, see https://docs.microsoft.com/en-us/azure/.
2. Open a web browser and enter the Administrator Console URL using the following syntax:

   http://<unique_KACE_SMA_appliance_name>/admin

   Where <unique_KACE_SMA_appliance_name> is the fully qualified virtual machine DNS name you configured in step 1.

   For example: http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

   The Software Transaction Agreement page appears.
3. Accept the agreement.

   The Initial Setup wizard appears.
4. In the Initial Setup wizard, on the Welcome page, verify that you have the information required to configure the appliance, then click Next.
5. On the Diagnostic Console Two-Factor Authentication page, review and record the secret key and offline tokens, then click Next.
6. On the Licensing and Administrator Settings page, provide the following information:

Option	Description
License Key	The license key you received in the Welcome email from Quest. If you do not have a license

Option	Description
	key, contact Quest Software Support at https://support.quest.com/contact-support.
Company Name	The name of your company or group.
Administrator Email	The email address where you want to receive communications from Quest.
Password	The password for the default admin account, which is the account you use to log in to the appliance Administrator Console. The default admin account is the only account on the appliance at this time. If you forget the password for this account, the system might have to be reset to factory defaults which can result in loss of data. If you have multiple KACE SMA or KACE SDA (Systems Deployment) appliances, Quest recommends that you use the same password for the admin account on all appliances. This enables you to link the appliances later. For more information, see the appliance Administrator Guide: Accessing the Administrator Guide and online Help.
Two-Factor Authentication	If you want to provide stronger security for users logging into the appliance, set this to Enabled. This feature adds an extra step to the login process. It relies on the Google Authenticator app to generate verification codes. The app generates a new six-digit code at regular intervals. When enabled, end users will be prompted for the current verification code each time they log in. If you enable this feature, ensure that KACE SMA server's clock is accurate, as well as the device running Google Authenticator. Google Authenticator relies on current time to create the token. If server's clock is not synchronized with those of the devices running Google Authenticator, token validation may fail, which may result in the account lockouts.

When done, click Next.

7. On the Enable File Sharing page, follow the on-screen instructions to complete this step.
8. On the Domain Settings page, specify the time zone, host name, and the domain name of your appliance.

   This page also allows you to enable custom DNS settings. A default installation uses Azure provided DNS servers.

   When you configure site-to-site VPN, you can also use your DNS IP to either make the appliance accessible to both internal and public networks (recommended), or just the internal network, depending on your DNS configuration. To do that, select Enable Custom DNS, and in the Primary DNS field, type your DNS IP address. For more information, review the help contents on this page.

   When done, click Next.
9. On the Confirm page, review your configuration.

   If you need to make any changes, use the Back button in the wizard to go to the appropriate step, and update your configuration.

   When done, click Finish.

   When the initial setup is complete, the appliance restarts and the Administrator Console login page appears.
10. Log in to the Administrator Console using the login ID admin and the password you chose during initial setup.

    If Two-Factor Authentication was enabled on the Licensing and Administrator Settings page in the Initial Setup wizard, the Configure Two-Factor Authentication page appears.
11. Two-Factor Authentication only. Follow the instructions on the Configure Two-Factor Authentication page to generate a Google Authenticator verification code using your smart phone. In the Verification Code field, type the Google Authenticator code, and click Finish Configuration. A new verification code is required on each subsequent login.

    To skip this step, click Skip Configuration. You can only bypass this step during a configured transition window. For more information, see the Administrator Guide.
12. Provide the fully qualified appliance DNS name on the Network Settings. When you reboot the appliance in Azure, its IP address changes. Devices connect to the appliance using this name.
    a. Log in to the KACE SMA Administrator Console, and click Settings.
    b. On the appliance Control Panel that appears, click Network Settings.
    c. On the Network Settings page, in the Appliance Network Configuration section, in the Web Server Name field, type the fully qualified appliance DNS name that you recorded in step 3.
    d. Click Save.

The Command Line Console is a terminal window interface to the appliance. This tool allows you to configure network settings. You must not use this tool to change the IP address for the appliance running in Azure.

The Administrator Console appears and the appliance is ready for use.

Enable SSL

You must enable secure communications between the appliance and managed devices, and you can use the appliance Administrator Console to generate an SSL certificate.

Obtain a registered domain name to be used for the appliance. This is required to generate an SSL certificate signing request using the appliance Administrator Console.

1. In the Administrator Console, click Settings to go to the appliance Control Panel.
2. Click Security Settings.

   The Security Settings page appears.
3. In the SSL section toward the bottom of the page, disable access to the HTTP port 80, and forward all port 80 traffic to the HTTPS port 443.

   Failing to disable port 80 enables transmission of sensitive information, such as passwords, in plain text over the internet.

   - Clear Enable port 80 access.
   - Select Enable SSL and Enable Forward port 80 to port 443.
4. Click SSL Certificate Form to display the SSL Certificate Form page.
5. In the Configure section, provide the following information:

Option	Description
Company Name	The name of your company.
Organization Name	The name of your organizational unit or business group.
Common Name	The common name of the appliance you are creating the SSL certificate for.
Email	Your email address.
City Name	The name of your locality.
State or Province Name	The name of your state or province.
Country Name	The name of your country.

6. Click Save.

7. Generate a self-signed certificate.
   a. Click Generate Self-Signed Certificate to generate and display the certificate below the Certificate Signing Request section.
   b. Click Deploy Self-Signed Certificate, then click Yes.
   c. On the Security Settings page, click Save and Restart Services.

   The SSL certificate is generated. Self-signed certificates are converted to PEM files, named kbox.pem, and they are placed in KACE SMA Agent data folders. For more details about security settings, see the Administrator Guide.

   If you create a self-signed certificate, you need to deploy that certificate to all Agent-managed devices.

8. Restart the appliance.

Best practices

Follow the guidelines and recommendations in this section when using the appliance.

Using VPN connections and network resources

If you are using the traditional Agent-server communication between the appliance and your managed devices, installing the Agent on managed devices is all that is required for communication. However, if you are using a VPN connection, it is your responsibility to complete the network handshake from your environment to the appliance. The appliance team can provide recommendations, such as the appropriate IP addresses and ports to allow, and it is essential to have your network administrator involved in the setup process. The appropriate cloud connections are configured, and you need to ensure connection from your side to complete the setup successfully.

In addition, some appliance features require a VPN connection to be used in the cloud, and a single VPN connection is usually sufficient for a single company. For example, you can use a single VPN connection even if you have remote locations provided that those locations can route traffic through the main corporate site where the VPN connection exists. All KACE SMA Agent traffic is routed through the VPN and then to the appliance through the VPN connection. If remote locations cannot see the main corporate site, or if you want each site to have a direct VPN link to the appliance, you need to purchase a VPN connection for each site. For more information about features that require VPN connections, see Feature exceptions.

Product pricing is based upon shared network bandwidth. To purchase additional network resources, or to purchase VPN connections, contact Quest sales at https://www.quest.com/company/contact-us.aspx.

Using VPN connections with multiple domains

The appliance is designed to be used with a single domain and a single VPN connection. If you have multiple domains, you can manage devices (inventory) on other domains using the appliance, but features that require VPN access are available only to a single domain. For example, you can authenticate to a single Active Directory environment for Identity Access Management, but you cannot authenticate to more than one domain. Agent traffic from the domain with the VPN connection is routed through the VPN connection, whereas Agent traffic for other domains connects to the appliance using standard Internet access. For more information about features that require VPN connections, see Feature exceptions.

About the appliance IP address

The appliance is configured for a single IP address. The IP address is assigned by Quest and that address cannot be changed. You must create a Host (A) record in your internal DNS (domain name system) server for the appliance's static IP address, and you can create multiple A (host) records across multiple networks or domains to point to your appliance. If you need to use more than one public IP address for your network, you must purchase a separate instance of the appliance. Multiple appliance instances cannot share any data or database information. For more information, contact Quest sales at https://www.quest.com/company/contact-us.aspx.

About network settings

By default, all network protocols and their associated services are disabled except for HTTPS, and HTTP. These protocols are used for the appliance user interfaces and KACE SMA Agent communications. When the KACE SMA Agent software is provisioned to a device, the Agent always attempts to connect to the appliance using HTTPS over port 443 for encrypted communications if SSL is enabled. Otherwise, the Agent uses HTTP over port 80.

Provisioning the KACE SMA Agent to managed devices

The KACE SMA Agent is an application that can be installed on devices to enable device management and inventory reporting through the appliance. To provision the Agent software to devices directly from the appliance, you must have a VPN connection. However, there are alternative methods for deploying Agent software without VPN connectivity:

- Manually download and install the Agent on devices. For instructions, see the Administrator Guide.
- Install the Agent using Windows Group Policy (GPO). For more information, go to https://support.quest.com/kb/133776.
- Install the Agent using another management system: If the Quest solution is replacing another systems management solution, you can deploy the Agent using the distribution methods of the system being replaced prior to its decommission and cleanup.

Configuring KACE SMA Agent communication settings

Agents installed on managed devices periodically communicate with the appliance to report inventory, update scripts, and perform other tasks. You can configure the Agent settings, including the interval at which the Agents check in, messages displayed to users, and log retention time. If you have multiple organizations, you can configure Agent settings for each organization separately. For more information, see the KACE SMA Administrator Guide: Accessing the Administrator Guide and online Help.

About server monitoring

The appliance supports server monitoring, which provides basic performance and application monitoring for servers in inventory. You can enable monitoring for servers using the KACE SMA Agent, and for servers using Agentless management, and setup depends upon your IT department policies. Server monitoring is available for up to five servers using a standard appliance license, and you can obtain a license to increase that number.

If you enable monitoring for Agent-managed servers, alert information is transmitted over port 443 in addition to the existing Agent communication protocol. If you enable monitoring for servers using Agentless management, the appliance uses SSH or Telnet to connect to the server, read the logs, check for alerts, and display the alerts in the KACE SMA Administrator Console. Because VPN access is required for the use of SSH and Telnet, a VPN connection is required for Agentless server monitoring.

About file distribution (packages) and Replication Shares

With the appliance, every site is a remote site. Quest strongly recommends that you configure Replication Shares for each site to optimize bandwidth usage on the remote office Internet connections. Replication Shares are devices that keep copies of files for distribution, such as Managed Installations, patches, scripts, and Dell Updates.

With Samba file sharing turned off, file uploads to the appliance are limited to 2 GB. For files that exceed 2 GB, use an alternate download location to stage the files inside the corporate network.

An alternate download location can be any network location that has all the files required to install a particular application. You can distribute packages from alternate download locations including a UNC address or DFS source. The CIFS and SMB protocols, Samba servers, and file server appliances are supported. You specify the location when you create a Managed Installation. For more information, see the Distribution section of the KACE SMA Administrator Guide: Accessing the Administrator Guide and online Help.

About bandwidth usage and dedicated network bandwidth

The appliance uses a shared cloud network. To reduce the bandwidth requirements of the shared network, Quest strongly recommends the use of Replication Shares. If your appliance causes bandwidth issues on the shared network, you might be required to set up Replication Shares or purchase dedicated network bandwidth. For more information, contact Quest sales at https://quest.com/company/contact-us.aspx.

About data protection and security

The cloud Data Centers and Quest appliances have a Highly Available infrastructure and provide all the necessary protection and security for your appliance. For more information about appliance security settings, see the configuration section of the KACE SMA Administrator Guide: Accessing the Administrator Guide and online Help.

Using backup files

Backup files are used to restore your KACE as a Service appliance in the event of a data loss, or to preserve settings during upgrades, and Quest automatically makes offboard copies of the most recent nightly backup file for disaster recovery.

You can access backup files using the Administrator Console. If the files become too large to download using HTTP, you can access them using FTP. See Back up the appliance and enable FTP access. If network bandwidth is limited, consider using file distribution to download large backup files. See About file distribution (packages) and Replication Shares.

Restoring any type of backup file destroys the data currently configured in the appliance server. Quest recommends that you offload any backup files or data that you want to keep before you restore settings.

Configuring the appliance on the Internet

As with any web-server-based application, security best practices include limiting access to the KACE Systems Management Appliance (SMA) from the Internet. Careful consideration and review of the environment are necessary to ensure security. It is strongly recommended to consider firewalls, encryption, port access, roles, anti-virus, SSL, access control list, disaster recovery, and review the following topic prior to configuring the SMA on the Internet: https://support.quest.com/kb/267753/best-practices-for-securing-your-sma. At a minimum, if the KACE SMA is configured as internet/public facing, only port 443 (HTTPS) traffic should be allowed inbound through a firewall to the KACE SMA for UI access and agent communication traffic.

For more information, visit https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-.

Back up the appliance and enable FTP access

You can enable Quest to copy daily and monthly backup files to a local high-speed storage area by enabling FTP access and setting the FTP password to sepgetbxf as described in this section. FTP access requires a VPN connection.

1. In the Administrator Console, click Settings to go to the appliance Control Panel.
2. Click Security Settings.

   The Security Settings page appears.

3. In the top section, specify the following settings:

Option	Description
Enable backup via FTP	Select this check box to enable FTP access to backup files.
Make FTP writable	Select this check box to use FTP to upload backup files.
New FTP user password	Type the following password: sepgetbxf.

If the FTP user password is set, the backup server automatically copies daily and monthly backup files to a local high-speed storage area. For more information about managing backups, see the maintenance section of the KACE SMA Administrator Guide: Accessing the Administrator Guide and online Help.

Accessing the Administrator Guide and online Help

For help using the Administrator Console, click the Help link in the top-right corner of the interface to open the context-sensitive Help. To access the main Help system, click the links in context-sensitive Help topics.

Scheduling training

To help you begin using the appliance, Quest provides a training program called QuickStart. This program provides remote assistance to help get your solution up and running quickly to begin provisioning, managing, securing and servicing your network-connected devices.

Knowledge Base articles

For additional information, go to the Quest Support Knowledge Base site, https://support.quest.com/systems-management-appliance/kb .

- Network ports required by the appliance: https://support.quest.com/kb/111775
- Whitelisting required for patching: https://support.quest.com/kb/111785
- Installing the KACE SMA Agent using Windows Group Policy: https://support.quest.com/kb/133776
- Working with backup files: https://support.quest.com/kb/111736

About us

Quest provides software solutions for the rapidly-changing world of enterprise IT. We help simplify the challenges caused by data explosion, cloud expansion, hybrid datacenters, security threats, and regulatory requirements. We are a global provider to 130,000 companies across 100 countries, including 95% of the Fortune 500 and 90% of the Global 1000. Since 1987, we have built a portfolio of solutions that now includes database management, data protection, identity and access management, Microsoft platform management, and unified endpoint management. With Quest, organizations spend less time on IT administration and more time on business innovation. For more information, visit www.quest.com.

Technical support resources

Technical support is available to Quest customers with a valid maintenance contract and customers who have trial versions. You can access the Quest Support Portal at https://support.quest.com.

The Support Portal provides self-help tools you can use to solve problems quickly and independently, 24 hours a day, 365 days a year. The Support Portal enables you to:

- Submit and manage a Service Request
- View Knowledge Base articles
- Sign up for product notifications
- Download software and technical documentation
- View how-to-videos
- Engage in community discussions

- Chat with support engineers online
- View services to assist you with your product.

Configuration de l'appliance

Avant de commencer

Avant de configurer l'appliance, vous devez effectuer un certain nombre de tâches.

1. Assurez-vous de disposer d'un abonnement à Microsoft Azure. Lorsque vous installez votre appliance KACE SMA virtuelle, celle-ci s'exécute en tant que machine virtuelle dans le Cloud Azure. Pour plus d'informations sur la plate-forme Cloud Azure ou pour vous inscrire, voir http://azure.microsoft.com/en-us/.
2. Achetez une licence pour une appliance KACE SMA virtuelle Microsoft Azure auprès du service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx.
3. Assurez-vous que vos paramètres de réseau et de pare-feu autorisent un accès sortant vers KACE SMA sur le port 443. Ce port est utilisé pour les communications entre les consoles Web de l'appliance et l'agent via HTTPS. Il doit également être ouvert sur les appareils, notamment les ordinateurs de bureau et les serveurs, sur lesquels le logiciel de l'agent KACE SMA est installé :

Exceptions des fonctionnalités

Vous pouvez configurer toutes les fonctionnalités de la Console d'administration de l'appliance KACE SMA afin de les utiliser dans le Cloud. Cependant, certaines fonctionnalités nécessitent un accès direct à votre réseau, établi via une connexion VPN de site à site. Les connexions VPN exploitent le réseau partagé et une seule connexion VPN suffit généralement à activer la fonctionnalité pour une seule entreprise. Toutefois, dans certains cas, des connexions VPN supplémentaires, ainsi que de la bande passante réseau dédiée, peuvent être nécessaires. Pour plus d'informations, voir Utilisation de connexions VPN et de ressources réseau.

Fonctionnalités de la Console d'administration qui nécessitent une connexion VPN

Les fonctionnalités suivantes de la Console d'administration nécessitent une connexion VPN :

- Surveillance des serveurs à l'aide de la gestion des périphériques sans agent.
- Wake On LAN, découverte du réseau (notamment l'analyse IP, l'analyse Active Directory® et l'analyse NMAP), provisioning de l'agent KACE SMA à partir de l'appliance (voir Provisioning de l'agent KACE SMA sur des périphériques infogérés).

  Ces fonctionnalités ne nécessitent pas de VPN lorsque le relais d'agent est utilisé.

- Importation et exportation de ressources (le partage de fichiers est bloqué par le pare-feu du Cloud).

- Accès FTP aux fichiers de sauvegarde (l'accès FTP est bloqué par le pare-feu du Cloud).
- Les packages d'application et dépendances de script doivent être téléchargés via HTTP. Les téléchargements de packages volumineux peuvent expirer lorsque la connexion réseau est lente. Les packages de plus de 2 Go doivent être distribués via un autre emplacement de téléchargement à partir d'un serveur de fichiers interne.
- Étiquettes pour le périphérique et l'utilisateur LDAP.
- Authentification de l'utilisateur LDAP.
- Importation de l'utilisateur LDAP.
- Authentification unique Active Directory pour la Console d'administration et la Console utilisateur.

Exceptions concernant les fonctionnalités de la console utilisateur

La Console utilisateur est l'interface qui met les fonctionnalités de la Bibliothèque de logiciels et du Service Desk à la disposition des utilisateurs finaux. La fonctionnalité suivante de la Console utilisateur n'est pas prise en charge dans le Cloud :

- Installations automatiques de logiciels à partir de la Console utilisateur (les téléchargements sont pris en charge).

Création d'une machine virtuelle KACE SMA dans Azure

Cette rubrique décrit le processus de création d'une machine virtuelle (VM) dans Microsoft Azure pour servir d'appliance de gestion des systèmes (SMA) KACE à l'aide d'un modèle de machine virtuelle disponible sur Azure Marketplace.

Assurez-vous de disposer d'un abonnement Azure valide. Lorsque vous installez votre appliance KACE SMA virtuelle, celle-ci s'exécute en tant que machine virtuelle dans le Cloud Azure. Pour plus d'informations sur la plate-forme Cloud Azure ou pour vous inscrire, voir http://azure.microsoft.com/en-us/.

1. Connectez-vous à https://azuremarketplace.microsoft.com/ à l'aide de vos informations d'identification d'abonnement Azure.
2. Dans le champ Rechercher, saisissez KACE Systems Management Appliance.
3. Ouvrez l’application Appliance de gestion des systèmes KACE.
4. Consultez les informations de la section sur les plans et tarifs pour en savoir plus sur les ressources requises pour les machines virtuelles recommandées.
5. Cliquez sur OBTENIR MAINTENANT.

6. Cliquez sur Créer.

   La page Créer une machine virtuelle s'affiche, composée de plusieurs onglets. Certains de ces onglets contiennent les options requises pour configurer une machine virtuelle KACE SMA.

   > L'interface Azure change fréquemment. Certaines options peuvent ne pas correspondre précisément. Pour obtenir les informations les plus récentes sur cette page, rendez-vous sur le site https://docs.microsoft.com/en-us/azure/.

7. Sur la page Créer une machine virtuelle, dans l'onglet Informations de base, fournissez les informations suivantes :

Option	Description
Abonnement	Spécifiez le nom de votre abonnement Azure.
Groupe de ressources	Créez un groupe de ressources ou utilisez un groupe existant pour cette machine virtuelle.
Nom de la machine virtuelle	Saisissez le nom de la machine virtuelle que vous êtes sur le point de créer.
Image	Cette option affiche l'image de l'appliance de gestion des systèmes KACE sélectionnée.
Taille	a. Cliquez sur Modifier la taille. b. Sur la page Sélectionner une taille de machine virtuelle qui s'affiche, sélectionnez une configuration parmi les tailles de machine virtuelle recommandées, selon les besoins.
Type d'authentification	Fournissez les détails d'authentification du compte administrateur sur la machine virtuelle. > Les informations d'identification du compte administrateur ne seront pas utilisées pour accéder à l'appliance. Toutefois, ces informations sont obligatoires pour une machine virtuelle que vous créez dans Azure et vous devez les spécifier. a. Sélectionnez Mot de passe. b. Dans le champ Nom d'utilisateur, saisissez le nom d'utilisateur de l'administrateur de la machine virtuelle. c. Dans le champ Mot de passe, saisissez le mot de passe du compte administrateur.

8. Laissez toutes les autres options telles quelles, puis cliquez sur Suivant.
9. Dans l'onglet Disques, cliquez sur Type de disque du système d'exploitation et sélectionnez SDD premium. Il s'agit du minimum recommandé pour l'appliance.
10. Laissez toutes les autres options telles quelles, puis cliquez sur Suivant.
11. Dans l'onglet Mise en réseau, configurez les paramètres suivants :

Option	Description
Réseau virtuel	Sélectionnez un réseau virtuel existant ou créez-en un nouveau.
Sous-réseau	Sélectionnez un sous-réseau existant ou définissez-en un nouveau.
IP	Utilisez une adresse IP publique si vous souhaitez communiquer avec l'appliance SMA KACE depuis l'extérieur du réseau virtuel.

> Lorsque vous mettez à niveau l'appliance, pour suivre l'état de la mise à niveau dans le navigateur, vous devez ouvrir le port 52231. Fermez ce port lorsque la mise à niveau est terminée.

12. Laissez toutes les autres options de cet onglet et de tous les autres onglets telles quelles, puis cliquez sur Suivant jusqu'à atteindre l'onglet Révision.
13. Dans l'onglet Révision, cliquez sur Créer.

    Pendant le déploiement de la machine virtuelle, une barre de progression s'affiche dans le navigateur. Une fois l'opération terminée, une notification s'affiche brièvement et une vue d'ensemble de votre machine virtuelle s'affiche dans Azure.

Configuration de l'appliance

Utilisez l'assistant de configuration initiale pour configurer KACE en tant que service et vous connecter à l'appliance Console d'administration.

> Votre paramètre de navigateur détermine la langue affichée dans la Console d'administration au cours de votre première connexion. Pour plus d'informations sur la modification des paramètres de langue, consultez le Guide de l'administrateur de l'appliance : Accès au Guide de l'administrateur et à l'aide en ligne.

1. Obtenez le nom DNS complet de la machine virtuelle exécutant le logiciel de l'appliance dans Azure.
   a. Dans Azure, sélectionnez la machine virtuelle et accédez aux paramètres de présentation.
   b. Sur la page de présentation, cliquez sur Configurer et définissez un nom DNS pour l'appliance SMA KACE. Par exemple, my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com.

   Pour plus d'informations sur ces paramètres, voir https://docs.microsoft.com/en-us/azure/.

2. Ouvrez un navigateur Web et saisissez l'URL Console d'administration en utilisant la syntaxe suivante :

   http://<nom_appliance_SMA_KACE_unique>/admin

   Où <nom_appliance_SMA_KACE_unique> est le nom DNS complet de la machine virtuelle que vous avez configurée à l'étape 1.

   Par exemple : http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

   La page Contrat de transaction du logiciel apparaît.

3. Acceptez le contrat.

   L'assistant Installation initiale s'affiche.

4. Dans l'assistant de configuration initiale, sur la page d'accueil, vérifiez que vous disposez des informations nécessaires à la configuration de l'appareil, puis cliquez sur Suivant.
5. Sur la page Authentification à deux facteurs de la Console de diagnostic, vérifiez et enregistrez la clé secrète et les jetons hors ligne, puis cliquez sur Suivant.
6. À la page Paramètres de licence et d'administrateur, fournissez les informations suivantes :

Option	Description
Clé de licence	Saisissez la clé de licence que vous avez reçue dans le courrier électronique de bienvenue envoyé par Quest. Si vous ne disposez d'aucune clé de licence, contactez le Support Quest Software à l'adresse https://support.quest.com/contact-support.
Nom de l'entreprise	Nom de votre entreprise ou organisation.
E-mail de l'administrateur	Adresse e-mail à laquelle vous souhaitez recevoir les communications de Quest.
Mot de passe	Mot de passe du compte admin par défaut, qui est le compte que vous utilisez pour vous connecter à la Console d'administration de l'appliance. Le compte admin par défaut est le seul compte défini sur l'appliance à ce stade. Si vous oubliez le mot de passe de ce compte, il vous faudra probablement rétablir les paramètres d'usine par défaut du système, ce qui peut entraîner une perte de données. Si vous disposez de plusieurs appliances KACE SMA ou KACE SDA (déploiement des systèmes), Quest vous recommande d'utiliser un mot de passe identique pour le compte admin de chaque appliance. Cela vous

Option	Description
	permet de lier les appliances entre elles par la suite. Pour plus d'informations, consultez le Guide de l'administrateur de l'appliance : Accès au Guide de l'administrateur et à l'aide en ligne.
Authentification bifactorielle	Si vous voulez fournir une sécurité accrue aux utilisateurs se connectant à l'appliance, définissez cette option sur Activé. Cette fonction ajoute une étape au processus de connexion. Elle s'appuie sur l'application Google Authenticator pour générer des codes de vérification. L'application génère un nouveau code à six chiffres à intervalles réguliers. Lorsque cette option est activée, les utilisateurs sont invités à saisir le code de vérification actif à chaque connexion. Si vous activez cette fonction, assurez-vous que l'horloge du serveur KACE SMA est précise, ainsi que sur le périphérique exécutant Google Authenticator. Google Authenticator s'appuie sur l'heure actuelle pour créer le jeton. Si l'horloge du serveur n'est pas synchronisée avec celles des périphériques exécutant Google Authenticator, la validation du jeton peut échouer, ce qui peut entraîner le verrouillage du compte.

Cliquez ensuite sur Suivant.

7. Sur la page Activer le partage de fichiers, suivez les instructions à l'écran pour exécuter cette étape.
8. Sur la page Paramètres de domaine, indiquez le fuseau horaire, le nom d'hôte et le nom de domaine de votre appliance.

   Cette page permet également d'activer les paramètres DNS personnalisés. Une installation par défaut utilise les serveurs DNS fournis par Azure.

   Lorsque vous configurez un réseau privé virtuel de site à site, vous pouvez également utiliser votre IP DNS soit pour rendre l'appareil accessible à la fois aux réseaux internes et publics (recommandé), ou uniquement au réseau interne, en fonction de votre configuration DNS. Pour ce faire, sélectionnez Activer DNS personnalisé et dans le champ DNS principal, saisissez votre adresse IP DNS. Pour plus d'informations, consultez le sommaire de l'aide sur cette page.

   Cliquez ensuite sur Suivant.

9. Sur la page Confirmation, vérifiez votre configuration.

   Si vous souhaitez apporter des modifications, utilisez le bouton Retour de l'assistant pour passer à l'étape appropriée et mettre à jour votre configuration.

   Lorsque vous avez fini, cliquez sur Terminer.

   Une fois la configuration initiale terminée, l'appliance redémarre, puis la page de connexion à la Console d'administration s'affiche.

10. Connectez-vous à la Console d'administration avec l'ID de connexion admin et le mot de passe que vous avez défini lors de la configuration initiale.

    Si l'authentification à deux facteurs a été activée sur la page Paramètres de licence et d'administrateur de l'assistant de configuration initiale, la page Configurer l'authentification à deux facteurs s'affiche.

11. Authentification à deux facteurs uniquement. Suivez les instructions figurant sur la page Configurer l'authentification à deux facteurs pour générer un code de vérification Google Authenticator en utilisant votre smartphone. Dans le champ Code de vérification, saisissez le code d'authentification Google Authenticator et cliquez sur Terminer la configuration. Un nouveau code de vérification est nécessaire pour chaque nouvelle connexion.

    Pour ignorer cette étape, cliquez sur Ignorer la configuration. Vous ne pouvez ignorer cette étape que pendant une fenêtre de transition configurée. Pour plus d'informations à ce sujet, consultez le document Administrator Guide (Guide de l'administrateur).

12. Indiquez le nom DNS complet de l'appliance dans les Paramètres réseau. Lorsque vous redémarrez l'appliance dans Azure, son adresse IP change. Les périphériques se connectent à l'appliance en utilisant ce nom.
    a. Connectez-vous au KACE SMAConsole d'administration et cliquez sur Paramètres.
    b. Dans le Panneau de configuration de l'appliance qui s'affiche, cliquez sur Paramètres réseau.
    c. Sur la page Paramètres réseau, dans la section Configuration réseau de l'appliance, dans le champ Nom du serveur Web, saisissez le nom DNS complet d'appliance enregistrée à l'étape 3.
    d. Cliquez sur Enregistrer.

    > **!** La console de ligne de commande est une interface de fenêtre de terminal de l'appliance. Cet outil vous permet de configurer les paramètres réseau. Vous ne devez pas utiliser cet outil pour modifier l'adresse IP de l'appliance exécutée dans Azure.

La Console d'administration s'affiche et vous pouvez utiliser l'appliance.

Activer SSL

Vous devez activer les communications sécurisées entre l'appliance et les périphériques infogérés et vous pouvez utiliser la Console d'administration de l'appliance pour générer un certificat SSL.

Obtenez un nom de domaine enregistré à utiliser pour l'appliance. Cette étape est obligatoire si vous souhaitez générer une requête de signature de certificat SSL à l'aide de la Console d'administration de l'appliance.

1. Dans la Console d'administration, cliquez sur Paramètres pour accéder au Panneau de configuration de l'appliance.
2. Cliquez sur Paramètres de sécurité.

   La page Paramètres de sécurité apparaît.
3. Dans la section SSL en bas de la page, désactivez l'accès au port HTTP 80 et transférez tout le trafic du port 80 vers le port HTTPS 443.

   ! Si le port 80 n'est pas désactivé, les données sensibles, telles que les mots de passe, sont transmises en texte brut sur Internet.

   - Désélectionnez Activer l'accès au port 80.
   - Sélectionnez Activer SSL et Passer du port 80 au port 443.
4. Cliquez sur Formulaire du certificat SSL pour accéder à la page Formulaire du certificat SSL.
5. Dans la section Configurer, entrez les informations suivantes :

Option	Description
Nom de l'entreprise	Nom de votre entreprise.
Nom de l'organisation	Nom de votre groupe ou unité organisationnelle.
Nom courant	Nom courant de l'appliance pour laquelle vous créez le certificat SSL.
Messagerie	Votre adresse e-mail.
Nom de la ville	Nom de votre localité.
Nom de l'État/province	Nom de votre état ou province.
Nom du pays	Nom de votre pays.

6. Cliquez sur Enregistrer.
7. Générez un certificat auto-signé.
   a. Cliquez sur Générer un certificat auto-signé pour générer et afficher le certificat sous la section Demande de signature de certificat.
   b. Cliquez sur Déployer le certificat auto-signé, puis cliquez sur Oui.
   c. Sur la page Paramètres de sécurité, cliquez sur Enregistrer et redémarrer les services.

   Le certificat SSL est généré. Les certificats auto-signés sont convertis en fichiers PEM, intitulés kbox.pem et ils sont placés dans des dossiers de données de l'agent KACE SMA. Pour en savoir plus sur les paramètres de sécurité, consultez le Guide de l'administrateur.

Si vous créez un certificat autosigné, vous devez le déployer sur tous les périphériques gérés par l'agent.

8. Redémarrez l'appliance.

Pratiques d'excellence

Suivez les consignes et les recommandations de cette section lors de l'utilisation de l'appliance.

Utilisation de connexions VPN et de ressources réseau

Si vous utilisez une communication agent-serveur traditionnelle entre l'appliance et vos périphériques infogérés, il vous suffit d'installer l'agent sur les périphériques infogérés pour permettre la communication. Cependant, si vous utilisez une connexion VPN, vous devez établir la liaison réseau de votre environnement vers l'appliance. L'équipe de l'appliance peut vous conseiller, notamment en termes d'adresses IP et de ports à autoriser, et il est important que votre administrateur réseau soit impliqué dans le processus de configuration. Les connexions Cloud appropriées sont configurées et vous devez vérifier la connexion de votre côté pour le bon déroulement de la configuration.

De plus, certaines fonctionnalités de l'appliance nécessitent une connexion VPN dans le Cloud et une connexion VPN unique est généralement suffisante pour une seule entreprise. Par exemple, vous pouvez utiliser une seule connexion VPN même si vous avez des emplacements distants, à condition que ces emplacements puissent router le trafic via le site d'entreprise principal où se trouve la connexion VPN. L'ensemble du trafic de l'agent KACE SMA est routé via le VPN puis jusqu'à l'appliance par le biais de la connexion VPN. Si les emplacements distants ne parviennent pas à voir le site d'entreprise principal, ou si vous souhaitez que chaque site ait un lien VPN direct vers l'appliance, vous devez acheter une connexion VPN pour chaque site. Pour plus d'informations sur les fonctionnalités qui nécessitent des connexions VPN, voir Exceptions des fonctionnalités.

Le prix du produit est basé sur la bande passante du réseau partagé. Pour acheter des ressources réseau supplémentaires, ou pour acheter des connexions VPN, contactez le service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx.

Utilisation de connexions VPN avec plusieurs domaines

L'appliance a été conçue pour être utilisée avec un seul domaine et une seule connexion VPN. Si vous avez plusieurs domaines, vous pouvez gérer vos périphériques (inventaire) sur d'autres domaines via l'appliance, mais les fonctionnalités qui nécessitent un accès VPN ne sont accessibles qu'à un seul domaine. Par exemple, vous pouvez vous authentifier sur un environnement Active Directory pour Identity Access Management, mais vous ne pouvez pas vous authentifier sur plusieurs domaines. Le trafic de l'agent à partir du domaine avec la connexion VPN est routé via la connexion VPN, tandis que le trafic de l'agent pour les autres

domaines se connecte à l'appliance via un accès Internet standard. Pour plus d'informations sur les fonctionnalités qui nécessitent des connexions VPN, voir Exceptions des fonctionnalités.

À propos de l'adresse IP de l'appliance

L'appliance est configurée pour une seule adresse IP. Cette adresse IP est attribuée par Quest et ne peut pas être modifiée. Vous devez créer un enregistrement hôte (A) dans votre serveur DNS (Domain Name System) interne pour l'adresse IP statique de l'appliance et vous pouvez créer plusieurs enregistrements A (hôtes) sur plusieurs réseaux ou domaines afin qu'ils renvoient vers votre appliance. Si vous avez besoin d'utiliser plusieurs adresses IP publiques pour votre réseau, vous devez acheter une instance séparée de l'appliance. Plusieurs instances d'appliance ne peuvent pas partager des données ou des informations de base de données. Pour en savoir plus, contactez le service commercial Quest à l'adresse https://www.quest.com/company/contact-us.aspx.

À propos des paramètres réseau

Par défaut, tous les protocoles réseau et les services qui y sont associés sont désactivés, excepté HTTPS et HTTP. Ces protocoles sont utilisés pour les interfaces utilisateur de l'appliance et les communications de l'agent KACE SMA. Lorsque le logiciel de l'agent KACE SMA est provisionné sur un périphérique, l'agent tente toujours de se connecter à l'appliance à l'aide de HTTPS sur le port 443 pour les communications chiffrées si SSL est activé. Dans le cas contraire, l'agent utilise HTTP sur le port 80.

Provisioning de l'agent KACE SMA sur des périphériques infogérés

L'agent KACE SMA est une application qui peut être installée sur les périphériques afin de permettre la gestion des périphériques ainsi que la création de rapports d'inventaire par le biais de l'appliance. Pour assurer le provisioning du logiciel de l'agent sur des périphériques directement à partir de l'appliance, vous devez avoir une connexion VPN. Il y a toutefois d'autres méthodes permettant de déployer le logiciel de l'agent sans connectivité VPN :

- Téléchargez et installez l'agent manuellement sur les périphériques. Pour obtenir des instructions, consultez le Guide de l'administrateur.
- Installer l'agent à l'aide de la stratégie de groupe Windows. Pour plus d'informations, rendez-vous sur https://support.quest.com/kb/133776.
- Installer l'agent à l'aide d'un autre système de gestion : Si la solution Quest remplace une autre solution de gestion de systèmes, vous pouvez déployer l'agent en utilisant les méthodes de distribution du système qui est remplacé avant sa mise hors service et son nettoyage.

Configuration des paramètres de communication de l'agent KACE SMA

Les agents installés sur les périphériques infogérés communiquent régulièrement avec l'appliance pour établir un rapport d'inventaire, mettre à jour des scripts et effectuer d'autres tâches. Vous pouvez configurer les paramètres d'agent, notamment la fréquence à laquelle les agents se connectent, les messages affichés aux utilisateurs et le délai de conservation des fichiers journaux. En présence de plusieurs organisations, il est possible de configurer les paramètres d'agent pour chacune d'elles. Pour plus d'informations, consultez le Guide de l'administrateur du KACE SMA : Accès au Guide de l'administrateur et à l'aide en ligne.

À propos de la surveillance des serveurs

L'appliance prend en charge la surveillance des serveurs, ce qui offre une surveillance de base des performances et applications pour les serveurs dans l'inventaire. Vous pouvez activer la surveillance pour les serveurs utilisant l'agent KACE SMA et pour les serveurs utilisant la gestion sans agent. La configuration dépend des stratégies de votre service informatique. Vous pouvez surveiller jusqu'à cinq serveurs avec une licence d'appliance standard, et vous pouvez obtenir une licence supplémentaire afin d'augmenter le nombre de serveurs.

Si vous activez la surveillance pour les serveurs gérés par l'agent, les informations relatives aux alertes sont transmises via le port 443 en plus du protocole de communication de l'agent existant. Si vous activez la surveillance pour les serveurs utilisant la gestion sans agent, l'appliance utilise SSH ou Telnet pour se connecter au serveur, lire les journaux, rechercher et afficher les alertes dans la Console d'administration du KACE SMA. Étant donné qu'un accès VPN est nécessaire pour utiliser SSH et Telnet, la surveillance des serveurs sans agent requiert une connexion VPN.

À propos de la distribution de fichiers (packages) et des partages de réplication

Avec l'appliance, chaque site est un site distant. Quest vous recommande vivement de configurer des partages de réplication pour chaque site afin d'optimiser l'utilisation de la bande passante sur les connexions Internet des sites distants. Les partages de réplication sont des périphériques qui conservent des copies des fichiers à des fins de distribution, tels que les installations infogérées, les correctifs, les scripts et les mises à jour Dell.

Lorsque le partage de fichiers Samba est désactivé, les téléchargements de fichiers vers l'appliance sont limités à 2 Go. Pour les fichiers qui dépassent 2 Go, utilisez un autre emplacement de téléchargement pour placer les fichiers sur le réseau d'entreprise.

L'autre emplacement de téléchargement peut être un emplacement réseau contenant tous les fichiers requis pour installer une application donnée. Vous pouvez distribuer des packages à partir d'autres emplacements de téléchargement, y compris une adresse UNC ou une source DFS. Les protocoles CIFS et SMB, les serveurs Samba et les appliances serveurs de fichiers sont pris en charge. Vous spécifiez l'emplacement lorsque vous créez une installation infogérée. Pour plus

d'informations, consultez la section Distribution du Guide de l'administrateur du KACE SMA : Accès au Guide de l'administrateur et à l'aide en ligne.

À propos de l'utilisation de la bande passante et de la bande passante réseau dédiée

L'appliance utilise un réseau Cloud partagé. Pour réduire le besoin en bande passante du réseau partagé, Quest recommande vivement l'utilisation de partages de réplication. Si votre appliance entraîne des problèmes de bande passante sur le réseau partagé, vous devrez peut-être configurer des partages de réplication ou acheter de la bande passante réseau dédiée. Pour en savoir plus, contactez le service commercial Quest à l'adresse https://quest.com/company/contact-us.aspx.

À propos de la protection des données et de la sécurité

Les centres de données dans le Cloud et les appliances Quest ont une infrastructure hautement disponible et offrent toute la protection et la sécurité nécessaires à votre appliance. Pour plus d'informations sur les paramètres de sécurité de l'appliance, reportez-vous à la section relative à la configuration du Guide de l'administrateur du KACE SMA : Accès au Guide de l'administrateur et à l'aide en ligne.

Sécurisation des fichiers de sauvegarde

Les fichiers de sauvegarde vous permettent de restaurer votre appliance KACE en tant que service en cas de perte de données ou de préserver des paramètres pendant les mises à jour. Quest crée automatiquement des copies externes du fichier de sauvegarde quotidienne le plus récent à des fins de reprise après sinistre.

Vous pouvez accéder aux fichiers de sauvegarde à l'aide de la Console d'administration. Si les fichiers deviennent trop volumineux pour être téléchargés via HTTP, vous pouvez y accéder via FTP. Voir Sauvegarde de l'appliance et activation de l'accès FTP. Si la bande passante du réseau est limitée, pensez à utiliser la distribution de fichiers pour télécharger les fichiers de sauvegarde volumineux. Voir À propos de la distribution de fichiers (packages) et des partages de réplication.

La restauration d'un fichier de sauvegarde, quel que soit le type de fichier, détruit les données actuellement configurées dans le serveur de l'appliance. Avant de restaurer les paramètres, Quest recommande de décharger tous les fichiers de sauvegarde et les données que vous souhaitez conserver.

Configuration de l’appliance sur Internet

Comme pour toute application basée sur serveur Web, les meilleures pratiques de sécurité incluent la limitation de l’accès à l’appliance de gestion des systèmes (SMA) KACE depuis

Internet. Il est nécessaire de faire attention à l'environnement et de le vérifier attentivement pour garantir la sécurité. Il est fortement recommandé de prendre en compte les pare-feu, le chiffrement, l'accès aux ports, les rôles, l'antivirus, le SSL, la liste de contrôle d'accès, la récupération en cas de sinistre et de consulter la rubrique suivante avant de configurer le SMA sur Internet : https://support.quest.com/kb/267753/best-practices-for-securing-your-sma. Au minimum, si le SMA KACE est configuré en tant qu'interface Internet/publique, seul le trafic du port 443 (HTTPS) doit être autorisé en entrée, via un pare-feu vers le SMA KACE pour l'accès à l'interface utilisateur et le trafic de communication des agents.

Pour plus d'informations, visitez le site https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-.

Sauvegarde de l'appliance et activation de l'accès FTP

Vous pouvez activer l'option permettant à Quest de copier les fichiers des sauvegardes quotidiennes et mensuelles vers une zone de stockage haut débit locale en activant l'accès FTP et en définissant le mot de passe FTP sur sepgetbxf, comme indiqué dans cette section. L'accès FTP nécessite une connexion VPN.

1. Dans la Console d'administration, cliquez sur Paramètres pour accéder au Panneau de configuration de l'appliance.
2. Cliquez sur Paramètres de sécurité.

   La page Paramètres de sécurité apparaît.
3. Dans la section supérieure, spécifiez les paramètres ci-dessous :

Option	Description
Activer la sauvegarde via FTP	Cochez cette case pour permettre l'accès aux fichiers de sauvegarde via FTP.
Accéder en écriture à FTP	Cochez cette case pour télécharger les fichiers de sauvegarde via FTP.
Nouveau mot de passe d'utilisateur FTP	Saisissez le mot de passe suivant : sepgetbxf.

Si le mot de passe utilisateur FTP est défini, le serveur de sauvegarde copie automatiquement les fichiers des sauvegardes quotidiennes et mensuelles sur une zone de stockage haut débit locale. Pour plus d'informations sur la gestion des sauvegardes, reportez-vous à la section relative à la maintenance du Guide de l'administrateur du KACE SMA : Accès au Guide de l'administrateur et à l'aide en ligne.

Accès au Guide de l'administrateur et à l'aide en ligne

Pour obtenir de l'aide sur l'utilisation de la Console d'administration, cliquez sur le lien Aide situé en haut à droite de l'interface pour ouvrir l'aide contextuelle. Pour accéder au système d'aide principal, cliquez sur les liens des rubriques de l'aide contextuelle.

Programmation des formations

Afin de vous aider à commencer à utiliser l'appliance, Quest propose un programme de formations appelé QuickStart. Ce programme fournit une assistance à distance pour aider à obtenir votre solution rapidement afin de commencer l'approvisionnement, la gestion, la sécurité et la maintenance de vos périphériques connectés au réseau.

Articles de la base de connaissances

Pour plus d'informations, rendez-vous sur le site de la base de connaissances du support Quest, https://support.quest.com/systems-management-appliance/kb .

- Ports réseau requis par l'appliance : https://support.quest.com/kb/111775
- Liste blanche nécessaire à l'application de correctifs : https://support.quest.com/kb/111785
- Installation de l'agent KACE SMA à l'aide de la stratégie de groupe Windows : https://support.quest.com/kb/133776
- Utilisation des fichiers de sauvegarde : https://support.quest.com/kb/111736

Qui nous sommes

Quest propose des solutions logicielles pour le monde en constante évolution de l'informatique d'entreprise. Nous vous aidons à simplifier les défis liés à l'explosion des données, à l'expansion du Cloud, aux datacenters hybrides, aux menaces de sécurité et aux exigences réglementaires. Nous sommes le fournisseur mondial de 130 000 entreprises réparties dans 100 pays, dont 95 % sont des entreprises figurant dans le classement Fortune 500 et 90 % dans le classement Global 1000. Depuis 1987, nous avons développé un portefeuille de solutions qui comprend désormais la gestion des bases de données, la protection des données, la gestion des identités et des accès, la gestion des plates-formes Microsoft et la gestion unifiée des points de terminaison. Avec Quest, les entreprises consacrent moins de temps à l'administration informatique et plus de temps à l'innovation. Pour plus d'informations, visitez le site www.quest.com.

Ressources du support technique

Le support technique est disponible pour les clients Quest disposant d'un contrat de maintenance valide et les clients qui utilisent des versions d'évaluation. Vous pouvez accéder au portail du support technique Quest à l'adresse https://support.quest.com/fr-fr/.

Ce portail propose des outils d'auto-dépannage qui vous permettront de résoudre des problèmes rapidement et sans aide extérieure, 24 h/24 et 365 j/an. Il permet d'effectuer les opérations suivantes :

- Soumettre et gérer une demande de service
- Consulter les articles de la base de connaissances
- Vous inscrire pour recevoir des notifications sur les produits
- Télécharger des logiciels et de la documentation technique
- Visionner des vidéos de procédure
- Participer aux discussions de la communauté
- Discuter en ligne avec des ingénieurs du support technique
- Découvrir des services capables de vous aider avec votre produit.

Einrichten der Appliance

Vorbereitung

Vor dem Einrichten der Appliance müssen Sie einige Vorbereitungen treffen.

1. Stellen Sie sicher, dass Sie über ein Abonnement für Microsoft Azure verfügen. Wenn Sie Ihre virtuelle KACE SMA installieren, wird die Appliance als virtuelle Maschine in der Cloud von Azure ausgeführt. Weitere Informationen zur Cloud-Plattform von Azure oder zur Anmeldung finden Sie unter http://azure.microsoft.com/en-us/.
2. Erwerben Sie eine Lizenz für eine Microsoft Azure Virtual KACE SMA beim Quest Vertrieb unterhttps://www.quest.com/company/contact-us.aspx.
3. Stellen Sie sicher, dass Ihre Netzwerk- und Firewall-Einstellungen den ausgehenden Zugriff auf die KACE SMA an Port 443 ermöglichen. Dieser Port wird für die webbasierten Konsolen der Appliance und die Agentenkommunikation über HTTPS verwendet. Er sollte auch auf Geräten, einschließlich Desktops und Servern, offen sein, auf denen die KACE SMA Agenten-Software installiert werden soll.

Funktionsausnahmen

Sämtliche Funktionalität der KACE SMA Administratorkonsole kann für die Verwendung innerhalb der Cloud konfiguriert werden. Einige Funktionen erfordern jedoch den direkten Zugriff auf Ihr Netzwerk, der über eine VPN-Verbindung von Standort zu Standort hergestellt wird. VPN-Verbindungen nutzen das gemeinsame Netzwerk – eine einzelne VPN-Verbindung reicht hierbei für gewöhnlich aus, um die Funktionalität für ein einzelnes Unternehmen zu aktivieren. In einigen Fällen sind jedoch möglicherweise zusätzliche VPN-Verbindungen sowie dedizierte Netzwerkbandbreite erforderlich. Weitere Informationen hierzu finden Sie unter Verwenden von VPN-Verbindungen und Netzwerkressourcen.

Administratorkonsole-Funktionen, die eine VPN-Verbindung erfordern

Die folgenden Funktionen der Administratorkonsole erfordern eine VPN-Verbindung:

- Serverüberwachung mithilfe der Geräteverwaltung ohne Agenten-Software
- Wake-On-LAN, Netzwerkerkennung (einschließlich IP-Scan, Active Directory®-Scan und NMAP-Scan), KACE SMA Agent-Bereitstellung über die Appliance (siehe Provisionierung des KACE SMA Agenten auf verwalteten Geräten).

> Für diese Funktionen ist kein VPN erforderlich, wenn das Agent-Relay verwendet wird.

- Importieren und Exportieren von Ressourcen (Dateifreigabe wird von der Cloud-Firewall blockiert).
- FTP-Berechtigung für Sicherungsdateien (FTP-Zugang wird von der Cloud-Firewall blockiert).
- Anwendungspakete und Skriptabhängigkeiten müssen über HTTP hochgeladen werden. Große Pakete können bei langsamen Netzwerkanschlüssen ein Timeout verursachen. Pakete von mehr als 2 GB müssen über eine alternative Download-Quelle von einem internen Dateiserver verteilt werden.
- LDAP-Benutzer- und -Gerätelabel
- LDAP-Benutzerauthentifizierung
- LDAP-Benutzerimport
- Einmalige Active Directory-Anmeldung für die Administratorkonsole und Benutzerkonsole

Funktionsausnahmen der Benutzerkonsole

Die Benutzerkonsole ist die Schnittstelle, die Funktionen der Softwarebibliothek und des Service Desk für Enduser verfügbar macht. Die folgende Funktion der Benutzerkonsole wird in der Cloud nicht unterstützt:

- Automatische Softwareinstallationen über die Benutzerkonsole (Downloads werden unterstützt)

Erstellen einer virtuellen KACE SMA Maschine in Azure

In diesem Thema wird der Prozess der Erstellung einer virtuellen Maschine (VM) in Microsoft Azure beschrieben, die als KACE Systems Management Appliance (SMA) unter Verwendung einer VM-Vorlage verwendet wird, die über den Azure Marketplace verfügbar ist.

Stellen Sie sicher, dass Sie über ein gültiges Azure Abonnement verfügen. Wenn Sie Ihre virtuelle KACE SMA installieren, wird die Appliance als virtuelle Maschine in der Cloud von Azure ausgeführt. Weitere Informationen zur Cloud-Plattform von Azure oder zur Anmeldung finden Sie unter http://azure.microsoft.com/en-us/.

1. Melden Sie sich mit Ihren Azure-Anmeldedaten bei https://azuremarketplace.microsoft.com/ an.
2. Geben Sie im Feld Suche KACE Systems Management Appliance ein.
3. Öffnen Sie die KACE Systems Management Appliance-Anwendung.
4. Lesen Sie die Informationen im Abschnitt Pläne + Preise, um sich über die empfohlenen Ressourcenanforderungen für virtuelle Maschinen zu informieren.
5. Klicken Sie auf JETZT KAUFEN.

6. Klicken Sie auf Erstellen.

   Die Seite Virtuelle Maschine erstellen wird angezeigt, die aus mehreren Registerkarten besteht. Einige dieser Registerkarten enthalten Optionen, die zum Konfigurieren einer KACE SMA VM erforderlich sind.

   > Die Azure Schnittstelle ändert sich häufig. Einige Optionen stimmen möglicherweise nicht genau überein. Aktuelle Informationen zu dieser Seite finden Sie unter https://docs.microsoft.com/en-us/azure/.

7. Geben Sie auf der Seite Virtuelle Maschine erstellen auf der Registerkarte Basics die folgenden Informationen an.

Option	Beschreibung
Abonnement	Geben Sie den Namen Ihres Azure Abonnements an.
Ressourcengruppe	Erstellen Sie eine Ressourcengruppe oder verwenden Sie eine vorhandene Ressourcengruppe für diese virtuelle Maschine.
Name der virtuellen Maschine	Geben Sie den Namen der virtuellen Maschine ein, die Sie erstellen möchten.
Image	Mit dieser Option wird das ausgewählte KACE Systems Management Appliance-Image angezeigt.
Größe	a. Klicken Sie auf Größe ändern. b. Wählen Sie auf der angezeigten Seite VM-Größe auswählen nach Bedarf eine Konfiguration aus den empfohlenen VM-Größen aus.
Authentifizierungstyp	Geben Sie die Authentifizierungsdetails für das Administratorkonto auf der virtuellen Maschine an. > Administrator-Anmeldeinformationen werden nicht für den Zugriff auf die Appliance verwendet. Diese Informationen sind jedoch für alle virtuellen Maschinen, die Sie in Azure erstellen, obligatorisch, und Sie müssen sie angeben. a. Wählen Sie Kennwort aus. b. Geben Sie im Feld Benutzername den Benutzernamen des Administrators der virtuellen Maschine ein.

Option	Beschreibung
	c. Geben Sie im Feld Kennwort das Kennwort des Administratorkontos ein.

8. Lassen Sie alle anderen Optionen unverändert und klicken Sie auf Weiter.
9. Klicken Sie auf der Registerkarte Datenträger auf BS-Datenträgertyp und wählen Sie Premium-SSD aus. Dies ist das empfohlene Minimum für die Appliance.
10. Lassen Sie alle anderen Optionen unverändert und klicken Sie auf Weiter.
11. Konfigurieren Sie auf der Registerkarte Netzwerk die folgenden Optionen:

Option	Beschreibung
Virtuelles Netzwerk	Wählen Sie ein vorhandenes virtuelles Netzwerk aus oder erstellen Sie ein neues.
Subnetz	Wählen Sie ein vorhandenes Subnetz aus oder definieren Sie ein neues.
IP	Verwenden Sie eine öffentliche IP-Adresse, wenn Sie von außerhalb des virtuellen Netzwerks mit der KACE SMA kommunizieren möchten.

Wenn Sie die Appliance aktualisieren, müssen Sie Port 52231 öffnen, um den Aktualisierungsstatus im Browser zu verfolgen. Schließen Sie diesen Port, sobald die Aktualisierung erfolgreich durchgeführt wurde.

12. Lassen Sie alle anderen Optionen und alle übrigen Registerkarten unverändert und klicken Sie auf Weiter, bis Sie die Registerkarte Überprüfen erreichen.
13. Klicken Sie auf der Registerkarte Überprüfen auf Erstellen.

    Während die VM bereitgestellt wird, wird im Browser eine Fortschrittsleiste angezeigt. Nach Abschluss wird kurz eine Benachrichtigung angezeigt und in Azure wird eine Übersicht mit Details zu Ihrer VM angezeigt.

Konfigurieren der Appliance

Verwenden Sie den Assistenten für die Ersteinrichtung, um die Appliance zu konfigurieren und sich bei Administratorkonsole anzumelden.

Die Sprache, in der Ihnen die Administratorkonsole bei Ihrer ersten Anmeldung angezeigt wird, ist durch Ihre Browsereinstellungen festgelegt. Informationen zum Ändern der Spracheinstellungen finden Sie im Administratorhandbuch der Appliance: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

1. Ermitteln Sie den vollständig qualifizierten DNS-Namen der virtuellen Maschine, auf der die Appliance-Software in Azure ausgeführt wird.

a. Wählen Sie in Azure die virtuelle Maschine aus und navigieren Sie zu den Einstellungen Übersicht.

b. Klicken Sie auf der Seite Übersicht auf Konfigurieren und legen Sie einen DNS-Namen für die KACE SMA fest. Zum Beispiel: my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com.

Weitere Informationen zu diesen Einstellungen finden Sie unter https://docs.microsoft.com/en-us/azure/.

2. Öffnen Sie einen Webbrowser und geben Sie die Administratorkonsole-URL mit der folgenden Syntax ein:

   http://<unique_KACE_SMA_appliance_name>/admin

   Dabei ist <unique_KACE_SMA_appliance_name> der vollständig qualifizierte DNS-Name der virtuellen Maschine, den Sie in Schritt 1 konfiguriert haben.

   Beispiel: http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

   Die Seite Softwareübertragungsvereinbarung wird angezeigt.

3. Stimmen Sie der Vereinbarung zu.

   Der Assistent für die Ersteinrichtung wird angezeigt.

4. Vergewissern Sie sich, dass im Assistenten für die Ersteinrichtung auf der Seite Willkommen die erforderlichen Informationen zur Konfiguration der Appliance vorhanden sind und klicken Sie anschließend auf Weiter.
5. Überprüfen und erfassen Sie auf der Seite Diagnosekonsole für Zweifaktor-Authentifizierung den geheimen Schlüssel und die Offline-Tokens und klicken Sie anschließend auf Weiter.
6. Geben Sie auf der Seite Lizenzierungs- und Administratoreinstellungen folgende Informationen an:

Option	Beschreibung
Lizenzschlüssel	Der Lizenzschlüssel, den Sie in der Begrüßungs-E-Mail von Quest erhalten haben. Wenn Sie keinen Lizenzschlüssel besitzen, wenden Sie sich an den Quest Softwaresupport unter https://support.quest.com/contact-support.
Name der Firma	Der Name Ihrer Firma oder Gruppe.
E-Mail-Adresse des Administrators	Die E-Mail-Adresse, an die Sie Kommunikation von Quest erhalten möchten.
Kennwort	Das Kennwort für das Standardkonto admin. Mit diesem Konto melden Sie sich bei der Administratorkonsole der Appliance an. Das Standardkonto admin ist zu diesem Zeitpunkt das einzige Konto der Appliance. Wenn Sie das Kennwort für dieses Konto vergessen,

Option	Beschreibung
	muss das System möglicherweise auf die Werkseinstellungen zurückgesetzt werden, was einen Datenverlust zur Folge haben kann. Wenn Sie über mehrere KACE SMA oder KACE SDA (Systembereitstellung) Appliances verfügen, empfiehlt Quest, für alle Appliances dasselbe Kennwort für das admin-Konto zu verwenden. Dadurch können Sie die Appliances später verknüpfen. Weitere Informationen hierzu finden Sie im Administratorhandbuch der Appliance: Zugriff auf das Administratorhandbuch und die Onlinehilfe.
Zweifaktor-Authentifizierung	Wenn Sie mehr Sicherheit für die Benutzer bereitstellen möchten, die sich bei der Appliance anmelden, setzen Sie diese Option auf Aktiviert. Diese Funktion fügt einen zusätzlichen Schritt beim Anmeldevorgang hinzu. Sie vertraut auf die Google Authenticator-App, um Verifizierungscodes zu generieren. Die App generiert in regelmäßigen Abständen einen neuen sechsstelligen Code. Wenn diese Option aktiviert ist, werden die Endbenutzer bei jeder Anmeldung aufgefordert, den aktuellen Verifizierungscode einzugeben. Wenn Sie diese Funktion aktivieren, stellen Sie sicher, dass die Uhr des KACE SMA-Servers und diejenige des Geräts, auf dem Google Authenticator ausgeführt wird, korrekt sind. Der Google Authenticator verlässt sich auf die aktuelle Zeit, um das Token zu erstellen. Wenn die Zeit auf dem Server nicht mit der auf den Geräten synchronisiert ist, auf denen Google Authenticator ausgeführt wird, kann die Validierung von Tokens fehlschlagen, was zur Sperrung von Konten führen kann.

Klicken Sie auf Weiter, wenn Sie fertig sind.

7. Befolgen Sie auf der Seite Dateifreigabe aktivieren die Bildschirmanweisungen, um diesen Schritt abzuschließen.

8. Geben Sie auf der Seite Domäneneinstellungen die Zeitzone, den Hostnamen und den Domänennamen Ihrer Appliance ein.

   Auf dieser Seite können Sie auch benutzerdefinierte DNS-Einstellungen vornehmen. Bei einer standardmäßigen Installation werden durch Azure bereitgestellte DNS-Server verwendet.

   Wenn Sie eine VPN-Verbindung von Standort zu Standort konfigurieren, können Sie auch die IP-Adresse Ihres DNS-Servers verwenden, um die Appliance je nach Ihrer DNS-Konfiguration sowohl für interne als auch für öffentliche Netzwerke (empfohlen) oder nur für das interne Netzwerk zugänglich zu machen. Wählen Sie dazu Benutzerdefinierte DNS-Konfiguration aktivieren aus und geben Sie im Feld Primärer DNS die IP-Adresse Ihres DNS-Servers ein. Weitere Informationen finden Sie in den Hilfeinhalten auf dieser Seite.

   Klicken Sie auf Weiter, wenn Sie fertig sind.

9. Überprüfen Sie auf der Seite Bestätigen Ihre Konfiguration.

   Wenn Sie Änderungen vornehmen müssen, kehren Sie mithilfe der Schaltfläche Zurück im Assistenten zum gewünschten Schritt zurück und aktualisieren Sie Ihre Konfiguration.

   Klicken Sie anschließend auf Fertig stellen.

   Sobald die Ersteinrichtung abgeschlossen ist, wird die Appliance neu gestartet und die Administratorkonsole-Anmeldeseite wird angezeigt.

10. Melden Sie sich bei der Administratorkonsole an und verwenden Sie dazu die Anmelde-ID admin und das Kennwort, das Sie bei der Ersteinrichtung festgelegt haben.

    Wenn die Zweifaktor-Authentifizierung auf der Seite Lizenzierungs- und Administratoreinstellungen im Assistenten für die Ersteinrichtung aktiviert wurde, wird die Seite Zweifaktor-Authentifizierung konfigurieren angezeigt.

11. Nur Zweifaktor-Authentifizierung. Befolgen Sie die Anweisungen auf der Seite Zweifaktor-Authentifizierung konfigurieren, um einen Google Authenticator-Verifizierungscode mit Ihrem Smartphone zu erstellen. Geben Sie in das Feld Verifizierungscode den Google Authenticator-Code ein und klicken Sie auf Konfiguration fertig stellen. Bei jeder nachfolgenden Anmeldung wird ein neuer Verifizierungscode benötigt.

    Um diesen Schritt zu überspringen, klicken Sie auf Weiter. Sie können diesen Schritt nur innerhalb eines zuvor konfigurierten Übergangszeitfensters überspringen. Weitere Informationen finden Sie im Administratorhandbuch:

12. Geben Sie in den Netzwerkeinstellungen den vollständig qualifizierten DNS-Namen der Appliance an. Wenn Sie die Appliance in Azure neu starten, ändert sich ihre IP-Adresse. Geräte stellen über diesen Namen eine Verbindung mit der Appliance her.
    a. Melden Sie sich bei KACE SMA Administratorkonsole an und klicken Sie auf Einstellungen.
    b. Klicken Sie in der angezeigten Systemsteuerung des Geräts auf Netzwerkeinstellungen.
    c. Geben Sie auf der Seite Netzwerkeinstellungen im Abschnitt Appliance-Netzwerkkonfiguration im Feld Name des Webservers den vollständig qualifizierten DNS-Namen der Appliance ein, den Sie in Schritt 3 aufgezeichnet haben.

d. Klicken Sie auf Speichern.

> Die Befehlszeilenkonsole ist eine Terminalfenster-Schnittstelle für die Appliance. Mit diesem Tool können Sie Netzwerkeinstellungen konfigurieren. Sie dürfen dieses Tool nicht verwenden, um die IP-Adresse für die in Azure ausgeführte Appliance zu ändern.

Die Administratorkonsole wird angezeigt und die Appliance kann verwendet werden.

Aktivieren von SSL

Sie müssen die sichere Kommunikation zwischen der Appliance und verwalteten Geräten aktivieren. Mit der Administratorkonsole der Appliance können Sie ein SSL-Zertifikat generieren.

Beschaffen Sie sich einen eingetragenen Domainnamen, der für die Appliance verwendet werden soll. Dies ist erforderlich, um eine Signieranforderung für das SSL-Zertifikat mit der Administratorkonsole der Appliance generieren zu können.

1. Klicken Sie in der Administratorkonsole auf Einstellungen, um zur Systemsteuerung der Appliance zu navigieren.
2. Klicken Sie auf Sicherheitseinstellungen.

   Die Seite Sicherheitseinstellungen wird angezeigt.
3. Deaktivieren Sie im Abschnitt SSL unten auf der Seite den Zugriff auf den HTTP-Port 80 und leiten Sie den gesamten Port 80-Datenverkehr an den HTTPS-Port 443 weiter.

   > Wenn Port 80 nicht deaktiviert wird, können vertrauliche Informationen, wie z. B. Kennwörter, im Nur-Text-Format über das Internet übertragen werden.

   - Heben Sie die Auswahl von Zugriff auf Port 80 aktivieren auf.
   - Wählen Sie SSL aktivieren und Weiterleitung von Port 80 an Port 443 aktivieren aus.
4. Klicken Sie auf SSL-Zertifikatformular, um die Seite SSL-Zertifikatformular anzuzeigen.
5. Geben Sie im Bereich Konfigurieren die folgenden Informationen ein:

Option	Beschreibung
Name der Firma	Der Name Ihres Unternehmens
Name der Organisation	Der Name Ihrer Organisationseinheit oder Unternehmensgruppe
Allgemeiner Name	Der allgemeine Name der Appliance, für die Sie das SSL-Zertifikat erstellen
E-Mail	Ihre E-Mail-Adresse.
Name der Stadt	Der Name Ihres Ortes
Name für Bundesland/Kanton	Der Name Ihres Bundeslands oder Kantons

Option	Beschreibung
Ländername	Der Name Ihres Landes

6. Klicken Sie auf Speichern.
7. Generieren Sie ein selbstsigniertes Zertifikat.
   a. Klicken Sie zum Generieren auf Selbstsigniertes Zertifikat erstellen. Das Zertifikat können Sie sich im Abschnitt Zertifikat-Signierungsanfrage ansehen.
   b. Klicken Sie auf Selbstsigniertes Zertifikat bereitstellen und dann auf Ja.
   c. Klicken Sie auf der Seite Sicherheitseinstellungen auf Dienste speichern und neu starten.

   Das SSL-Zertifikat wird erzeugt. Selbstsignierte Zertifikate werden zu PEM-Dateien konvertiert, als kbox.pem benannt und im Datenordner des KACE SMA Agenten gespeichert. Weitere Informationen zu den Sicherheitseinstellungen finden Sie im Administratorhandbuch.

   Wenn Sie ein selbstsigniertes Zertifikat erstellen, müssen Sie es auf allen vom Agenten verwalteten Geräten bereitstellen.
8. Starten Sie die Appliance neu.

Best Practices

Befolgen Sie die Richtlinien und Empfehlungen in diesem Abschnitt bei der Verwendung der Appliance.

Verwenden von VPN-Verbindungen und Netzwerkressourcen

Wenn Sie eine herkömmliche Agenten-Server-Kommunikation zwischen der Appliance und Ihren verwalteten Geräten verwenden, ist für die Kommunikation lediglich die Installation des Agenten auf den verwalteten Geräten erforderlich. Wenn Sie jedoch eine VPN-Verbindung verwenden, unterliegt es Ihrer Verantwortung, den Netzwerk-Handshake zwischen Ihrer Umgebung und der Appliance zu konfigurieren. Beim Appliance-Team erhalten Sie Empfehlungen, z. B. zu den zuzulassenden IP-Adressen und Ports. Das Mitwirken des Netzwerkadministrators beim Setup-Vorgang ist hierbei unverzichtbar. Die entsprechenden Cloud-Verbindungen werden konfiguriert und Sie müssen sicherstellen, dass die Verbindung auf Ihrer Seite aufgebaut werden kann, um die Einrichtung erfolgreich abzuschließen.

Darüber hinaus erfordern einige Appliance-Funktionen die Verwendung einer VPN-Verbindung in der Cloud. Hierbei reicht für gewöhnlich eine VPN-Verbindung für ein einzelnes Unternehmen. Sie können beispielsweise eine einzige VPN-Verbindung verwenden, selbst wenn Sie über Remote-Standorte verfügen – vorausgesetzt, dass diese Standorte Datenverkehr über den Hauptunternehmensstandort umleiten können, an dem die VPN-Verbindung vorhanden ist. Sämtlicher KACE SMA Agentenverkehr wird über das VPN und daraufhin über die VPN-Verbindung an die Appliance geleitet. Wenn die Remote-Standorte den Hauptunternehmensstandort nicht erkennen können oder wenn Sie es bevorzugen, dass jeder Standort über eine direkte VPN-Verbindung zur Appliance verfügt, müssen Sie für jeden Standort

eine VPN-Verbindung erwerben. Informationen zu den Funktionen, die eine VPN-Verbindung erfordern, finden Sie unter Funktionsausnahmen.

Die Produktpreise basieren auf der gemeinsam genutzten Netzwerkbandbreite. Um weitere Netzwerkressourcen oder VPN-Verbindungen zu erwerben, wenden Sie sich unter https://www.quest.com/company/contact-us.aspx an Quest Sales.

Verwenden von VPN-Verbindungen mit mehreren Domains

Die Appliance wurde für die Verwendung mit einer einzelnen Domain und einer einzelnen VPN-Verbindung entwickelt. Wenn Sie über mehrere Domains verfügen, können Sie Geräte (Inventar) in anderen Domains zwar mithilfe der Appliance verwalten, jedoch sind Funktionen, die einen VPN-Zugriff erfordern, nur für eine einzige Domain verfügbar. Sie können sich beispielsweise für die Identitätszugriffsverwaltung bei einer Active Directory-Umgebung authentifizieren, jedoch nicht bei mehr als einer Domain. Der Agentenverkehr von der Domain mit der VPN-Verbindung wird über die VPN-Verbindung geleitet, während der Agentenverkehr für andere Domains über den standardmäßigen Internetzugriff eine Verbindung mit der Appliance herstellt. Informationen zu den Funktionen, die eine VPN-Verbindung erfordern, finden Sie unter Funktionsausnahmen.

Informationen zur IP-Adresse der Appliance

Die Appliance ist für eine einzelne IP-Adresse konfiguriert. Die IP-Adresse wird von Quest zugewiesen und kann nicht geändert werden. Sie müssen einen Host-Datensatz (A) in Ihrem internen DNS (Domain Name System) für die statische IP-Adresse der Appliance erstellen und können dann verschiedene A-Datensätze (für Hosts) über mehrere Netzwerke und Domains hinweg erstellen, um Ihre Appliance zuzuweisen. Wenn Sie mehr als eine öffentliche IP-Adresse für Ihr Netzwerk benötigen, müssen Sie eine separate Instanz der Appliance erwerben. Mehrere Appliance-Instanzen können keine Daten oder Datenbankinformationen gemeinsam nutzen. Wenden Sie sich für weitere Informationen unter https://www.quest.com/company/contact-us.aspx an Quest Sales.

Informationen zu Netzwerkeinstellungen

Standardmäßig sind alle Netzwerkprotokolle und die jeweils zugehörigen Dienste außer HTTPS und HTTP deaktiviert. Diese Protokolle werden für die Benutzeroberflächen der Appliance und die KACE SMA Agentenkommunikationen verwendet. Wenn die KACE SMA Agenten-Software auf einem Gerät bereitgestellt wird und SSL aktiviert ist, versucht der Agent immer, für eine verschlüsselte Kommunikation eine Verbindung per HTTPS über Port 443 mit dem Gerät herzustellen. Andernfalls verwendet der Agent HTTP über Port 80.

Provisionierung des KACE SMA Agenten auf verwalteten Geräten

Der KACE SMA Agent ist eine Anwendung, die auf Geräten installiert werden kann, um die Geräteverwaltung und Inventarberichte über die Appliance zu ermöglichen. Um die Agenten-Software direkt von der Appliance auf Geräten bereitzustellen, müssen Sie über eine VPN-Verbindung verfügen. Es gibt jedoch alternative Methoden zur Bereitstellung der Agenten-Software ohne VPN-Verbindung:

- Manuelles Herunterladen und Installieren des Agenten auf Geräten. Anweisungen hierzu finden Sie im Administratorhandbuch.
- Installieren des Agenten mithilfe einer Windows Gruppenrichtlinie (GPO) Weitere Informationen hierzu finden Sie unter https://support.quest.com/kb/133776.
- Installieren des Agenten mithilfe eines anderen Verwaltungssystems: Wenn die Quest Lösung eine andere Systemverwaltungslösung ersetzen soll, können Sie den Agenten mithilfe der Verteilungsmethoden des zu ersetzenden Systems bereitstellen, bevor Sie dieses entfernen und das System bereinigen.

Konfigurieren der Kommunikationseinstellungen für den KACE SMA Agenten

Agenten, die auf verwalteten Geräten installiert sind, kommunizieren regelmäßig mit der Appliance, um Inventarinformationen zu melden, Skripte zu aktualisieren und andere Aufgaben auszuführen. Sie können die Agenteneinstellungen einschließlich des Anmeldeintervalls der Agenten, der Meldungen für Benutzer sowie der Dauer der Aufbewahrung des Protokolls konfigurieren. Wenn Sie mehrere Organisationen haben, können Sie die Agenten-Einstellungen für jede Organisation individuell anpassen. Weitere Informationen hierzu finden Sie im Administratorhandbuch der KACE SMA. Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Informationen zur Serverüberwachung

Die Appliance unterstützt die Serverüberwachung, wodurch eine grundlegende Leistungs- und Anwendungsüberwachung für Server im Inventar ermöglicht wird. Sie können die Überwachung für Server, die den KACE SMA Agenten verwenden, sowie für Server mit Verwaltung ohne Agenten-Software aktivieren. Die Einrichtung hängt von den Richtlinien Ihrer IT-Abteilung ab. Die Serverüberwachung ist unter Verwendung einer standardmäßigen Appliancelizenz für bis zu fünf Server verfügbar. Sie können eine zusätzliche Lizenz erwerben, um diese Anzahl zu erhöhen.

Wenn Sie die Überwachung für mithilfe von Agenten verwaltete Server aktivieren, werden Warnungsinformationen zusätzlich zum vorhandenen Agentenkommunikationsprotokoll über Port 443 übertragen. Wenn Sie die Überwachung für Server mit Verwaltung ohne Agenten-Software aktivieren, verwendet das Gerät SSH oder Telnet, um eine Verbindung zum Server herzustellen, die Protokolle zu lesen, nach Warnungen zu suchen und die Warnungen in der KACE SMA Administratorkonsole anzuzeigen. Da für die Verwendung von SSH und Telnet ein VPN-Zugang erforderlich ist, wird für die Serverüberwachung ohne Agenten-Software eine VPN-Verbindung benötigt.

Informationen zur Dateiverteilung (Pakete) und zu Replikationsfreigaben

Mit der Appliance ist jeder Standort ein Remote-Standort. Quest empfiehlt dringend, die Replikationsfreigaben für jeden Standort zu konfigurieren, um die Bandbreitennutzung der Internetverbindungen des Remote-Standorts zu optimieren. Replikationsfreigaben sind Geräte, die Kopien von Dateien für die Verteilung aufbewahren, wie z. B. verwaltete Installationen, Patches, Skripte und Dell Aktualisierungen.

Wenn die Samba Dateifreigabe deaktiviert ist, wird die Größe von Uploads zur Appliance auf 2 GB beschränkt. Verwenden Sie für Dateien von mehr als 2 GB eine alternative Download-Quelle, um die Dateien innerhalb des Unternehmensnetzwerks bereitzustellen.

Eine alternative Download-Quelle kann jeder beliebige Netzwerkspeicherort sein, an dem sich alle erforderlichen Dateien zur Installation einer bestimmten Anwendung befinden. Sie können Pakete von alternativen Download-Quellen bereitstellen, beispielsweise von einer UNC-Adresse oder einer DFS-Quelle. Die CIFS- und SMB-Protokolle, Samba-Server und Dateiserver-Appliances werden unterstützt. Sie müssen den Speicherort angeben, wenn Sie eine verwaltete Installation erstellen. Weitere Informationen finden Sie im KACE SMA Administratorhandbuch im Abschnitt zur Verteilung: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Informationen zur Bandbreitennutzung und dedizierten Netzwerkbandbreite

Die Appliance verwendet ein gemeinsam genutztes Cloud-Netzwerk. Um die Bandbreitenanforderungen des gemeinsamen Netzwerks zu reduzieren, empfiehlt Quest dringend die Verwendung von Replikationsfreigaben. Wenn Ihre Appliance Bandbreitenprobleme im gemeinsamen Netzwerk verursacht, müssen Sie möglicherweise Replikationsfreigaben einrichten oder dedizierte Netzwerkbandbreite erwerben. Wenden Sie sich für weitere Informationen unter https://quest.com/company/contact-us.aspx an Quest Sales.

Informationen zur Datensicherheit

Die Cloud-Rechenzentren und Quest Appliances zeichnen sich durch eine hoch verfügbare Infrastruktur aus und bieten den erforderlichen Schutz und die nötige Sicherheit für Ihre Appliance. Weitere Informationen zu den Sicherheitseinstellungen der Appliance finden Sie im Konfigurationsabschnitt im KACE SMA Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Verwenden von Sicherungsdateien

Sicherungsdateien werden verwendet, um Ihre KACE als Service Appliance im Falle eines Datenverlusts wiederherzustellen oder um Einstellungen während Upgrades zu bewahren.

Quest erstellt zum Zwecke der Notfallwiederherstellung automatisch externe Kopien der letzten Sicherungsdatei.

Sie können über die Administratorkonsole auf Sicherungsdateien zugreifen. Werden die Dateien zu groß für einen HTTP-Download, können Sie über FTP darauf zugreifen. Siehe Sichern der Appliance und Aktivieren des FTP-Zugriffs. Wenn die Netzwerkbandbreite beschränkt ist, sollten Sie in Betracht ziehen, größere Sicherungsdateien mithilfe der Dateiverteilung herunterzuladen. Siehe Informationen zur Dateiverteilung (Pakete) und zu Replikationsfreigaben.

Durch das Wiederherstellen jeglicher Sicherungsdateien werden die aktuell auf dem Appliance-Server gespeicherten Daten gelöscht. Quest empfiehlt, zunächst eine externe Sicherung aller Sicherungsdateien oder Daten durchzuführen, die Sie aufbewahren möchten, bevor Sie die Einstellungen wiederherstellen.

Konfigurieren der Appliance im Internet

Wie bei jeder webserverbasierten Anwendung umfassen die bewährten Sicherheitsverfahren die Beschränkung des Zugriffs auf die KACE Systems Management Appliance (SMA) aus dem Internet. Zur Gewährleistung der Sicherheit ist eine sorgfältige Überprüfung der Umgebung erforderlich. Es wird dringend empfohlen, Firewalls, Verschlüsselung, Portzugriff, Rollen, Virenschutz, SSL, die Zugriffssteuerungsliste sowie die Notfallwiederherstellung zu berücksichtigen und vor der Konfiguration der SMA im Internet das folgende Thema zu lesen: https://support.quest.com/kb/267753/best-practices-for-securing-your-sma. Wenn die KACE SMA als Internet-/öffentliche Schnittstelle konfiguriert ist, sollte zumindest nur zur KACE SMA eingehender Port 443-Datenverkehr (HTTPS) über eine Firewall für UI-Zugriff und Agenten-Kommunikationsverkehr zugelassen werden.

Weitere Informationen finden Sie unter https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-.

Sichern der Appliance und Aktivieren des FTP-Zugriffs

Sie können einstellen, dass Quest tägliche und monatliche Sicherungsdateien in einen lokalen High-Speed-Speicherbereich kopiert, indem Sie den FTP-Zugriff aktivieren und das FTP-Kennwort wie in diesem Abschnitt beschrieben auf sepgetbxf festlegen. Der FTP-Zugriff erfordert eine VPN-Verbindung.

1. Klicken Sie in der Administratorkonsole auf Einstellungen, um zur Systemsteuerung der Appliance zu navigieren.
2. Klicken Sie auf Sicherheitseinstellungen.

   Die Seite Sicherheitseinstellungen wird angezeigt.
3. Geben Sie im oberen Abschnitt folgende Einstellungen an:

Option	Beschreibung
Sicherung über FTP aktivieren	Aktivieren Sie dieses Kontrollkästchen, um den FTP-Zugriff auf Sicherungsdateien zu aktivieren.
Schreibschutz für FTP aufheben	Aktivieren Sie dieses Kontrollkästchen, um FTP für das Hochladen von Sicherungsdateien zu verwenden.
Neues FTP-Benutzerkennwort	Geben Sie folgendes Kennwort ein: sepgetbxf.

Wenn das FTP-Benutzerkennwort festgelegt wurde, kopiert der Sicherungsserver automatisch tägliche und monatliche Sicherungsdateien in einen lokalen High-Speed-Speicherbereich. Weitere Informationen zur Verwaltung von Sicherheitskopien finden Sie im Serviceabschnitt im KACE SMA Administratorhandbuch: Zugriff auf das Administratorhandbuch und die Onlinehilfe.

Zugriff auf das Administratorhandbuch und die Onlinehilfe

Um Hilfe zur Verwendung der Administratorkonsole zu erhalten, klicken Sie auf den Hilfelink in der oberen rechten Ecke der Oberfläche, um die kontextbezogene Hilfe aufzurufen. Klicken Sie auf die Links in den Themen der kontextbezogenen Hilfe, um auf das Haupthilfesystem zuzugreifen.

Zeitplanung für Schulungen

Um Sie bei der Verwendung der Appliance zu unterstützen, bietet Quest ein Schulungsprogramm mit dem Titel "QuickStart" an. Dieses Programm bietet Remote-Unterstützung, sodass Ihre Lösung schnell einsatzbereit gemacht werden kann, um die Bereitstellung, Verwaltung, Sicherung und Wartung Ihrer mit dem Netzwerk verbundenen Geräte zu beschleunigen.

Knowledge Base-Artikel

Weitere Informationen finden Sie auf der Knowledge Base-Seite des Quest Softwaresupports unter https://support.quest.com/systems-management-appliance/kb .

- Von der Appliance benötigte Netzwerkports: https://support.quest.com/kb/111775
- Für Patching erforderliches Whitelisting: https://support.quest.com/kb/111785

- Installieren des KACE SMA Agenten mithilfe einer Windows Gruppenrichtlinie: https://support.quest.com/kb/133776
- Arbeiten mit Sicherungsdateien: https://support.quest.com/kb/111736

Über uns

Quest bietet Softwarelösungen für die sich schnell verändernde Welt der Unternehmens-IT. Wir unterstützen Sie dabei, die Herausforderungen zu vereinfachen, die durch Datenexplosion, Cloud-Erweiterung, hybride Rechenzentren, Sicherheitsbedrohungen und behördliche Auflagen entstehen. Wir sind ein globaler Anbieter für 130.000 Unternehmen in 100 Ländern, darunter 95 % der Fortune 500 und 90 % der Global 1000. Seit 1987 haben wir ein Lösungsportfolio aufgebaut, das nun Datenbankmanagement, Datenschutz, Identitäts- und Zugriffsmanagement, Microsoft-Plattformmanagement und einheitliches Endpoint-Management umfasst. Mit Quest verbringen Unternehmen weniger Zeit mit der IT-Administration und mehr Zeit mit geschäftlichen Innovationen. 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

アプライアンスのセットアップ

はじめに

アプライアンスを設定する前に、いくつかの作業を行っていただく必要があります。

1. Microsoft Azure へのサブスクリプションを持っていることを確認します。仮想 KACE SMA をインストールすると、アプライアンスは Azure クラウドで仮想マシンとして実行されます。Azure クラウドプラットフォームの詳細、またはサインアップの詳細については、http://azure.microsoft.com/en-us/ を参照してください。
2. Microsoft Azure 仮想 KACE SMA のライセンスを Quest の営業担当から購入します (https://www.quest.com/company/contact-us.aspx) 。
3. 使用するネットワークおよびファイアウォールの設定で、KACE SMA へのアウトバウンドアクセスがポート 443 で許可されることを確認します。このポートはアプライアンスのウェブベースのコンソールおよび HTTPS によるエージェント通信に使用されます。このポートは、デスクトップとサーバを含めた、KACE SMA エージェントソフトウェアがインストールされるデバイスでも開かれている必要があります。

機能の例外

KACE SMA 管理者コンソールのすべての機能は Cloud 内で使用するために設定できます。ただし、一部の機能はネットワークへの直接アクセスを必要とし、その確立にはサイト間の VPN 接続を使用します。VPN 接続は共有ネットワークを利用します。通常は、企業 1 社の機能を有効にするには 1 つの VPN 接続で十分です。ただし、場合によっては、追加の VPN 接続が必要になり、専用ネットワーク帯域幅が要求されることがあります。詳細については、「VPN 接続およびネットワークリソースの使用」を参照してください。

VPN 接続を必要とする管理者コンソール機能

次に挙げる管理者コンソール機能には、VPN 接続が必要です。

- エージェント不要デバイス管理を使用するサーバ監視
- Wake on LAN、ネットワーク検出 (IP スキャン、Active Directory® スキャン、NMAP スキャンを含む) 、アプライアンスからの KACE SMA エージェントのプロビジョニング (「管理対象デバイスへのKACE SMAエージェントのプロビジョニング」を参照) 。

  エージェントリレーを使用する場合、これらの機能に VPN は必要ありません。

- リソースのインポートおよびエクスポート (ファイル共有は Cloud ファイアウォールによってブロックされます)
- バックアップファイルへの FTP アクセス (FTP アクセスは Cloud ファイアウォールによってブロックされます)

- アプリケーションパッケージおよびスクリプトの依存関係は、HTTP を使用してアップロードする必要があります。より速度の遅いネットワーク接続では、サイズの大きいパッケージのアップロードがタイムアウトする可能性があります。2 GB を超えるパッケージは、代替のダウンロード場所を使用して、内部ファイルサーバーから配布する必要があります。
- LDAP ユーザーラベルおよびデバイスラベル
- LDAP ユーザー認証
- LDAP ユーザーのインポート
- 管理者コンソールおよびユーザーコンソールに対する Active Directory シングルサインオン

ユーザーコンソール機能の例外

ユーザーコンソールは、エンドユーザーがソフトウェアライブラリとサービスデスクの機能を利用できるようにするためのインタフェースです。次に示すユーザーコンソール機能は、クラウドではサポートされていません。

- ユーザーコンソールからのソフトウェアの自動インストール (ダウンロードはサポートされます)

Azure での KACE SMA 仮想マシンの作成

このトピックでは、Azure Marketplace から入手可能な VM テンプレートを使用して KACE システム管理アプライアンス (SMA) として機能する仮想マシン (VM) を Microsoft Azure で作成するプロセスについて説明します。

Azure サブスクリプションが有効であることを確認します。仮想 KACE SMA をインストールすると、アプライアンスは Azure クラウドで仮想マシンとして実行されます。Azure クラウドプラットフォームの詳細、またはサインアップの詳細については、http://azure.microsoft.com/en-us/ を参照してください。

1. Azure サブスクリプション資格情報を使用して https://azuremarketplace.microsoft.com/ に口グインします。
2. 検索フィールドに「KACE Systems Management Appliance」と入力します。
3. KACE システム管理アプライアンスアプリケーションを開きます。
4. プランと価格セクションの情報を確認して、推奨される仮想マシンリソースの要件を確認してください。
5. 今すぐ取得をクリックします。
6. Create をクリックします。

   仮想マシンの作成 ページが表示されます。このページには複数のタブがあります。これらのタブの一部には、KACE SMA VM の設定に必要なオプションが含まれています。

   Azure インターフェイスは頻繁に変更されます。一部のオプションが正確に一致しない場合があります。このページの最新情報については、https://docs.microsoft.com/en-us/azure/ を参照してください。

7. 仮想マシンの作成 ページの 基本 タブで、次の情報を入力します。

オプション	説明
サブスクリプション	Azure サブスクリプションの名前を指定します。
リソースグループ	この仮想マシンでリソースグループを作成するか既存のリソースグループを使用します。
仮想マシン名	作成しようとしている仮想マシンの名前を入力します。
イメージ	このオプションは、選択した KACE システム管理アプライアンスのイメージを表示します。
サイズ	a. サイズの変更 をクリックします。 b. 表示されたVM サイズの選択ページで、必要に応じて推奨される VM サイズから設定を選択します。
認証タイプ	仮想マシンの管理者アカウントの認証の詳細を入力します。 管理者アカウントの資格情報は、アプライアンスへのアクセスには使用されません。ただし、この情報は Azure で作成するすべての仮想マシンに必須であり、指定する必要があります。 a. パスワード を選択します。 b. ユーザー名 フィールドに、仮想マシン管理者のユーザー名を入力します。 c. パスワード フィールドに、管理者アカウントのパスワードを入力します。

8. 他のすべてのオプションはそのままにして、次へ をクリックします。
9. ディスクタブで、OS ディスクタイプをクリックし、プレミアム SSD を選択します。これは、アプライアンスに推奨される最小値です。
10. 他のすべてのオプションはそのままにして、次へ をクリックします。
11. ネットワークタブで、次のオプションを設定します。

オプション	説明
仮想ネットワーク	既存の仮想ネットワークを選択するか、新しい仮想ネットワークを作成します。
サブネット	既存のサブネットを選択するか、新しいサブネットを定義します。

オプション	説明
IP	仮想ネットワークの外部から KACE SMA と通信する場合は、パブリック IP アドレスを使用します。

アプライアンスをアップグレードする場合、ブラウザでアップグレードステータスを追跡するには、ポート 52231 を開く必要があります。アップグレードが正常に適用されたら、このポートを閉じます。

12. このタブと残りのタブで、他のすべてのオプションをそのままにしてをクリックし、確認 タブに到達するまで 次へ をクリックします。
13. 確認 タブで、作成 をクリックします。

    VM の展開中は、ブラウザに進捗バーが表示されます。完了すると、通知が短時間表示され、VM の概要と詳細が Azure に表示されます。

アプライアンスの設定

初期セットアップ ウィザードを使用して、アプライアンスを設定し、管理者コンソール にログインします。

使用しているブラウザの設定に基づいて、初回ログイン時に管理者コンソールに表示される言語が決定されます。言語設定の変更の詳細については、アプライアンスの『Administrator Guide』（管理者ガイド）を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス

1. Azure でアプライアンスソフトウェアを実行している仮想マシンの完全修飾 DNS 名を取得します。
   a. Azure で仮想マシンを選択して、概要設定に移動します。
   b. 概要ページで設定をクリックして、KACE SMA の DNS 名を設定します。たとえば、my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com のように入力します。

   これらの設定の詳細については、https://docs.microsoft.com/en-us/azure/を参照してください。
2. Web ブラウザを開き、次の構文を使用して管理者コンソール URL を入力します。

   http://<unique_KACE_SMA_appliance_name>/admin

   <unique_KACE_SMA_appliance_name>は、手順 1 で設定した完全修飾仮想マシンの DNS 名です。

   例：http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

   ソフトウェア取引契約書 ページが表示されます。
3. 契約書に同意します。

   初期セットアップ ウィザードが表示されます。

4. 初期セットアップウィザードの ようこそ ページで、アプライアンスの設定に必要な情報がすべてそろっていることを確認したら、次へ をクリックします。
5. 診断コンソールの 2 要素認証 ページで、秘密キーとオフライントークンを確認して記録し、次へ をクリックします。
6. ライセンスと管理者の設定 ページで、以下の情報を入力します。

オプション	説明
ライセンスキー	Questからの案内のEメールに記載されているライセンスキーです。ライセンスキーがない場合は、Quest Software サポート（https://support.quest.com/contact-support）にお問い合わせください。
会社名	会社またはグループの名前です。
管理者Eメール	Questからの連絡の宛先となるEメールアドレスです。
パスワード	デフォルトの admin アカウントのパスワードです。このアカウントは、アプライアンスの管理者コンソールにログインするために使用します。この時点でデフォルトの admin アカウントがアプライアンス上で唯一のアカウントになります。このアカウントのパスワードを忘れると、システムを出荷時のデフォルト状態にリセットすることが必要になる場合があり、データロスが発生します。 **i** 複数のKACE SMAまたはKACE SDA（システム導入）アプライアンスを使用する場合、Questでは、すべてのアプライアンスのadminアカウントに同じパスワードを使用することをお勧めします。これにより、後でアプライアンス同士をリンクすることが可能になります。詳細については、アプライアンスの『Administrator Guide』（管理者ガイド）を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス
2 要素認証	アプライアンスにログインしているユーザーのセキュリティをより強力にするには、この設定を 有効 にします。この機能では、ログインプロセスにステップが 1 つ追加されます。これは、Google Authenticator アプリケーションに依存して検証コードを生成します。このアプリは、定期的に新しい 6 桁のコードを生成しま

オプション	説明
	す。有効にすると、エンドユーザーはログインするたびに現在の検証コードを要求されます。 この機能を有効にする場合は、KACE SMA サーバのクロック、および Google Authenticator を実行しているデバイスが正確であることを確認してください。Google Authenticator は、現在の時刻に依存してトークンを作成します。サーバのクロックが Google Authenticator を実行しているデバイスのクロックと同期されていない場合、トークンの検証が失敗し、アカウントのロックアウトが発生する可能性があります。

終了したら、次へ をクリックします。

7. ファイル共有を有効にする ページで、画面の指示に従って、この手順を完了します。
8. ドメイン設定 ページで、タイムゾーン、ホスト名、およびアプライアンスのドメイン名を指定します。

   このページでは、カスタム DNS 設定を有効にすることもできます。デフォルトのインストールでは、Azure 提供の DNS サーバを使用します。

   サイト間 VPN を設定する場合は、DNS の設定に応じて、DNS IP を使用して、内部ネットワークとパブリックネットワークの両方にアクセスできるようにする（推奨）ことも、内部ネットワークのみを使用することもできます。そのためには、カスタム DNS を有効にする を選択し、プライマリ DNS フィールドに DNS IP アドレスを入力します。詳細については、このページのヘルプの内容を確認してください。

   終了したら、次へ をクリックします。

9. 確認 ページで、設定を確認します。

   変更が必要な場合は、ウィザードの 戻る ボタンを使用して適切なステップに移動し、設定を更新します。

   終了したら、完了 をクリックします。

   初期セットアップが完了すると、アプライアンスが再起動し、管理者コンソールのログインページが表示されます。

10. ログイン ID「admin」と、初期セットアップ中に選択したパスワードを使用して、管理者コンソールにログインします。

    初期セットアップウィザードの ライセンスと管理者の設定 ページで 2 要素認証が有効になっている場合は、2 要素認証の設定 ページが表示されます。

11. 2 要素認証のみ。2 要素認証の設定 ページの指示に従い、スマートフォンを使用して Google Authenticator の検証コードを生成します。検証コード フィールドに、Google

Authenticator のコードを入力し、設定を完了 をクリックします。その後はログインのたびに新しい検証コードが要求されます。

この手順をスキップするには、設定をスキップ をクリックします。このステップは、設定されている移行ウィンドウでのみバイパスできます。詳細については、『管理者ガイド』を参照してください。

12. ネットワーク設定 で完全修飾アプライアンスの DNS 名を指定します。Azure でアプライアンスを再起動すると、その IP アドレスが変更されます。デバイスは、この名前を使用してアプライアンスに接続します。
    a. KACE SMA 管理者コンソール にログインし、設定 をクリックします。
    b. 表示されるアプライアンスの コントロールパネル で、ネットワーク設定 をクリックします。
    c. ネットワーク設定ページのアプライアンスのネットワーク設定セクションにある Web サーバ名フィールドに、手順 3 で記録した完全修飾アプライアンスの DNS 名を入力します。
    d. 保存 をクリックします。

    > アプライアンスへのターミナルウィンドウのインターフェイスはコマンドラインコンソールです。このツールを使用すると、ネットワーク設定を構成できます。このツールを使用して、Azure で実行されているアプライアンスの IP アドレスを変更することはできません。

管理者コンソールが表示され、アプライアンスが使用可能になります。

SSLを有効にする

アプライアンスと管理対象デバイスとの間でセキュアな通信を有効にする必要があります。アプライアンスの管理者コンソールを使用して SSL 証明書を生成できます。

アプライアンスに使用する登録済みのドメイン名を取得します。これは、アプライアンスの管理者コンソールを使用して SSL 証明書署名要求を生成するために必要です。

1. 管理者コンソールで、設定 をクリックして、アプライアンスの コントロールパネル に移動します。
2. セキュリティ設定 をクリックします。

   セキュリティ設定 ページが表示されます。
3. ページの下部にある SSL セクションで、HTTP ポート 80 へのアクセスを無効にし、すべてのポート 80 トラフィックを HTTPS ポート 443 に転送します。

   > ポート 80 を無効にしないと、パスワードなどの機密情報をインターネット経由でプレーンテキストで伝送できます。

   - ポート 80 接続を有効にするをクリアします。
   - SSL を有効にするとポート 80 からポート 443 への転送を有効にするを選択します。
4. SSL証明書フォーム をクリックして、SSL証明書フォーム ページを表示します。
5. 設定 セクションで、次の情報を入力します。

オプション	説明
会社名	会社の名前。
組織名	組織のユニットまたはビジネスグループの名前。
共通名	SSL証明書を作成するアプライアンスの共通名。
Eメール	Eメールアドレス。
市区町村名	地域の名前。
都道府県名	都道府県の名前。
国名	国の名前。

6. 保存 をクリックします。
7. 自己署名証明書を生成するには、次の手順を実行します。
   a. 自己署名証明書の作成 をクリックして、証明書を生成し、Certificate Signing Request (証明書署名要求) セクションの下に表示します。
   b. 自己署名証明書の作成 をクリックし、はい をクリックします。
   c. セキュリティ設定 ページで、保存してサービスを再起動 をクリックします。

   SSL証明書が生成されます。自己署名証明書はkbox.pemという名前のPEMファイルに変換され、KACE SMAエージェントのデータフォルダに配置されます。セキュリティ設定についての詳細は、『管理者ガイド』を参照してください。

   自己署名証明書を作成した場合は、エージェントが管理するすべてのデバイスにその証明書を展開する必要があります。
8. アプライアンスを再起動します。

ベストプラクティス

アプライアンスを使用するときは、本項のガイドラインと推奨事項に従ってください。

VPN 接続およびネットワークリソースの使用

アプライアンスと管理対象デバイスとの間で従来のエージェントサーバ通信を使用する場合、エージェントを管理対象デバイスにインストールするのみで通信できます。ただし、VPN 接続を使用する場合は、使用する環境からアプライアンスまでのネットワークハンドシェイクはユーザーが完了させる必要があります。アプライアンスチームでは、許可することが適切な IP アドレスとポートなどの推奨事項を提供することができますが、セットアッププロセスにユーザー側のネットワーク管理者が関与することが不可欠です。適切な Cloud 接続は設定されますので、ユーザー側から接続を確認して、セットアップを正常に完了していただく必要があります。

さらに、アプライアンスの一部の機能では、クラウドで VPN 接続を使用する必要があります。通常、1 企業に 1 つの VPN 接続で十分です。例えば、リモートサイトが複数あっても、それらのサイトが、VPN 接続が存在する会社のメインサイトを経由してトラフィックをルーティングできる場合は、1 つの VPN 接続を使用できます。KACE SMAエージェントのすべてのトラフィックがVPN経由でルーティングされ、その後、VPN接続経由でアプライアンスにルーティングされます。リモートサイトで会社のメインサイトを参照できない場合、または各サイトからアプライアンスに直接の VPN リンクを設定する必要がある場合は、サイトごとに VPN 接続を購入する必要があります。VPN 接続を必要とする機能の詳細については、「機能の例外」を参照してください。

製品価格は、共有ネットワーク帯域幅に基づいて決定されます。追加のネットワークリソースのご購入、または VPN 接続のご購入については、Quest の営業担当 (https://www.quest.com/company/contact-us.aspx) にお問い合わせください。

複数ドメインでの VPN 接続の使用

アプライアンスは、単一ドメインおよび単一の VPN 接続で使用するように設計されています。ドメインが複数ある場合、アプライアンスを使用して他のドメイン上のデバイス (インベントリ) を管理することはできますが、VPN アクセスを必要とする機能は 1 つのドメインに対してのみ使用可能です。例えば、ID およびアクセス管理のために 1 つの Active Directory 環境に対して認証することはできますが、複数のドメインに対して認証することはできません。VPN 接続のあるドメインからのエージェントトラフィックは VPN 接続経由でルーティングされますが、その他のドメインのエージェントトラフィックは通常のインターネットアクセスを使用してアプライアンスに接続します。VPN 接続を必要とする機能の詳細については、「機能の例外」を参照してください。

アプライアンスの IP アドレスについて

アプライアンスは単一の IP アドレスに対して設定されます。この IP アドレスは Quest が割り当てるもので、変更することはできません。社内の DNS (ドメインネームシステム) サーバーに、アプライアンスの静的 IP アドレスのホスト (A) レコードを作成する必要があります。複数のネットワークまたはドメインにわたる複数の A (ホスト) レコードを作成して、アプライアンスを参照することができます。ネットワークに複数のパブリック IP アドレスを使用するには、アプライアンスの別個のインスタンスを購入する必要があります。複数のアプライアンスインスタンスでデータまたはデータベース情報を共有することはできません。詳細については、Quest の営業担当 (https://www.quest.com/company/contact-us.aspx) にお問い合わせください。

ネットワーク設定について

デフォルトでは、すべてのネットワークプロトコルとその関連サービスは HTTPS と HTTP を除き、無効になっています。これらのプロトコルは、アプライアンスのユーザーインタフェースと KACE SMAエージェントの通信に使用されます。KACE SMAエージェントソフトウェアがデバイスにプロビジョニングされているとき、SSL が有効になっている場合、エージェントは、暗号

化された通信に対しては常にポート 443 で HTTPS を使用してアプライアンスへの接続を試みます。それ以外の場合、エージェントはポート 80 で HTTP を使用します。

管理対象デバイスへのKACE SMAエージェントのプロビジョニング

KACE SMA エージェントは、デバイスにインストールすることで、アプライアンスを通じてデバイス管理とインベントリのレポートを可能にするアプリケーションです。エージェントのソフトウェアをデバイスに直接プロビジョニングするには、VPN 接続が必要です。ただし、VPN 接続なしでエージェントのソフトウェアを展開するための、次の代替方法があります。

- エージェントを手動でダウンロードしてデバイスにインストールする方法：詳細については、『管理者ガイド』を参照してください。
- Windows グループポリシー（GPO）を使用してエージェントをインストールする方法：詳細については、https://support.quest.com/kb/133776を参照してください。
- 他の管理システムを使用してエージェントをインストールする方法：他のシステムの管理ソリューションを Quest ソリューションで置き換える場合は、置き換えるシステムの使用を停止してクリーンアップする前に、そのシステムの配布方法を使用してエージェントを展開できます。

KACE SMAエージェントの通信設定

管理対象デバイスにインストールされたエージェントは、定期的にアプライアンスと通信して、インベントリのレポートやスクリプトの更新などのタスクを実行します。エージェントチェックインの間隔、ユーザーに表示されるメッセージ、ログの保持期間などのエージェント設定を定義できます。組織が複数ある場合は、それぞれの組織にエージェント設定を個別に定義できます。詳細については、KACE SMAの『Administrator Guide』（管理者ガイド）を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス

サーバ監視について

アプライアンスはサーバ監視をサポートします。これは、インベントリでサーバに対して基本的なパフォーマンスとアプリケーションの監視を行うものです。KACE SMAエージェントを使用するサーバの監視、およびエージェント不要管理を使用するサーバの監視を有効にすることができ、セットアップは現行のIT部門のポリシーによって異なります。サーバの監視は、アプライアンスの標準ライセンスを使用してサーバ 5 台まで可能です。ライセンスを取得することにより、この台数を増やすことができます。

エージェント管理対象サーバの監視を有効にすると、既存のエージェント通信プロトコルに加えて、警告情報がポート 443 で送信されます。エージェント不要管理を使用するサーバの監視を有効にすると、アプライアンスは SSH または Telnet を使用してサーバに接続し、ログを読み込み、警告がないか確認し、見つかった警告を KACE SMA 管理者コンソール に表示します。SSH

および telnet の使用には VPN アクセスが必要になるため、エージェント不要サーバの監視には VPN 接続が必要です。

ファイル配布（パッケージ）およびレプリケーション共有について

アプライアンスでは、すべてのサイトがリモートサイトになります。Quest では、各サイトにレプリケーション共有を設定して、リモートオフィスのインターネット接続における帯域幅使用率を最適化することを強くお勧めします。レプリケーション共有とは、管理対象インストール、パッチ、スクリプト、Dell アップデートなどの配布用にファイルのコピーを保持するデバイスです。

SAMBA のファイル共有がオフになっている場合、アプライアンスへのファイルのアップロードは 2 GB までに制限されます。2 GB を超えるファイルには、代替のダウンロード場所を使用して、会社のネットワーク内にファイルをステージングします。

代替のダウンロード場所には、特定のアプリケーションをインストールするために必要なすべてのファイルが格納されている任意のネットワーク上の場所を指定できます。UNCアドレスやDFSソースなどの代替のダウンロード場所からパッケージを配布できます。CIFSとSMBのプロトコル、SAMBAサーバー、およびファイルサーバーアプライアンスがサポートされています。代替のダウンロード場所は、管理対象インストールを作成する際に指定します。詳細については、KACE SMAの『Administrator Guide』（管理者ガイド）の配布の項を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス

帯域幅使用率と専用ネットワーク帯域幅について

アプライアンスは、共有クラウドネットワークを使用します。共有ネットワークの帯域幅要件を削減するために、レプリケーション共有を使用することを強くお勧めします。アプライアンスが原因で共有ネットワークに帯域幅の問題が発生した場合は、レプリケーション共有をセットアップするか、専用ネットワーク帯域幅を購入することが必要になることがあります。詳細については、Quest の営業担当（https://quest.com/company/contact-us.aspx）にお問い合わせください。

データの保護とセキュリティについて

Cloud データセンターおよび Quest アプライアンスでは、高可用性インフラストラクチャを備え、アプライアンスに必要なあらゆる保護とセキュリティを提供します。アプライアンスのセキュリティ設定の詳細については、KACE SMAの『Administrator Guide』（管理者ガイド）の設定の項を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス

バックアップファイルの使用

バックアップファイルは、データロスが発生した場合にサービスとしてのKACEアプライアンスを復元したり、アップグレード中に設定を保持したりするために使用します。Questでは、ディ

ザスタリカバリのために、最新の夜間バックアップファイルのオフボードコピーを自動的に作成します。

バックアップファイルには管理者コンソールを使用してアクセスできます。ファイルが大きすぎるため、HTTP を使用してダウンロードできなくなった場合は、FTP を使用してアクセスできます。詳細については、「アプライアンスのバックアップおよび FTP アクセスの有効化」を参照してください。ネットワーク帯域幅に制限がある場合は、サイズの大きなバックアップファイルのダウンロードにファイル配布を使用することを検討してください。詳細については、「ファイル配布（パッケージ）およびレプリケーション共有について」を参照してください。

復元にどのような種類のバックアップファイルを使用しても、アプライアンスサーバーで現在設定されているデータは破棄されます。Quest では、設定を復元する前に、残しておきたいあらゆるバックアップファイルまたはデータをオフロードすることをお勧めします。

インターネット上でのアプライアンスの設定

Web サーバーベースのアプリケーションと同様に、セキュリティのベストプラクティスには、インターネットからの KACE システム管理アプライアンス（SMA）へのアクセスを制限することが含まれます。セキュリティを確保するためには、環境を慎重に検討し、確認する必要があります。インターネット上で SMA を構成する前に、ファイアウォール、暗号化、ポートアクセス、役割、ウイルス対策、SSL、アクセス制御リスト、ディザスタリカバリを検討し、次のトピックを確認することを強くお勧めします：https://support.quest.com/kb/267753/best-practices-for-securing-your-sma。少なくとも、KACE SMA がインターネット / パブリックフェーシングとして構成されている場合は、UI アクセスおよびエージェント通信トラフィック用にファイアウォールを介して KACE SMA に受信するポート 443（HTTPS）トラフィックのみを許可する必要があります。

詳細については、https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-を参照してください。

アプライアンスのバックアップおよび FTP アクセスの有効化

本項で説明するように、FTP アクセスを有効にして FTP パスワードを sepgetbxf に設定することにより、Quest で日ベースおよび月ベースのバックアップファイルをローカルの高速ストレージ領域にコピーできます。FTP アクセスには VPN 接続が必要です。

1. 管理者コンソールで、設定 をクリックして、アプライアンスの コントロールパネル に移動します。
2. セキュリティ設定 をクリックします。

   セキュリティ設定 ページが表示されます。
3. 一番上のセクションで、各設定を次のように指定します。

オプション	説明
FTP経由のバックアップを有効にする	バックアップファイルへの FTP アクセスを有効にするには、このチェックボックスをオンにします。
FTPを書き込み可能にする	FTP を使用してバックアップファイルをアップロードするには、このチェックボックスをオンにします。
新しいFTPユーザーパスワード	パスワードとして「sepgetbxf」と入力します。

FTP ユーザーパスワードを設定すると、バックアップサーバーは日ベースおよび月ベースのバックアップファイルをローカルの高速ストレージ領域に自動的にコピーします。バックアップ管理の詳細については、KACE SMAの『Administrator Guide』（管理者ガイド）のメンテナンスの項を参照してください：管理者ガイドおよびオンラインヘルプへのアクセス

管理者ガイドおよびオンラインヘルプへのアクセス

管理者コンソールの使用のヘルプを表示するには、インタフェースの右上隅にあるヘルプリンクをクリックして、コンテキスト依存ヘルプを開きます。メインのヘルプシステムにアクセスするには、コンテキスト依存ヘルプのトピック内のリンクをクリックします。

トレーニングのスケジュール設定

Quest では、アプライアンスの使用に役立てていただけるように、QuickStart と呼ばれるトレーニングプログラムを提供しています。このプログラムは、ネットワーク接続されたデバイスのプロビジョニング、管理、セキュリティ保護、およびサービスを開始するために、ソリューションを迅速に導入して実行するためのリモートアシスタンスを提供します。

サポート技術情報記事

追加の情報については、Quest サポートのサポート技術情報サイト、https://support.quest.com/systems-management-appliance/kb を参照してください。

- アプライアンスに必要なネットワークポート： https://support.quest.com/kb/111775
- パッチ適用に必要なホワイトリストへの追加： https://support.quest.com/kb/111785

- Windowsグループポリシーを使用したKACE SMAエージェントのインストール： https://support.quest.com/kb/133776
- バックアップファイルの操作： https://support.quest.com/kb/111736

当社について

Quest は、急速に変化するエンタープライズ IT の世界にソフトウェアソリューションを提供しています。データの急増、クラウドの拡張、ハイブリッドデータセンター、セキュリティの脅威、規制要件によって生じる課題を簡素化することができます。当社は、Fortune 500 企業の 95 % や Global 1000 企業の 90 % など、100 か国 130,000 社にサービスを提供するグローバルプロバイダです。1987 年以来、データベース管理、データ保護、ID およびアクセス管理、Microsoft プラットフォーム管理、統合エンドポイント管理などのソリューションのポートフォリオを構築してきました。Quest を使用することで、組織は IT 管理に費やす時間を短縮し、ビジネスの革新により多くの時間を費やすことができます。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

Configuração do equipamento

Antes de começar

Antes de configurar a solução, há algumas ações preliminares que você precisa realizar.

1. Verifique se você tem uma inscrição do Microsoft Azure. Após instalar o KACE SMA virtual, a solução funcionará como uma máquina virtual na nuvem do Azure. Para obter mais informações sobre a plataforma de nuvem Azure, ou para se inscrever, consulte http://azure.microsoft.com/en-us/.
2. Compre uma licença para um KACE SMA virtual do Microsoft Azure de vendas da Quest no https://www.quest.com/company/contact-us.aspx.
3. Certifique-se de que as configurações da rede e do firewall permitem acesso de saída para o KACE SMA na porta 443. Essa porta é usada nas comunicações via HTTPS do agente e dos consoles da solução baseados na Web. A porta também deve estar aberta nos dispositivos, incluindo computadores e servidores, que terão o software do agente do KACE SMA instalado.

Exceções de recursos

Todas as funcionalidades do Console do administrador do KACE SMA podem ser configuradas para serem usadas dentro da nuvem. No entanto, alguns recursos exigem acesso direito à sua rede, o que é estabelecido usando uma conexão VPN site-a-site. As conexões VPN aproveitam a rede compartilhada, e uma conexão VPN normalmente é o suficiente para permitir a funcionalidade para uma única empresa. No entanto, em alguns casos, conexões VPN adicionais podem ser necessárias e uma largura de banda de rede dedicada pode ser exigidas. Para obter mais informações, consulte Usar conexões VPN e recursos de rede.

Recursos do Console do administrador que exigem uma conexão VPN

Os seguintes recursos do Console do administrador exigem uma conexão VPN:

- Monitoramento de servidor usando o gerenciamento de dispositivo sem agente.
- Wake On LAN, Descoberta de rede (incluindo Varredura IP, do Active Directory® e do NMAP), provisionamento de agente KACE SMA com base na solução (consulte Provisionamento do agente do KACE SMA para dispositivos gerenciados).

  Esses recursos não exigem uma VPN quando a retransmissão do Agente é usada.

- Recursos de importação e exportação (o compartilhamento de arquivos é bloqueado pelo firewall de nuvem).

- Acesso do FTP aos arquivos de backup (o acesso do FTP é bloqueado pelo firewall de nuvem).
- Os pacotes de soluções e dependências de script devem ser carregados usando o HTTP. Uploads de pacotes grandes podem atingir o tempo limite em conexões de rede mais lentas. Pacotes maiores de 2 GB devem ser distribuídos usando um local de download alternativo de um servidor de arquivos interno.
- Usuário LDAP e rótulos de dispositivos.
- Autenticação de usuário LDAP.
- Importação de usuário LDAP.
- Login único no Active Directory para o Console do administrador e Console do usuário.

Exceções de recursos do Console do usuário

O Console do usuário é a interface que disponibiliza os recursos da biblioteca de software e do service desk para usuários finais. O seguinte recurso do Console do usuário não é compatível com a nuvem:

- Instalações automáticas de software do Console do usuário (downloads são compatíveis).

Criar um máquina virtual KACE SMA no Azure

Este tópico descreve o processo de criação de uma máquina virtual (VM) no Microsoft Azure para servir como KACE Systems Management Appliance (SMA) usando um modelo de VM disponível no Azure Marketplace.

Verifique se você tem uma assinatura do Azure válida. Após instalar o KACE SMA virtual, a solução funcionará como uma máquina virtual na nuvem do Azure. Para obter mais informações sobre a plataforma de nuvem Azure, ou para se inscrever, consulte http://azure.microsoft.com/en-us/.

1. Faça login no https://azuremarketplace.microsoft.com/ usando as credenciais de assinatura do Azure.
2. No campo Pesquisar, digite Solução de gerenciamento de sistemas KACE.
3. Abra o aplicativo da Solução de gerenciamento de sistemas KACE.
4. Revise as informações na seção Planos + Preços para saber mais sobre os requisitos recomendados de recursos de máquina virtual.
5. Clique em OBTER AGORA.
6. Clique em Criar.

A página Criar máquina virtual é exibida e apresenta várias guias. Algumas dessas guias contêm opções que são obrigatórias para configurar uma VM KACE SMA.

> A interface do Azure muda com frequência. Algumas opções podem não corresponder precisamente. Para obter os detalhes mais recentes sobre esta página, visite https://docs.microsoft.com/en-us/azure/.

7. Na página Criar máquina virtual, na guia Básico, forneça as seguintes informações:

Opção	Descrição
Assinatura	Especifique o nome de sua assinatura do Azure.
Grupo de recursos	Crie um grupo de recursos ou use um existente para esta máquina virtual.
Nome da máquina virtual	Digite o nome da máquina virtual que você está prestes a criar.
Imagem	Essa opção exibe a imagem selecionada da Solução de gerenciamento de sistemas KACE.
Tamanho	a. Clique em Alterar tamanho. b. Na página Selecionar tamanho da VM exibida, selecione uma configuração de acordo com os tamanhos de VM recomendados, conforme necessário.
Tipo de autenticação	Forneça os detalhes da autenticação da conta de administrador na máquina virtual. > As credenciais da conta de administrador não serão usadas para acessar a solução. No entanto, estas informações são obrigatórias para qualquer máquina virtual que você criar no Azure, e você precisa especificá-las. a. Selecione Senha. b. No campo Nome de usuário, digite o nome de usuário do administrador da máquina virtual. c. No campo Senha, digite a senha da conta de administrador.

8. Deixe todas as outras opções como estão e clique em Avançar.
9. Na guia Discos, clique em Tipo de disco do SO e selecione SSD Premium. Isso é o mínimo recomendado para a solução.
10. Deixe todas as outras opções como estão e clique em Avançar.
11. Na guia Rede, configure as opções a seguir:

Opção	Descrição
Rede virtual	Selecione uma rede virtual existente ou crie uma.
Sub-rede	Selecione uma sub-rede existente ou defina uma nova.
IP	Use um endereço IP público se quiser se comunicar com o KACE SMA de fora da rede virtual.

Ao atualizar a solução, para rastrear o status da atualização no navegador, você deve abrir a porta 52231. Feche essa porta quando a atualização for aplicada com êxito.

12. Deixe todas as outras opções desta e de todas as guias restantes como estão e clique em Avançar até chegar na guia Revisão.
13. Na guia Revisão, clique em Criar.

    Enquanto a VM é implantada, uma barra de progresso é exibida no navegador. Quando concluído, uma notificação é exibida brevemente, e uma visão geral com os detalhes de sua VM aparece no Azure.

Configurar a solução

Use o assistente Configuração inicial para configurar a solução e fazer login no Console do administrador.

A configuração do navegador determinará o idioma exibido no Console do administrador na primeira vez que você fizer login. Para obter mais informações sobre como alterar as configurações de idioma, consulte o Guia do Administrador do equipamento: Acessar o Guia do administrador e a Ajuda on-line.

1. Obtenha o nome DNS totalmente qualificado da máquina virtual que executa o software da solução no Azure.
   a. No Azure, selecione a máquina virtual e acesse as configurações da Visão geral.
   b. Na página Visão geral, clique em Configurar e defina um nome DNS para o KACE SMA. Por exemplo, my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com.

   Para obter mais informações sobre essas configurações, consulte https://docs.microsoft.com/en-us/azure/.
2. Abra um navegador da Web e insira o URL do Console do administrador usando a seguinte sintaxe:

   http://<nome_único_da_solução_KACE_SMA>/admin

   Onde <nome_único_da_solução_KACE_SMA> é o nome DNS totalmente qualificado da máquina virtual que você configurou na etapa 1.

Por exemplo: http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

A página Acordo de transação de software será exibida.

3. Aceite o acordo.

   O assistente de Configuração inicial será exibido.

4. No assistente Configuração inicial, na página Bem-vindo, verifique se você tem as informações necessárias para configurar o equipamento e clique em Avançar.
5. Na página Autenticação de dois fatores do Console de diagnóstico, confira e anote a chave secreta e os tokens off-line; em seguida, clique em Avançar.
6. Na página Configurações do administrador e licenciamento, forneça as seguintes informações:

Opção	Descrição
Chave de licença	A chave de licença recebida no e-mail de boas-vindas da Quest. Se você não tem uma chave de licença, entre em contato com o Suporte ao software da Quest em https://support.quest.com/contact-support.
Nome da empresa	O nome de sua empresa ou grupo.
E-mail do administrador	O endereço de e-mail em que você deseja receber as comunicações da Quest.
Senha	A senha para a conta de administrador padrão, que é a conta usada para fazer o login no Console do administrador da solução. A conta de administrador padrão é a única conta na solução nesse momento. Caso você esqueça a senha para essa conta, pode ser necessário reiniciar o sistema de volta aos padrões de fábrica, o que pode resultar em perda de dados. **i** Se houver várias soluções KACE SMA ou KACE SDA (Implantação de sistemas) a Quest recomenda usar a mesma senha para a conta de administrador em todas as soluções. Isso permitirá vincular as soluções posteriormente. Para obter mais informações, consulte o Guia do administrador da solução: Acessar o Guia do administrador e a Ajuda on-line.
Autenticação de dois fatores	Se você deseja fornecer mais segurança para os usuários que fizerem login no equipamento, defina essa opção como Ativado. Esse recurso

Opção	Descrição
	adiciona uma etapa adicional para o processo de login. Depende do aplicativo Google Authenticator para gerar códigos de verificação. O aplicativo gera um novo código de seis dígitos em intervalos regulares. Quando ativado, o código de verificação atual será solicitado aos usuários finais sempre que eles fizerem o login. **Nota:** Se você ativar esse recurso, certifique-se de que o relógio do servidor KACE SMA esteja correto, bem como o dispositivo que executa o Google Authenticator. O Google Authenticator depende da hora atual para criar o token. Se o relógio do servidor não estiver sincronizado com os dos dispositivos que executam o Google Authenticator, a validação do token pode falhar, o que pode resultar em bloqueios de contas.

Quando terminar, clique em Avançar.

7. Na página Habilitar compartilhamento de arquivo, siga as instruções na tela para concluir essa etapa.
8. Na página Configurações de domínio, especifique o fuso horário, o nome do host e o nome de domínio da sua solução.

   Essa página também permite que você ative as configurações de DNS personalizadas. Uma instalação padrão usa servidores DNS fornecidos pelo Azure.

   Quando você configurar a VPN site-a-site, também poderá usar seu IP do DNS para tornar o dispositivo acessível para redes internas e públicas (recomendado), ou apenas para a rede interna, dependendo de sua configuração de DNS. Para fazer isso, selecione Ativar DNS personalizado, e no campo DNS principal, digite o endereço IP do DNS. Para obter mais informações, consulte o índice da ajuda nesta página.

   Quando terminar, clique em Avançar.
9. Na página Confirmar, verifique a configuração.

   Caso seja necessário fazer alterações, use o botão Voltar no assistente para ir para a etapa adequada, e atualize sua configuração.

   Quando terminar, clique em Concluir.

   Quando a configuração inicial for concluída, a solução será reiniciada e a página de login do Console do administrador exibida.
10. Faça login no Console do administrador usando a ID de login admin e a senha escolhida durante a configuração inicial.

Se a Autenticação de dois fatores tiver sido ativada na página Configurações do administrador e licenciamento no assistente Configuração inicial, a página Configurar a autenticação de dois fatores será exibida.

11. Apenas Autenticação de dois fatores. Siga as instruções na página Configurar autenticação de dois fatores para gerar um código de verificação do Google Authenticator usando seu smartphone. No campo Código de verificação, digite o código do Google Authenticator, e clique em Concluir configuração. Um novo código de verificação é obrigatório em cada login subsequente.

    Para ignorar essa etapa, clique em Ignorar configuração. Você só pode ignorar essa etapa durante uma janeça de transição configurada. Para obter mais informações, consulte o Guia do administrador.

12. Forneça o nome DNS totalmente qualificado da solução no campo Configurações de rede. Quando você reinicializa a solução no Azure, seu endereço IP é alterado. Os dispositivos se conectam à solução usando esse nome.
    a. Faça login no Console do administrador do KACE SMA e clique em Configurações.
    b. No Painel de controle da solução que aparece, clique em Configurações de rede.
    c. Na página Configurações de rede, na seção Configuração de rede da solução, no campo Nome do servidor web, digite o nome DNS totalmente qualificado da solução registrado na etapa 3.
    d. Clique em Salvar.

    > **!** O Console da linha de comando é uma interface da janela do terminal com a solução. Esta ferramenta permite que você defina as configurações de rede. Não use esta ferramenta para alterar o endereço IP da solução que está em execução no Azure.

O Console do administrador será exibido e a solução estará pronta para uso.

Ativar SSL

Você deve habilitar comunicações seguras entre a solução e os dispositivos gerenciados, e pode usar o Console do administrador da solução para gerar um certificado de SSL.

Obtenha um nome de domínio registrado a ser usado para a solução. Essa etapa é necessária para gerar uma solicitação de assinatura do certificado SSL usando o Console do administrador da solução.

1. No Console do administrador, clique em Configurações para acessar o Painel de controle do equipamento.
2. Clique em Configurações de segurança.

    A página Configurações de segurança é exibida.

3. Na seção SSL, na parte inferior da página, desative o acesso à porta HTTP 80 e encaminhe todo o tráfego da porta 80 para a porta HTTPS 443.

A falha em desativar a porta 80 permite a transmissão de informações confidenciais, como senhas, em texto sem formatação pela Internet.

- Desmarque Ativar acesso à porta 80.
- Selecione Ativar SSL e Ativar encaminhamento da porta 80 para a porta 443.

4. Clique em Formulário de certificado SSL para exibir a página Formulário de certificado SSL.
5. Na seção Configurar, forneça as seguintes informações:

Opção	Descrição
Nome da empresa	O nome de sua empresa.
Nome da organização	O nome de sua unidade organizacional ou grupo de negócios.
Nome comum	O nome comum do dispositivo para o qual você está criando o certificado SSL.
E-mail	Seu endereço de e-mail.
Nome da cidade	O nome da sua localidade.
Nome do estado ou província	O nome do seu estado ou província.
Nome do país	O nome do seu país.

6. Clique em Salvar.
7. Gere um certificado autoassinado.
   a. Clique em Gerar certificado autoassinado para gerar e exibir o certificado abaixo a seção Solicitação de assinatura de certificado.
   b. Clique em Implantar certificado autoassinado e, em seguida, clique em Sim.
   c. Na página Configurações de segurança, clique em Salvar e reiniciar serviços.

   O certificado SSL será gerado. Os certificados autoassinados são convertidos em arquivos PEM, chamados kbox.pem e colocados nas pastas de dados do Agente do KACE SMA. Para mais detalhes sobre as configurações de segurança, consulte o Guia do administrador.

   Se você criar um certificado autoassinado, será necessário implantá-lo a todos os dispositivos gerenciados por Agentes.
8. Reinicie a solução.

Práticas recomendadas

Siga as orientações e recomendações contidas nesta seção ao usar a solução.

Usar conexões VPN e recursos de rede

Se você estiver usando a comunicação tradicional agente-servidor entre a solução e os dispositivos gerenciados, a instalação do agente nos dispositivos gerenciados é tudo o que é necessário para a comunicação. No entanto, se você estiver usando uma conexão VPN, é sua responsabilidade concluir o handshake de rede do ambiente para a solução. A equipe da solução pode fornecer recomendações, como os endereços IP apropriados e portas para liberar, e é fundamental que o administrador de rede esteja envolvido no processo de configuração. As conexões apropriadas de nuvem são configuradas e você precisa assegurar a conexão do seu lado para concluir a configuração com sucesso.

Além disso, alguns recursos da solução exigem uma conexão VPN para serem usados na nuvem, e geralmente uma única conexão VPN é suficiente para uma única empresa. Por exemplo, você pode usar uma única conexão VPN, mesmo que você tenha locais remotos, desde que esses locais possam rotear o tráfego através do site corporativo principal onde a conexão VPN existe. Todo o tráfego do agente do KACE SMA é roteado através da VPN e, em seguida, até a solução através da conexão VPN. Se os locais remotos não puderem ver o site corporativo principal ou se você quiser que cada site tenha um link VPN direto para a solução, você precisa comprar uma conexão VPN para cada site. Para obter mais informações sobre os recursos que exigem conexões VPN, consulte Exceções de recursos.

Os preços de produto baseiam-se na largura de banda da rede compartilhada. Para adquirir recursos de rede adicionais ou para adquirir conexões VPN, entre em contato com o departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx.

Usar conexões VPN com múltiplos domínios

A solução foi projetada para ser usada com um único domínio e uma única conexão VPN. Se você tiver múltiplos domínios, você pode gerenciar os dispositivos (inventário) em outros domínios usando a solução, mas os recursos que exigem acesso VPN estão disponíveis apenas para um único domínio. Por exemplo, você pode fazer a autenticação em um único ambiente do Active Directory para Identity Access Management, mas não pode fazer a autenticação em mais de um domínio. O tráfego do agente a partir do domínio com a conexão VPN é roteado através da conexão VPN, enquanto o tráfego do agente a partir de outros domínios se conecta à solução usando o acesso padrão à Internet. Para obter mais informações sobre os recursos que exigem conexões VPN, consulte Exceções de recursos.

Sobre o endereço IP da solução

A solução é configurada com um único endereço IP. O endereço IP é atribuído pela Quest e esse endereço não pode ser alterado. Você deve criar um registro de Host (A) no seu servidor DNS (Domain Name System) interno para o endereço IP estático da solução, e você pode criar

múltiplos registros A (host) através de várias redes ou domínios para apontar para a sua solução. Se você precisar usar mais de um endereço IP público na rede, terá de adquirir uma instância separada da solução. Várias instâncias da solução não podem compartilhar alguns dados ou algumas informações do banco de dados. Para obter mais informações, entre em contato com o departamento de vendas da Quest em https://www.quest.com/company/contact-us.aspx.

Sobre as configurações de rede

Por padrão, todos os protocolos de rede e seus serviços associados estão desativados, exceto HTTPS e HTTP. Esses protocolos são utilizados nas interfaces de usuário da solução e nas comunicações do agente do KACE SMA. Quando o software KACE SMA Agent é provisionado em um dispositivo, o Agent sempre tenta se conectar ao equipamento usando HTTPS na porta 443 para comunicações criptografadas, se o SSL estiver ativado. Caso contrário, o agente utiliza HTTP através da porta 80.

Provisionamento do agente do KACE SMA para dispositivos gerenciados

O agente do KACE SMA é um aplicativo que pode ser instalado em dispositivos para permitir seu gerenciamento e relatório de inventário por meio da solução. Para provisionar o software do agente para dispositivos diretamente da solução, você deve ter uma conexão VPN. No entanto, há métodos alternativos para implantar o software do agente sem conectividade VPN:

- Baixar e instalar manualmente o agente nos dispositivos. Para obter instruções, consulte o Guia do administrador.
- Instalar o agente usando a Diretiva de Grupo do Windows (GPO). Para obter mais informações, vá para https://support.quest.com/kb/133776.
- Instalar o agente usando outro sistema de gerenciamento: Se a solução Quest estiver substituindo outra solução de gerenciamento de sistemas, é possível implantar o agente usando os métodos de distribuição do sistema que está sendo substituído antes de seu descomissionamento e limpeza.

Configurações de comunicação do agente do KACE SMA

Agentes instalados em dispositivos gerenciados se comunicam periodicamente com a solução para reportar inventários, atualizar scripts e realizar outras tarefas. É possível configurar as definições do agente, incluindo o intervalo de conexão dos agentes, as mensagens exibidas ao usuário e o tempo de retenção de registros. Se houver várias organizações, você pode configurar definições do agente para cada organização separadamente. Para obter mais informações, consulte o Guia do administrador do KACE SMA: Acessar o Guia do administrador e a Ajuda on-line.

Sobre o monitoramento do servidor

A solução tem suporte para o monitoramento do servidor, que proporciona desempenho básico e monitoramento de aplicativos para servidores no inventário. Você pode habilitar o monitoramento para servidores com o agente do KACE SMA e para servidores usando gerenciamento sem agente, e a configuração depende das políticas do departamento de TI. O monitoramento de servidor está disponível para até cinco servidores usando uma licença padrão da solução, e você pode obter uma licença para aumentar esse número.

Se você habilitar o monitoramento de servidores gerenciados por agente, as informações de alerta serão transmitidas pela porta 443 além do protocolo de comunicação de agente existente. Se você ativar o monitoramento para servidores usando o gerenciamento sem agentes, o equipamento utilizará SSH ou Telnet para se conectar ao servidor, ler os logs, verificar se há alertas e exibir os alertas no Console do administrador do KACE SMA. Como o acesso VPN é necessário para o uso do SSH e Telnet, uma conexão VPN é necessária para o monitoramento do servidor sem agente.

Sobre distribuição de arquivos (pacotes) e Compartilhamento de replicação

Com a solução, cada local é uma localidade remota. A Quest recomenda enfaticamente que você configure Compartilhamentos de replicação para cada localidade para otimizar o uso da largura de banda nas conexões com a Internet de escritórios remotos. Os Compartilhamentos de replicação são dispositivos que mantêm cópias de arquivos para distribuição, como, por exemplo, instalações gerenciadas, patches, scripts e atualizações da Dell.

Com o compartilhamento de arquivo Samba desligado, os uploads de arquivo para a solução são limitados a 2 GB. Para arquivos acima de 2 GB, utilize um local de download alternativo para preparar os arquivos dentro da rede corporativa.

Um local alternativo de download pode ser qualquer local de rede que possua todos os arquivos necessários para a instalação de um aplicativo específico. É possível distribuir pacotes a partir de locais de download alternativos, incluindo um endereço de UNC ou fonte DFS. Os protocolos CIFS e SMB, servidores Samba e soluções de servidores de arquivos são compatíveis. O local é especificado ao criar uma Instalação gerenciada. Para obter mais informações, consulte a seção Distribuição do Guia do administrador do KACE SMA: Acessar o Guia do administrador e a Ajuda on-line.

Sobre o uso de largura de banda e largura de banda de rede dedicada

A solução usa uma rede compartilhada de nuvem. Para reduzir os requisitos da largura de banda da rede compartilhada, a Quest recomenda enfaticamente o uso de Compartilhamentos de replicação. Se a solução pode provocar problemas de largura de banda na rede compartilhada, pode ser necessário configurar Compartilhamentos de replicação ou adquirir largura de banda de

rede dedicada. Para obter mais informações, entre em contato com o departamento de vendas da Quest em https://quest.com/company/contact-us.aspx.

Sobre proteção de dados e segurança

Os data centers em nuvem e as soluções da Quest têm uma infraestrutura altamente disponível e fornecem toda a proteção e segurança necessária para a solução. Para obter mais informações sobre as configurações de segurança da solução, consulte a seção de configuração do Guia do administrador do KACE SMA: Acessar o Guia do administrador e a Ajuda on-line.

Uso dos arquivos de backup

Os arquivos de backup são usados para restaurar a solução KACE como um Serviço em caso de perda de dados ou para preservar as configurações durante upgrades, e a Quest automaticamente faz cópias externas do arquivo de backup noturno mais recente para fins de recuperação de desastres.

Você pode acessar os arquivos de backup usando o Console do Administrador. Se os arquivos ficarem muito grandes para download através de HTTP, você pode acessá-las usando FTP. Consulte Fazer backup da solução e ativar o acesso de FTP. Se a largura de banda da rede for limitada, considere a possibilidade de usar uma distribuição de arquivos para baixar grandes arquivos de backup. Consulte Sobre distribuição de arquivos (pacotes) e Compartilhamento de replicação.

A restauração de qualquer tipo de arquivo de backup destruirá os dados configurados no servidor da solução. A Quest recomenda descarregar todos os arquivos de backup ou dados a serem mantidos antes de restaurar as configurações.

Configuração da solução na Internet

Assim como acontece com qualquer aplicativo baseado em servidor Web, as práticas recomendadas de segurança incluem limitar o acesso da Solução de gerenciamento de sistemas KACE (SMA) à Internet. É necessário considerar e revisar cuidadosamente o ambiente para garantir a segurança. É altamente recomendável considerar firewalls, criptografia, acesso a portas, funções, antivírus, SSL, lista de controle de acesso, recuperação de desastres e verificar o tópico a seguir antes de configurar o SMA na Internet: https://support.quest.com/kb/267753/best-practices-for-securing-your-sma. No mínimo, se o KACE SMA estiver configurado como voltado para a Internet/público, apenas o tráfego da porta 443 (HTTPS) deve ter permissão de entrada no firewall, para que o KACE SMA forneça acesso à interface do usuário e tráfego de comunicação do agente.

Para obter mais informações, visite https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-.

Fazer backup da solução e ativar o acesso de FTP

Você pode permitir que a Quest copie arquivos de backup diária e mensalmente para uma área de armazenamento local de alta velocidade, permitindo o acesso de FTP e definindo a senha de FTP para sepgetbxf, conforme descrito nesta seção. O acesso de FTP exige uma conexão VPN.

1. No Console do administrador, clique em Configurações para acessar o Painel de controle do equipamento.
2. Clique em Configurações de segurança.

   A página Configurações de segurança é exibida.
3. Na seção superior, especifique as seguintes configurações:

Opção	Descrição
Habilitar backup via FTP	Marque esta caixa de seleção para permitir o acesso de FTP a arquivos de backup.
Tornar FTP gravável	Marque esta caixa de seleção para usar FTP para carregar arquivos de backup.
Senha de novo usuário do FTP	Digite a seguinte senha: sepgetbxf.

Se a senha de usuário de FTP estiver definida, o servidor de backup automaticamente copia, diariamente e mensalmente, os arquivos de backup para uma área de armazenamento local de alta velocidade. Para obter mais informações sobre o gerenciamento de backups, consulte a seção de manutenção do Guia do administrador do KACE SMA: Acessar o Guia do administrador e a Ajuda on-line.

Acessar o Guia do administrador e a Ajuda on-line

Para obter ajuda usando o Console do administrador, clique no ícone de Ajuda no canto direito superior da interface para abrir a Ajuda contextual. Para acessar o sistema principal da Ajuda, clique nos links nos tópicos de Ajuda contextual.

Programação de treinamento

Para ajudá-lo a começar a usar a solução, a Quest oferece um programa de treinamento chamado QuickStart. Este programa oferece assistência remota para ajudar a preparar rapidamente a solução para uso e começar o provisionamento, o gerenciamento, a proteção e a manutenção de seus dispositivos conectados à rede.

Artigos da Base de conhecimento

Para obter informações adicionais, acesse o site da Base de conhecimento do Suporte da Quest, https://support.quest.com/systems-management-appliance/kb .

- Portas de rede exigidas pela solução: https://support.quest.com/kb/111775
- Listas brancas necessárias para os patches: https://support.quest.com/kb/111785
- Instalar o Agente KACE SMA usando a Política de grupo do Windows: https://support.quest.com/kb/133776
- Trabalhar com arquivos de backup: https://support.quest.com/kb/111736

Sobre nós

A Quest fornece soluções de software para o mundo de TI corporativa em rápida transformação. Ajudamos a simplificar os desafios causados por explosão de dados, expansão de nuvem, data centers híbridos, ameaças de segurança e requisitos normativos. Somos um provedor global de 130.000 empresas em 100 países, incluindo 95% das empresas da Fortune 500 e 90% das empresas da Global 1000. Desde 1987, criamos um portfólio de soluções que agora inclui gerenciamento de banco de dados, proteção de dados, gerenciamento de identidade e acesso, gerenciamento de plataforma da Microsoft e gerenciamento de ponto de extremidade unificado. Com a Quest, as organizações gastam menos tempo na administração de TI e mais tempo na inovação dos negócios. Para obter mais informações, visite www.quest.com.

Recursos de suporte técnico

O suporte técnico está disponível para clientes da Quest com um contrato de manutenção válido e clientes que estão usando versões de teste. Acesse o Portal de suporte da Quest em https://support.quest.com.

O Portal de suporte oferece ferramentas de autoajuda que podem ser usadas para solucionar problemas de forma rápida e independente, 24 horas por dia, 365 dias por ano. O Portal de suporte permite:

- Enviar e gerenciar uma solicitação de serviço
- Consultar artigos da Base de conhecimento
- Inscrever-se para receber notificações de produtos
- Fazer download de software e documentação técnica

- Assista a vídeos de instruções
- Participe de discussões da comunidade
- Converse com os engenheiros de suporte on-line
- Consulte os serviços disponíveis para ajudá-lo com o seu produto.

Configuración del dispositivo

Antes de comenzar

Antes de configurar el dispositivo, hay diversas medidas preliminares que debe tomar.

1. Asegúrese de tener una suscripción a Microsoft Azure. Cuando instale el SMA virtual de KACE, el dispositivo se ejecutará como una máquina virtual en la nube de Azure. Para obtener más información sobre la plataforma de la nube de Azure o para registrarse, consulte http://azure.microsoft.com/en-us/.
2. Adquiera una licencia del SMA virtual de KACE de Microsoft Azure desde Quest Sales en https://www.quest.com/company/contact-us.aspx.
3. Asegúrese de que la configuración de su red y del firewall permita el acceso saliente a KACE SMA en el puerto 443. Este puerto se utiliza para consolas basadas en la web de dispositivos y comunicaciones del agente a través de HTTPS. También debe estar abierto en los dispositivos, incluidos equipos de escritorio y servidores, que tendrán el software agente KACE SMA instalado.

Excepciones de características

Todas las funcionalidades de la Consola del administrador del SMA de KACE se pueden configurar para su uso dentro de la nube. Sin embargo, algunas funciones requieren de acceso directo a la red, el cual se establece mediante una conexión VPN de sitio a sitio. Las conexiones VPN aprovechan la red compartida, y a menudo una única conexión VPN es suficiente para activar la funcionalidad para una sola empresa. Sin embargo, puede que en algunos casos se necesiten conexiones VPN adicionales y un ancho de banda de red dedicado. Para obtener más información, consulte Uso de los recursos de la red y conexiones VPN.

Funciones de la Consola del administrador que requieren una conexión VPN

Las siguientes funciones de la Consola del administrador requieren una conexión VPN:

- Supervisión de servidores mediante administración de dispositivos sin agente.
- Wake On LAN, detección de redes (incluido el análisis de IP, el análisis de Active Directory® y el análisis de NMAP) y aprovisionamiento del agente de SMA de KACE desde el dispositivo (consulte Aprovisionamiento del agente de SMA de KACE en los dispositivos administrados).

Estas funciones no requieren una VPN cuando se utiliza el agente relé.

- Importación y exportación de recursos (el uso compartido de archivos está bloqueado por el firewall de la nube).
- Acceso FTP a los archivos de copia de seguridad (el acceso FTP está bloqueado por el firewall de la nube).
- Los paquetes de aplicaciones y las dependencias de scripts se deben cargar mediante HTTP. Las cargas de paquetes grandes podrían superar el tiempo de espera en conexiones de red lentas. Los paquetes de más de 2 GB se deben distribuir a través de una ubicación de descarga alternativa desde un servidor de archivos interno.
- Etiquetas LDAP de dispositivo y usuario.
- Autenticación de usuario LDAP.
- Importación de usuario LDAP.
- Inicio de sesión único de Active Directory para la Consola del administrador y la Consola de usuario.

Excepciones de características de la consola de usuario

La Consola de usuario es la interfaz que permite que la biblioteca de software y las características de la mesa de servicio estén disponibles para los usuarios finales. La siguiente función de la Consola de usuario no se admite en la nube:

- Instalaciones automáticas de software desde la Consola de usuario (las descargas son compatibles).

Crear una máquina virtual SMA de KACE en Azure

En este tema se describe el proceso de creación de una máquina virtual (VM) en Microsoft Azure para que actúe como el dispositivo KACE Systems Management Appliance (SMA) mediante una plantilla de VM disponible en Azure Marketplace.

Asegúrese de tener una suscripcion de Azure válida. Cuando instale el SMA virtual de KACE, el dispositivo se ejecutará como una máquina virtual en la nube de Azure. Para obtener más información sobre la plataforma de la nube de Azure o para registrarse, consulte http://azure.microsoft.com/en-us/.

1. Inicie sesión en https://azuremarketplace.microsoft.com/ usando sus credenciales de suscripcion a Azure.
2. En el campo Buscar, escriba KACE Systems Management Appliance.
3. Abra la aplicación KACE Systems Management Appliance.

4. Revise la información de la sección Planes + Precios para conocer los requisitos de recursos recomendados para las máquinas virtuales.
5. Haga clic en OBTENER AHORA.
6. Haga clic en Crear.

   Aparece la página Crear máquina virtual, que consta de varias pestañas. Algunas de estas pestañas contienen opciones necesarias para configurar una máquina virtual del SMA de KACE.

   > La interfaz de Azure cambia con frecuencia. Es posible que algunas opciones no coincidan exactamente. Para obtener la información más reciente acerca de esta página, visite https://docs.microsoft.com/en-us/azure/.

7. En la página Crear máquina virtual, en la pestaña Conceptos básicos, proporcione la siguiente información:

Opción	Descripción
Suscripción	Especifique el nombre de su suscripción a Azure.
Grupo de recursos	Cree un grupo de recursos o utilice uno existente para esta máquina virtual.
Nombre de la máquina virtual	Escriba el nombre de la máquina virtual que se va a crear.
Imagen	En esta opción se muestra la imagen seleccionada de KACE Systems Management Appliance.
Tamaño	a. Haga clic en Cambiar tamaño. b. En la página Seleccionar un tamaño de VM que aparezca, seleccione una configuración del tamaño recomendado de la máquina virtual, según sea necesario.
Tipo de autenticación	Proporcione los detalles de autenticación de la cuenta de administrador en la máquina virtual. Las credenciales de la cuenta de administrador no se utilizarán para acceder al dispositivo. Sin embargo, esta información es obligatoria para cualquier máquina virtual que cree en Azure, y debe especificarla. a. Seleccione Contraseña.

Opción	Descripción
	b. En el campo Nombre de usuario, escriba el nombre de usuario del administrador de la máquina virtual. c. En el campo Contraseña, escriba la contraseña de la cuenta de administrador.

8. Deje las opciones restantes sin modificar y haga clic en Siguiente.
9. En la pestaña Discos, haga clic en Tipo de disco del SO y seleccione SSD premium. Este es el mínimo recomendado para el dispositivo.
10. Deje las opciones restantes sin modificar y haga clic en Siguiente.
11. En la pestaña Redes, configure las siguientes opciones:

Opción	Descripción
Red virtual	Seleccione una red virtual existente o cree una nueva.
Subred	Seleccione la subred existente o defina una nueva.
IP	Utilice una dirección IP pública si desea comunicarse con KACE SMA desde fuera de la red virtual.

> Al actualizar el dispositivo, para realizar un seguimiento del estado de la actualización en el navegador, debe abrir el puerto 52231. Cuando la actualización se aplique correctamente, cierre este puerto.

12. Deje sin modificar las opciones restantes en esta pestaña y todas las restantes, y haga clic en Siguiente hasta llegar a la pestaña Revisar.
13. En la pestaña Revisar, haga clic en Crear.

    Mientras se implementa la máquina virtual, aparece una barra de progreso en el navegador. Cuando se completa, en Azure aparece brevemente una notificación, además de una descripción general con los detalles de su Máquina Virtual.

Configurar el dispositivo

Utilice el asistente Configuración inicial para configurar el dispositivo e iniciar sesión en la Consola del administrador.

> La configuración del navegador determina el idioma que se muestra en la Consola del administrador la primera vez que inicia sesión. Para obtener información sobre cómo cambiar los ajustes de idioma, consulte la Guía para el administrador del dispositivo: Acceso a la Guía para el administrador y la ayuda en línea.

1. Obtenga el nombre DNS completo de la máquina virtual que ejecuta el software de dispositivo en Azure.
   a. En Azure, seleccione la máquina virtual y vaya a la configuración de Información general.
   b. En la página Información general, haga clic en Configurar y seleccione un nombre DNS para KACE SMA. Por ejemplo, my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com.

   Para obtener más información sobre estos ajustes, consulte https://docs.microsoft.com/en-us/azure/.

2. Abra un explorador web e ingrese la URL de Consola del administrador utilizando la siguiente sintaxis:

   http://<unique_KACE_SMA_appliance_name>/admin

   Donde <unique_KACE_SMA_appliance_name> es el nombre DNS completo de la máquina virtual que configuró en el paso 1.

   Por ejemplo: http://my-kace-sma-azure-eng.westcentralus.cloudapp.azure.com/admin

   Aparece la página Acuerdo de transacción de software.

3. Acepte el acuerdo.

   Aparece el asistente de Configuración inicial.

4. En el asistente de Configuración inicial, en la página de Bienvenida, verifique que tenga la información necesaria para configurar el dispositivo y, luego, haga clic en Siguiente.
5. En la página Autenticación de dos factores de la consola de diagnóstico, revise y registre la clave secreta y los tokens fuera de línea, y, luego, haga clic en Siguiente.
6. En la página Licencias y ajustes de administrador, proporcione la siguiente información:

Opción	Descripción
Clave de licencia	La clave de licencia que recibió en el correo electrónico de bienvenida de Quest. Si no cuenta con una clave de licencia, comuníquese con Soporte de software de Quest en https://support.quest.com/contact-support.
Nombre de la compañía	El nombre de su compañía o grupo.
Correo electrónico del administrador	La dirección de correo electrónico en la que desea recibir las comunicaciones de Quest.
Contraseña	La contraseña para la cuenta de administrador predeterminada, que es la cuenta que utiliza para iniciar sesión en la Consola del administrador del dispositivo. La cuenta de administrador predeterminada es la única cuenta en el dispositivo en este momento. Si

Opción	Descripción
	olvida la contraseña de esta cuenta, el sistema podría tener que reajustarse a los ajustes de fábrica que pueden resultar en pérdida de datos. Si cuenta con varios dispositivos de SMA de KACE o SDA de KACE (implementación de sistemas), Quest recomienda que use la misma contraseña para la cuenta de administrador en todos los dispositivos. Esto le permitirá vincular los dispositivos posteriormente. Para obtener más información, consulte la Guía para el administrador del dispositivo: Acceso a la Guía para el administrador y la ayuda en línea.
Autenticación de dos factores	Si desea proporcionar una mayor seguridad para los usuarios que inician sesión en el dispositivo, establezca este valor como Habilitado. Esta función agrega un paso adicional en el proceso de inicio de sesión. Se basa en la aplicación Google Authenticator para generar códigos de verificación. La aplicación genera un nuevo código de seis dígitos a intervalos regulares. Cuando esta opción esté habilitada, a los usuarios finales se les solicitará el código de verificación cada vez que inicien sesión. Si habilita esta función, asegúrese de que la hora del servidor KACE SMA sea exacta, así como los dispositivos que ejecutan Google Authenticator. Google Authenticator se basa en la hora actual para crear el token. Si la hora del servidor no está sincronizada con la de los dispositivos que ejecutan Google Authenticator, la validación del token puede fallar, lo que podría ocasionar un bloqueo de la cuenta.

Cuando haya terminado, haga clic en Siguiente.

7. En la página Habilitar uso compartido de archivos, siga las instrucciones en pantalla para completar este paso.
8. En la página Ajustes de dominio, especifique la zona horaria, el nombre de host y el nombre de dominio de su dispositivo.

Esta página también le permite activar ajustes personalizados de DNS. En una instalación predeterminada, se utilizan servidores DNS proporcionados por Azure.

Cuando configure VPN de sitio a sitio, también puede usar su IP de DNS para acceder al dispositivo desde redes públicas e internas (recomendado) o simplemente desde la red interna, según su configuración de DNS. Para ello, seleccione Habilitar DNS personalizado y, en el campo DNS primario, escriba la dirección IP del DNS. Para obtener más información, consulte el contenido de ayuda en esta página.

Cuando haya terminado, haga clic en Siguiente.

9. En la página Confirmar, revise la configuración.

   Si debe realizar cambios, utilice el botón Atrás en el asistente para ir al paso correspondiente y actualizar la configuración.

   Cuando haya terminado, haga clic en Finalizar.

   Cuando finaliza la configuración inicial, el dispositivo se reinicia y aparece la página de inicio de sesión de Consola del administrador.

10. Inicie sesión en Consola del administrador con la ID de inicio de sesión admin y la contraseña que eligió en la configuración inicial.

    Si la autenticación de dos factores está habilitada en la página Licencias y ajustes de administrador, en el asistente de Configuración inicial, aparecerá la pantalla Configurar autenticación de dos factores.

11. Autenticación de dos factores solamente. Siga las instrucciones que aparecen en la página Configurar autenticación de dos factores para generar un código de verificación de Google Authenticator utilizando su teléfono inteligente. En el campo Código de verificación, escriba el código de Google Authenticator y haga clic en Finalizar configuración. Se necesita un nuevo código de verificación para cada inicio de sesión posterior.

    Para omitir este paso, haga clic en Omitir configuración. Solo se puede omitir este paso durante un período de transición configurado. Para obtener más información, consulte la Guía para el administrador.

12. Proporcione el nombre DNS completo del dispositivo en los Ajustes de redes. Cuando reinicia el dispositivo en Azure, cambia su dirección IP. Los clientes se conectan al dispositivo mediante este nombre.
    a. Inicie sesión en el SMA de KACE Consola del administrador y haga clic en Ajustes.
    b. En el Panel de control del dispositivo que aparece, haga clic en Ajustes de redes.
    c. En la página Configuración de redes, en la sección Configuración de red del dispositivo, en el campo Nombre del servidor web, escriba el nombre DNS completo del dispositivo que registró en el paso 3.
    d. Haga clic en Guardar.

La consola de la línea de comandos es una interfaz de ventana de terminal para el dispositivo. Esta herramienta le permite configurar los ajustes de redes. No debe usar esta herramienta para cambiar la dirección IP del dispositivo que se ejecuta en Azure.

Aparece la Consola del administrador y el dispositivo está listo para usarse.

Habilite SSL

Debe habilitar las comunicaciones seguras entre el dispositivo y los dispositivos administrados, y puede utilizar la Consola del administrador del dispositivo para generar un certificado SSL.

Obtenga un nombre de dominio registrado para usarlo en el dispositivo. Esto es necesario para generar una solicitud de firma de certificado SSL mediante la Consola del administrador del dispositivo.

1. En la Consola del administrador, haga clic en Ajustes para ir al Panel de control del dispositivo.
2. Haga clic en Ajustes de seguridad.

   Aparece la página Ajustes de seguridad.
3. En la sección SSL, que se encuentra en la parte inferior de la página, deshabilite el acceso al puerto HTTP 80 y reenvíe todo el tráfico del puerto 80 al puerto HTTPS 443.

   ! Si no se deshabilita el puerto 80, se puede transmitir información confidencial, como contraseñas, en texto sin formato a través de Internet.

   - Desactive Habilitar acceso al puerto 80.
   - Seleccione Habilitar SSL y Habilitar reenvío del puerto 80 al puerto 443.
4. Haga clic en Formulario de certificado SSL para visualizar la página Formulario de certificado SSL.
5. En la sección de Configuración, escriba la siguiente información:

Opción	Descripción
Nombre de la compañía	El nombre de su compañía.
Nombre de la organización	El nombre de su unidad organizativa o su grupo de negocios.
Nombre común	El nombre común del dispositivo para el que está creando el certificado SSL.
Correo electrónico	Su dirección de correo electrónico.
Nombre de la ciudad	El nombre de su localidad.
Nombre del estado o provincia	El nombre de su estado o provincia.
Nombre del país	El nombre de su país.

6. Haga clic en Guardar.
7. Genere un certificado autofirmado.

a. Haga clic en Crear un certificado autofirmado para generar y mostrar el certificado bajo la sección Solicitud de firma de certificado.
b. Haga clic en Implementar certificado autofirmado, a continuación, haga clic en Sí.
c. En la página Ajustes de seguridad, haga clic en Guardar y reiniciar los Servicios.

Se genera el certificado SSL. Los certificados autofirmados se convierten en archivos PEM, denominados kbox.pem, y se colocan en las carpetas de datos del agente de SMA de KACE. Para obtener más detalles sobre la configuración de seguridad, consulte la Guía para el administrador.

Si crea un certificado autofirmado, tendrá que implementar ese certificado en todos los dispositivos administrados por el agente.

8. Reinicie el dispositivo.

Mejores prácticas

Siga las directrices y recomendaciones en esta sección cuando utilice el dispositivo.

Uso de los recursos de la red y conexiones VPN

Si está utilizando la comunicación agente-servidor tradicional entre el equipo y sus dispositivos administrados, todo lo que se requiere para la comunicación es instalar el agente en los dispositivos administrados. Sin embargo, si está utilizando una conexión VPN, es su responsabilidad completar el protocolo de enlace de su entorno al equipo. El equipo del dispositivo puede proporcionar recomendaciones, como las direcciones IP y los puertos apropiados para autorizar, y es esencial que el administrador de red se involucre en el proceso de configuración. Las conexiones correspondientes a la nube están configuradas; debe asegurarse de que la conexión en su lado permita completar la configuración correctamente.

Además, algunas características del dispositivo requieren el uso de una conexión VPN en la nube y generalmente una única conexión VPN es suficiente para una sola empresa. Por ejemplo, puede utilizar una única conexión VPN incluso si tiene ubicaciones remotas siempre que dichas ubicaciones puedan enrutar el tráfico a través del sitio corporativo principal donde existe la conexión VPN. Todo el tráfico del agente de SMA de KACE se envía a través de la VPN y luego al dispositivo a través de la conexión VPN. Si las ubicaciones remotas no pueden ver el sitio corporativo principal o si desea que cada sitio tenga un vínculo VPN directo al dispositivo, necesita comprar una conexión VPN para cada sitio. Para obtener más información sobre las funciones que requieren conexiones VPN, consulte Excepciones de características.

Los precios del producto se basan en el ancho de banda de red compartida. Para adquirir recursos de red adicionales o conexiones VPN, comuníquese con ventas de Quest en https://www.quest.com/company/contact-us.aspx.

Uso de conexiones VPN con varios dominios

El dispositivo está diseñado para su uso con un dominio único y una conexión VPN única. Si tiene varios dominios, puede administrar los dispositivos (inventario) en otros dominios utilizando el dispositivo, pero las características que requieren acceso VPN solo están disponibles para un solo dominio. Por ejemplo, puede autenticarse en un único entorno de Active Directory para la administración de acceso de identidad, pero no puede autenticarse en más de un dominio. El tráfico de agente desde el dominio con la conexión VPN se enruta a través de la conexión VPN, mientras que el tráfico de agente para otros dominios se conecta al dispositivo utilizando el acceso a Internet estándar. Para obtener más información sobre las funciones que requieren conexiones VPN, consulte Excepciones de características.

Acerca de la dirección IP del dispositivo

El dispositivo está configurado para una única dirección IP. La dirección IP la asigna Quest y no se puede cambiar. Debe crear un registro host (A) en el servidor del sistema de nombres de dominio (DNS) interno para la dirección IP estática del dispositivo y puede crear varios registros A (host) en varias redes o dominios para señalar su dispositivo. Si necesita usar más de una dirección IP pública para su red, deberá adquirir una instancia independiente del dispositivo. Varias instancias del dispositivo no pueden compartir ningún dato ni información de la base de datos. Para obtener más información, comuníquese con ventas de Quest en https://www.quest.com/company/contact-us.aspx.

Acerca de los ajustes de redes

De manera predeterminada, todos los protocolos de red y sus servicios asociados están deshabilitados, excepto para HTTPS y HTTP. Estos protocolos se utilizan para las interfaces de usuario de dispositivos y en las comunicaciones del agente de SMA de KACE. Cuando el software KACE SMA Agent se integra en un dispositivo, siempre intenta conectarse a este mediante HTTPS a través del puerto 443 para comunicaciones cifradas si SSL está habilitado. En caso contrario, el agente utiliza HTTP a través del puerto 80.

Aprovisionamiento del agente de SMA de KACE en los dispositivos administrados

El agente de SMA de KACE es una aplicación que se puede instalar en los dispositivos para permitir la administración de dispositivos y los informes de inventario a través del dispositivo. Para aprovisionar el software agente en los dispositivos directamente desde el dispositivo, debe tener una conexión VPN. Sin embargo, existen métodos alternativos para implementar el software agente sin conectividad VPN:

- Descargue e instale manualmente el agente en los dispositivos. Para ver las instrucciones, consulte la Guía para el administrador.

- Instale el agente mediante la Directiva de grupo de Windows (GPO). Para obtener más información, visite https://support.quest.com/kb/133776.
- Instale el agente utilizando otro sistema de administración: Si la solución Quest está reemplazando a otra solución de administración de sistemas, puede implementar el Agente mediante los métodos de distribución del sistema que se va a reemplazar antes de su retiro y limpieza.

Configuración de los ajustes de comunicación del agente de SMA de KACE

Los agentes instalados en dispositivos administrados se comunican periódicamente con el dispositivo para informar el inventario, actualizar scripts y realizar otras tareas. Puede configurar los ajustes del agente, como el intervalo en el que se registran los agentes, los mensajes que se muestran a los usuarios y el tiempo de retención de registros. Si tiene varias organizaciones, puede configurar ajustes del agente para cada organización por separado. Para obtener más información, consulte la Guía para el administrador de SMA de KACE: Acceso a la Guía para el administrador y la ayuda en línea.

Acerca de la supervisión del servidor

El dispositivo admite supervisión de servidores, que corresponde a una supervisión básica de rendimiento y aplicaciones de los servidores en el inventario. Puede habilitar la supervisión de servidores con el agente de SMA de KACE y de servidores que utilizan administración sin agente; la configuración depende de las políticas del departamento de TI. La supervisión de servidores está disponible para un máximo de cinco servidores que utilizan una licencia estándar del dispositivo. Puede obtener una licencia para aumentar esa cantidad.

Si habilita la supervisión de servidores administrados por agente, la información de la alerta se transmite a través del puerto 443, además del protocolo de comunicaciones de agente existente. Si habilita la supervisión de servidores con administración sin agente, el dispositivo utiliza SSH o Telnet para conectarse al servidor, leer los registros, verificar las alertas y visualizar las alertas en la Consola del administrador de SMA de KACE. Puesto que se requiere acceso VPN para el uso de SSH y Telnet, se requiere una conexión VPN para la supervisión de servidores sin agente.

Acerca de la distribución de archivos (paquetes) y recursos compartidos de replicación

Con el dispositivo, cada sitio es un sitio remoto. Quest recomienda encarecidamente configurar recursos compartidos de replicación para cada sitio con el fin de optimizar el uso de ancho de banda en las conexiones a Internet en oficinas remotas. Los recursos compartidos de replicación son dispositivos que mantienen copias de los archivos para su distribución, tales como instalaciones administradas, parches, scripts y actualizaciones de Dell.

Con los recursos compartidos de archivo Samba desactivados, las cargas de archivos en el dispositivo están limitadas a 2 GB. Para archivos que exceden 2 GB, utilice una ubicación de descarga alternativa para guardar los archivos dentro de la red corporativa.

Una ubicación de descarga alternativa puede ser cualquier ubicación de la red que tenga todos los archivos necesarios para instalar una aplicación en particular. Puede distribuir paquetes desde ubicaciones de descarga alternativas, como una dirección UNC o un origen DFS. Admite los protocolos CIFS y SMB, los servidores Samba y los dispositivos del servidor de archivos. Especifica la ubicación cuando crea una instalación administrada. Para obtener más información, consulte la sección Distribución de la Guía para el administrador de SMA de KACE: Acceso a la Guía para el administrador y la ayuda en línea.

Acerca del uso del ancho de banda y ancho de banda de red dedicada

El dispositivo utiliza una red en la nube compartida. Para reducir los requisitos de ancho de banda de la red compartida, Quest recomienda encarecidamente el uso de recursos compartidos de replicación. Si el dispositivo produce problemas de ancho de banda en la red compartida, puede ser necesario configurar recursos compartidos de replicación o adquirir ancho de banda de red dedicada. Para obtener más información, comuníquese con ventas de Quest en https://quest.com/company/contact-us.aspx.

Acerca de la seguridad y la protección de datos

Los centros de datos en la nube y los dispositivos Quest disponen de una infraestructura de alta disponibilidad y proporcionan toda la protección y la seguridad necesarias para el dispositivo. Para obtener más información acerca de los ajustes de seguridad de los dispositivos, consulte la sección sobre configuración de la Guía para el administrador de SMA de KACE: Acceso a la Guía para el administrador y la ayuda en línea.

Uso de archivos de copia de seguridad

Los archivos de copia de seguridad se utilizan para restaurar el dispositivo KACE como un servicio en caso de pérdida de datos o para conservar los ajustes durante una actualización; Quest hace automáticamente copias externas del archivo de copia de seguridad nocturna más reciente para la recuperación ante desastres.

Puede tener acceso a los archivos de copia de seguridad utilizando la consola del administrador. Si los archivos son demasiado grandes para descargarlos con HTTP, puede acceder a ellos mediante FTP. Consulte Hacer copia de seguridad del dispositivo y habilitar el acceso a FTP. Si el ancho de banda es limitado, considere el uso de distribución de archivos para descargar archivos de copia de seguridad grandes. Consulte Acerca de la distribución de archivos (paquetes) y recursos compartidos de replicación.

La restauración de cualquier tipo de archivo de copia de seguridad destruye todos los datos actualmente configurados en el servidor del dispositivo. Quest recomienda que descargue

todos los datos o archivos de copia de seguridad que quiera conservar antes de realizar una restauración de los ajustes.

Configuración del dispositivo en Internet

Al igual que con cualquier aplicación basada en servidor web, las prácticas recomendadas de seguridad incluyen la limitación del acceso a KACE Systems Management Appliance (SMA) desde Internet. Para garantizar la seguridad, es necesario considerar y verificar cuidadosamente el entorno. Se recomienda encarecidamente considerar los firewall, el cifrado, el acceso a los puertos, las funciones, el antivirus, el SSL, la lista de control de acceso, la recuperación ante desastres y la revisión del siguiente tema antes de configurar SMA en Internet: https://support.quest.com/kb/267753/best-practices-for-securing-your-sma. Como mínimo, si KACE SMA está configurado como orientado a Internet/público, solo el tráfico del puerto 443 (HTTPS) debería permitir la entrada a través de un firewall a KACE SMA para el acceso a la interfaz de usuario y el tráfico de comunicaciones del agente.

Para obtener más información, visite https://support.quest.com/kb/111775/which-network-ports-and-urls-are-required-for-the-kace-k1000-appliance-to-function-.

Hacer copia de seguridad del dispositivo y habilitar el acceso a FTP

Puede habilitar Quest para copiar archivos de copia de seguridad diarios y mensuales a un área de almacenamiento de alta velocidad local mediante la habilitación de acceso a FTP y la configuración de la contraseña de FTP como sepgetbxf, según se describe en esta sección. El acceso a FTP requiere una conexión VPN.

1. En la Consola del administrador, haga clic en Ajustes para ir al Panel de control del dispositivo.
2. Haga clic en Ajustes de seguridad.

   Aparece la página Ajustes de seguridad.
3. En la sección superior, especifique los siguientes ajustes:

Opción	Descripción
Habilitar copia de seguridad a través del FTP	Seleccione esta casilla de verificación para habilitar el acceso de FTP a los archivos de copia de seguridad.
Convertir el FTP en grabable	Seleccione esta casilla para utilizar FTP para cargar archivos de copia de seguridad.
Contraseña de nuevo usuario de FTP	Escriba la siguiente contraseña: sepgetbxf.

   Si la contraseña de usuario de FTP está configurada, el servidor de copia de seguridad copia automáticamente los archivos de copia de seguridad diarios y mensuales a un área

de almacenamiento de alta velocidad local. Para obtener más información acerca de la administración de copias de seguridad, consulte la sección sobre mantenimiento de la Guía para el administrador de SMA de KACE: Acceso a la Guía para el administrador y la ayuda en línea.

Acceso a la Guía para el administrador y la ayuda en línea

Para obtener ayuda a través de la Consola del administrador, haga clic en el vínculo de Ayuda en la esquina superior derecha de la interfaz para abrir la ayuda contextual. Para acceder al sistema de ayuda principal, haga clic en los vínculos incluidos en los temas de ayuda contextual.

Programación de la capacitación

Para ayudarlo a comenzar a usar el dispositivo, Quest proporciona un programa de capacitación denominado QuickStart. En este programa se proporciona asistencia remota para ayudarlo a poner en marcha su solución rápidamente y comenzar el aprovisionamiento, la gestión, la protección y el mantenimiento de sus dispositivos conectados a la red.

Artículos de la base de conocimientos

Para obtener información adicional, vaya al sitio de la base de conocimientos de soporte de Quest https://support.quest.com/systems-management-appliance/kb .

- Puertos de red requeridos por el dispositivo: https://support.quest.com/kb/111775
- Listas blancas requeridas para la aplicación de parches: https://support.quest.com/kb/111785
- Instalación del agente de SMA de KACE mediante la política de grupo de Windows: https://support.quest.com/kb/133776
- Trabajo con archivos de copia de seguridad: https://support.quest.com/kb/111736

Acerca de nosotros

Quest proporciona soluciones de software para los rápidos cambios en el mundo de la TI empresarial. Ayudamos a simplificar los desafíos causados por la explosión de datos, la expansión de la nube, los centros de datos híbridos, las amenazas de seguridad y los requisitos regulatorios. Somos un proveedor global de 130 000 empresas en 100 países, incluido el 95 % de las primeras 500 empresas del mundo y el 90 % de las primeras 1000 empresas globales. Desde 1987, hemos creado una cartera de soluciones que ahora incluye administración de

bases de datos; administración de protección, identidad y acceso de datos; administración de la plataforma de Microsoft; y administración de terminales unificados. Con Quest, las organizaciones invierten menos tiempo en la administración de TI y más tiempo en la innovación empresarial. Para obtener más información, visite www.quest.com.

Recursos del soporte técnico

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

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

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

Legal notices

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.

Trademarks

trademark-information.aspx. All other trademarks and registered trademarks are property of their respective owners.

Legend

A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.

An information icon indicates supporting information.

KACE Systems Management Appliance Setup Guide for Azure Platforms

Updated - June 2019

Software Version - 10.0