

Quest® InTrust 11.6.1

Auditing Microsoft Azure



© 2024 Quest Software Inc. ALL RIGHTS RESERVED.

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

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

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

Quest Software Inc.

Attn: LEGAL Dept

4 Polaris Way

Aliso Viejo, CA 92656

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



Patents

Quest Software is proud of our advanced technology. Patents and pending patents may apply to this product. For the most current information about applicable patents for this product, please visit our website at <https://www.quest.com/legal>.

Trademarks

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

Legend

-  **CAUTION: A CAUTION icon indicates potential damage to hardware or loss of data if instructions are not followed.**
-  **IMPORTANT, NOTE, TIP, MOBILE, or VIDEO: An information icon indicates supporting information.**

InTrust Auditing Microsoft Azure

Updated - September 2024

Version - 11.6.1

Contents

Overview	4
How It Works	5
Retrieval of Logs from Virtual Machines	5
Retrieval of Azure Logs	5
Installation	6
Providing Access to Your Azure Environment	7
Get Your Shortcuts Handy	7
Look Up the Tenant ID, Application ID and Application Key	9
Look Up the Subscription ID	13
Look Up the Storage Account Connection String	14
Look Up the Event Hub Connection Strings and Consumer Group	17
Collecting Events from Azure Virtual Machines	20
Azure Collection Specifics	20
Collecting Events from Azure Event Hubs	21
Azure Log (Event Hub) Collection Specifics	22
Analyzing Azure Events	23
Known Issues	24
About us	26
Contacting Quest	26
Technical support resources	26

Overview

The Azure Knowledge Pack for InTrust helps you extend your auditing scope to your Azure-based resources. Using the familiar InTrust Deployment Manager workflow with minor adjustments, you can collect the following:

- Events from Windows virtual machines hosted in Azure.
- Events that originate in Azure and are directed to event hubs.

i **IMPORTANT:** This distribution of the Azure Knowledge Pack is a technical preview with known limitations and issues, which are noted in the documentation (see [Known Issues](#)). Quest appreciates your feedback on the available functionality and will try hard to complete the solution and align it with your expectations. In the final release of the Azure Knowledge Pack, the workflow will be more streamlined and auditing of a variety of other Azure resources will be supported, including the Activity log, Azure portal permission and role assignments and Managed SQL.

To download the Azure Knowledge Pack technical preview, go to <https://support.quest.com/intrust/11.4.1/download-new-releases>. Note that the Knowledge Pack is compatible only with InTrust 11.4.1 *without* Update 1.

How It Works

The Azure Knowledge Pack adds two dedicated types of collection to InTrust Deployment Manager:

- **Azure collection**
This type of collection contains virtual machines that are included in the Azure resource group that you specify. In a fully populated Azure collection, the items look and feel the same as Windows computers in a regular Windows collection.
- **Azure log (Event Hub) collection**
This type of collection contains Azure event hubs instead of computers.

Retrieval of Logs from Virtual Machines

The Azure Knowledge Pack provides the Azure Proxy Service, which resides both on the on-premises InTrust server and on the individual Azure virtual machines that events come from. The service performs the following sets of tasks, depending on where it is running:

- On an Azure virtual machine, it works alongside a regular InTrust agent and collects data directly to the Azure blob storage.
- On the InTrust server, it retrieves data from the Azure blob storage and puts it in a repository.

The two parts of the solution never communicate with each other. Their only shared resource is the blob storage.

Retrieval of Azure Logs

Azure logs are collected through communication with Azure event hubs. A specialized Azure Knowledge Pack component on the InTrust server is responsible for connection to the specified event hub and retrieval of events from it.

Installation

Due to the technical preview status of this distribution of the Azure Knowledge Pack, it is recommended that you deploy it in a dedicated sandboxed InTrust organization. The best configuration for the Azure Knowledge Pack technical preview is InTrust Server and InTrust Deployment Manager on the same server, which is in its own InTrust organization.

In this configuration, to install the Azure Knowledge Pack on the server of your choice:

1. Make sure none of the following applications are running: InTrust Deployment Manager, InTrust Manager, Repository Viewer.
2. Run the **InTrust_AzureKP.11.4.1.*.msi** file provided to you. This will upgrade InTrust Server on the computer.
3. Run the **RTC_UI.11.4.1.*.msi** file. This will upgrade InTrust Deployment Manager on the computer.

If you need to work with this instance of the Azure Knowledge Pack on a different computer, install InTrust Deployment Manager on that computer, and then upgrade InTrust Deployment Manager using the **RTC_UI.11.4.1.*.msi** file.

i **IMPORTANT:** Deploying this technical preview in your production environment is discouraged, because this may result in InTrust configuration conflicts. In addition, upgrading InTrust from version 11.4.1 will cause the features of this technical preview to stop working.
For more details and caveats, see [Known Issues](#).

Providing Access to Your Azure Environment

Before you can set up Azure auditing in InTrust, you need to retrieve a number of settings from your Azure environment and possibly create a few dedicated Azure objects for auditing purposes. After you have made notes of the necessary configuration data, you will be ready to supply it in InTrust Deployment Manager. The following configuration information is required:

- For real-time collection from Azure virtual machines:
 - Resource group name
 - Tenant ID
 - Application ID
 - Application key
 - Subscription ID
 - Storage account connection string
- For gathering from event hubs:
 - Consumer group name
 - Event hub connection strings
 - Storage account connection string

All of these settings are available on the Azure portal. If you are not sure where to look up any of them, see the following few topics. If you don't need guidance for getting them, skip directly to [Collecting Events from Azure Virtual Machines](#) or [Collecting Events from Azure Event Hubs](#).



IMPORTANT:

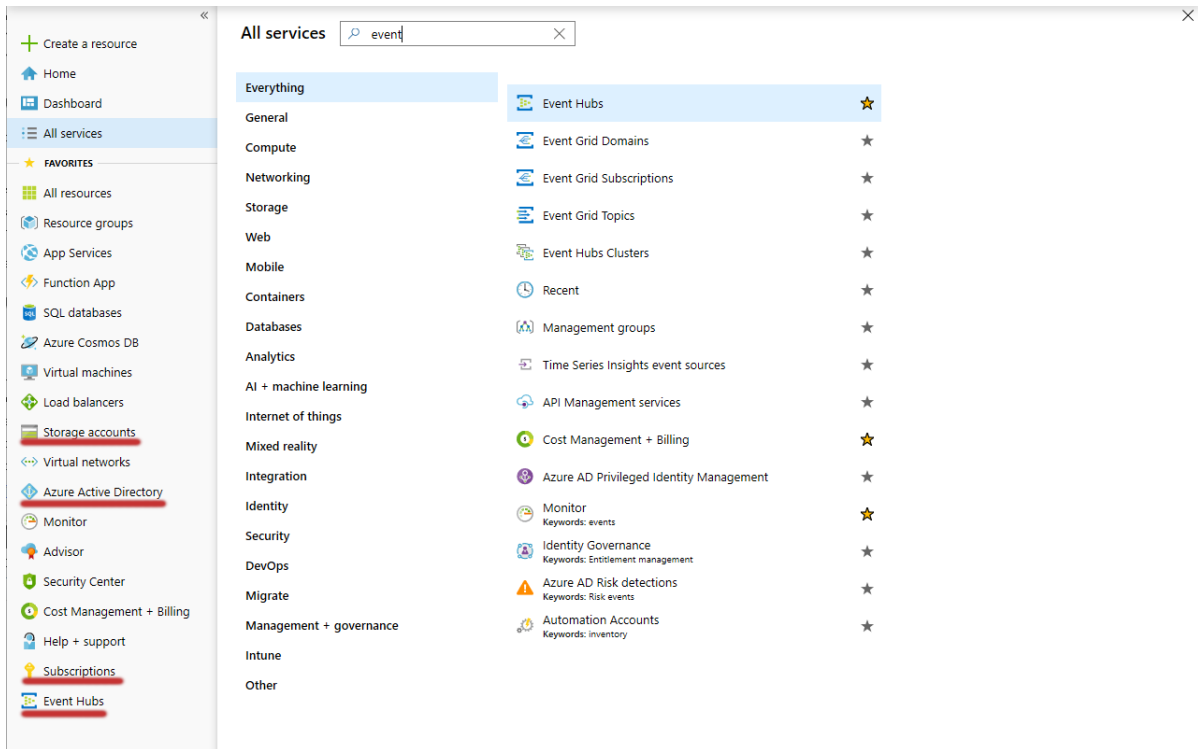
- In this technical preview, the scope of auditing for Azure virtual machines is a single resource group. A single Azure Knowledge Pack deployment cannot audit multiple resource groups. Populate your resource groups accordingly.
- If you want to use multiple deployments of the Azure Knowledge Pack for auditing Azure virtual machines (for example, as a way to audit multiple resource groups), make sure each resource group is audited and each storage account is used by only one deployment.

Get Your Shortcuts Handy

For quick access to all the necessary configuration data, make sure the Favorites list on the Azure portal contains the followings items:

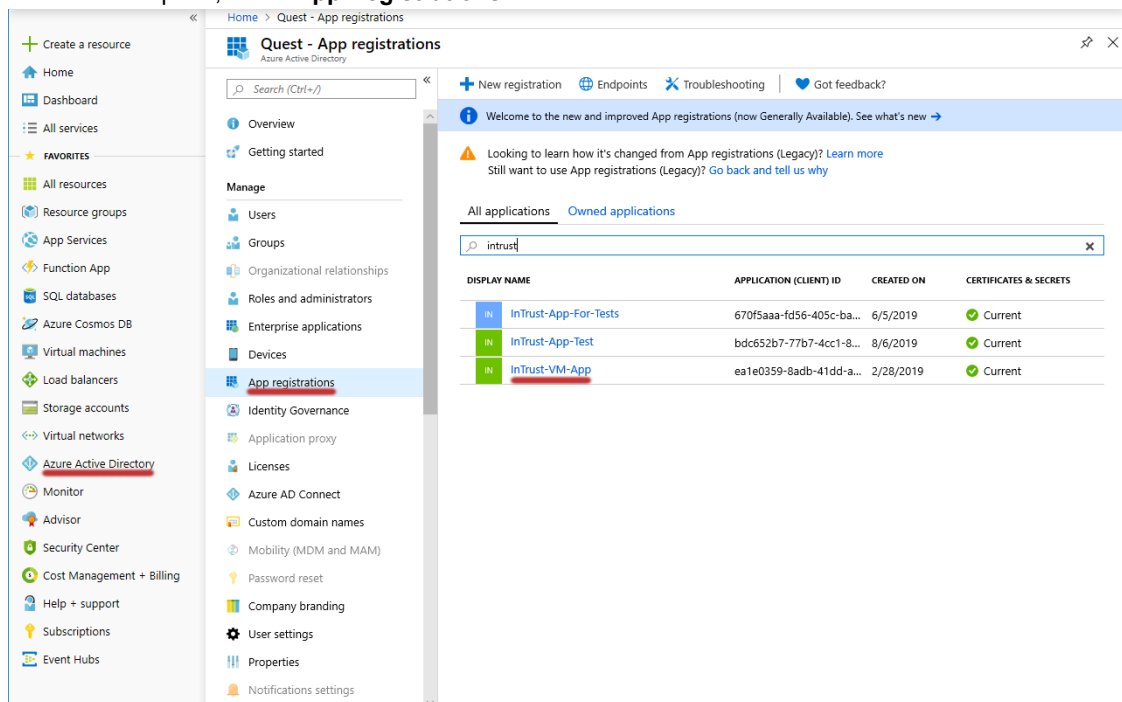
- Azure Active Directory
- Subscriptions
- Storage accounts
- Event hubs

If any of these items is absent from the list, click **All services** above the list, search for them and add them by selecting their star icons.



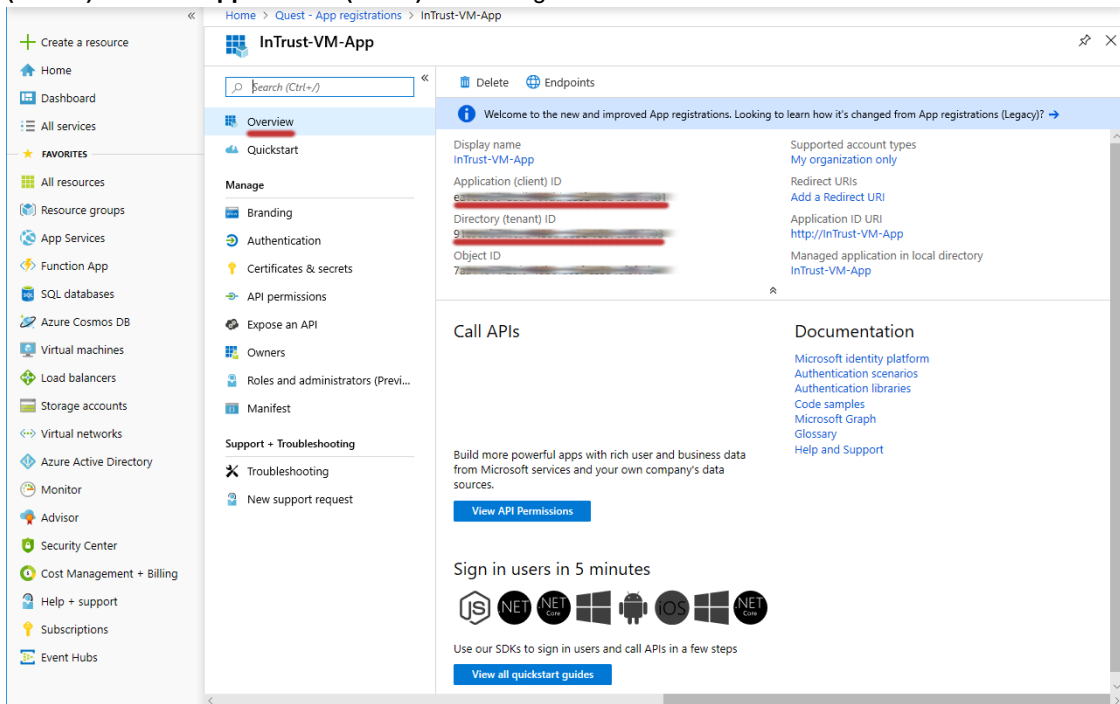
Look Up the Tenant ID, Application ID and Application Key

1. In the Favorites list, click **Azure Active Directory**.
2. In the menu pane, click **App registrations**.

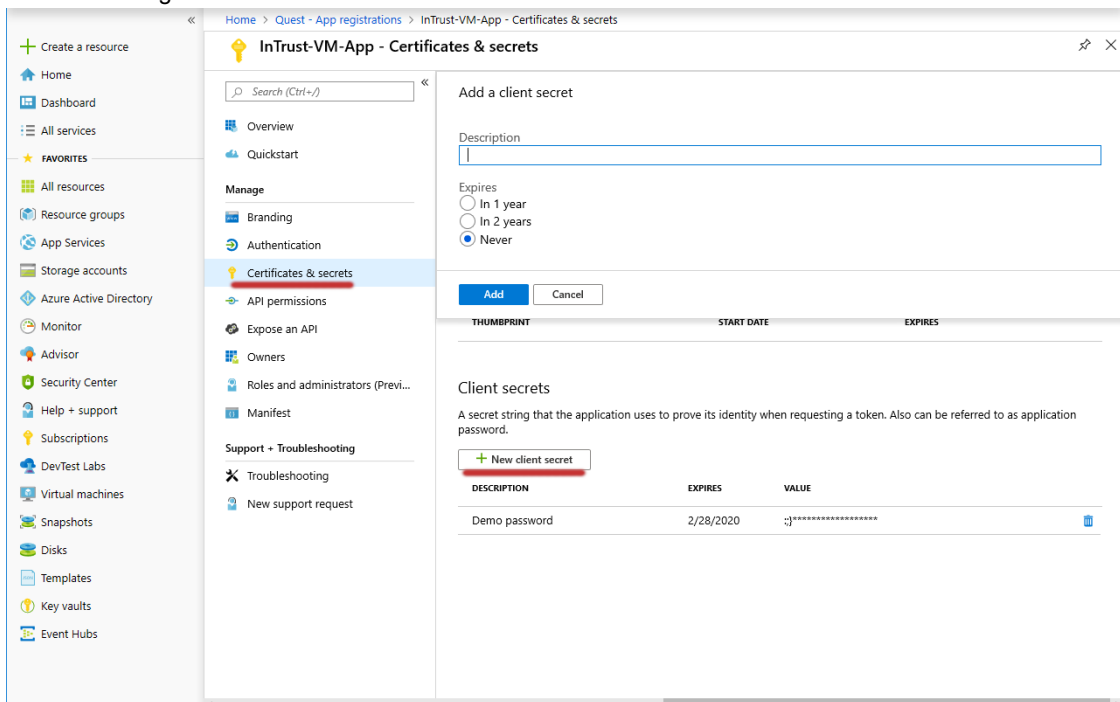


3. If you have an existing application dedicated to InTrust, search for it and select it. Otherwise, create a new application by clicking **New**. Supply a meaningful name, and for the remaining options you can leave the default settings.
4. Make sure the application is registered with the right Azure subscription. If you need details, see the **To register an application with a subscription** procedure below.

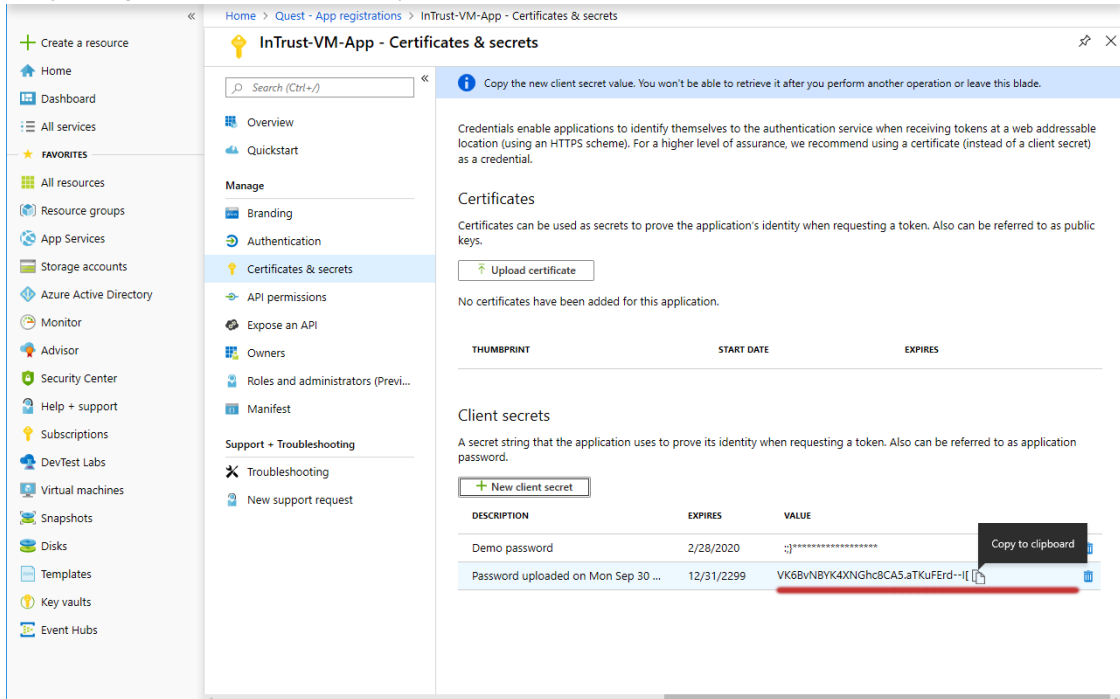
- On the **Overview** screen for the application you specified, copy the values of the **Directory (tenant) ID** and **Application (client) ID** settings and save them for later use.



- In the menu pane, switch to the **Certificates & secrets** screen.
- Under **Client secrets**, click **New client secret**. In the popup that is displayed, configure the secret's settings and click **Add**.

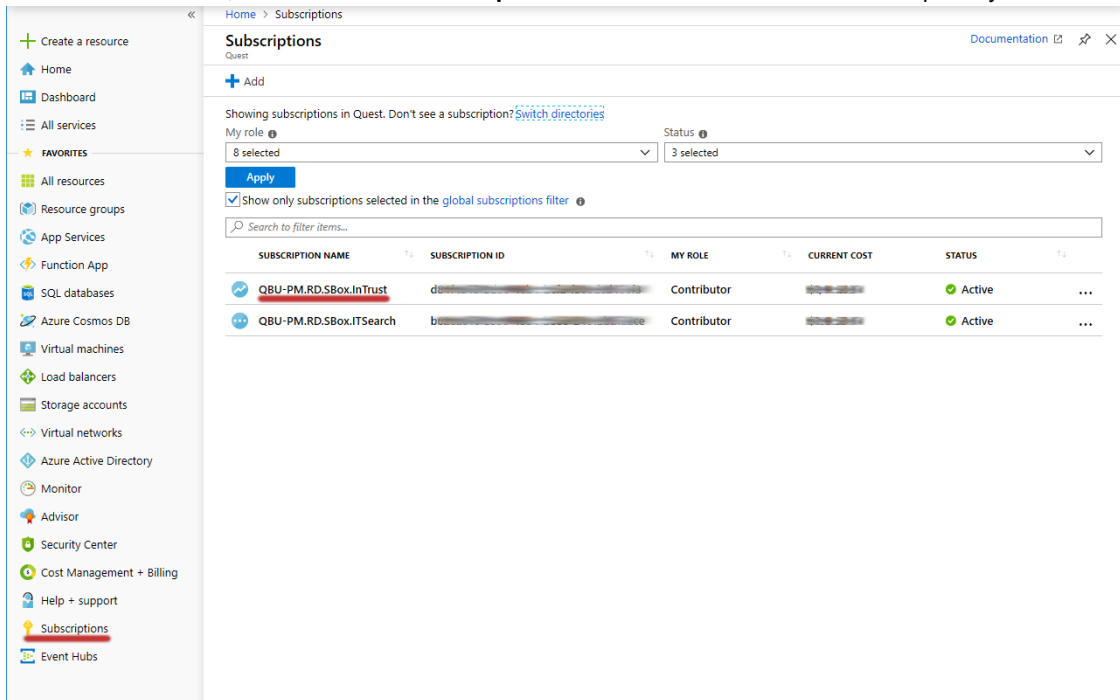


- Copy the generated application key and save it for later use.



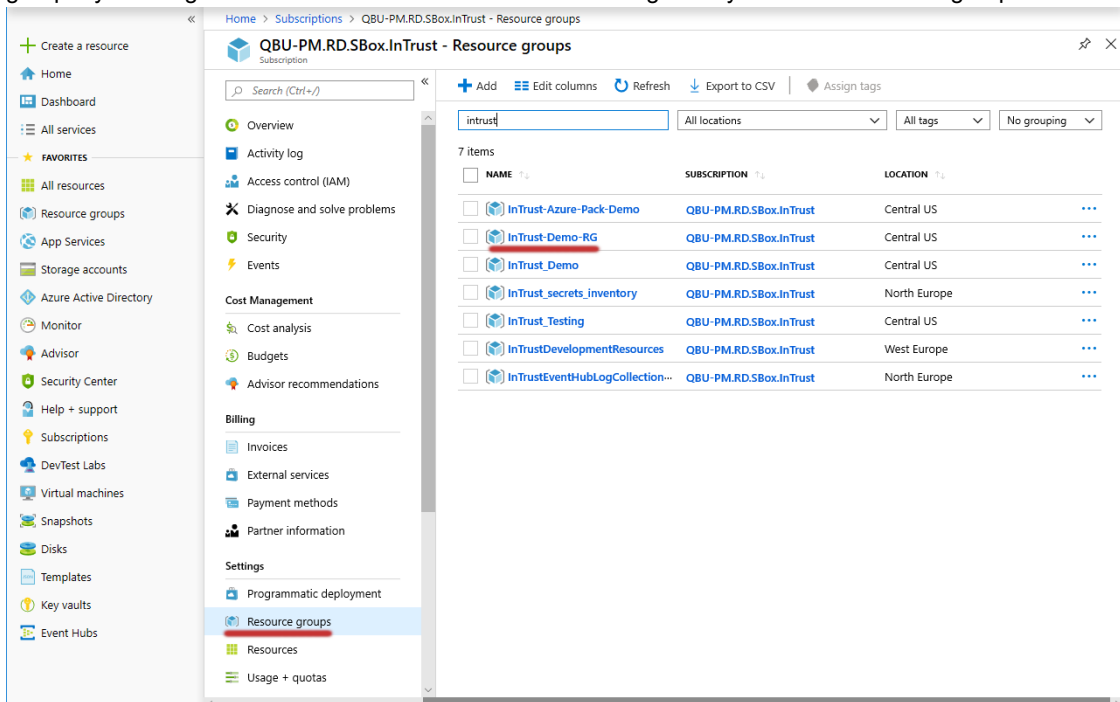
To register an application with a subscription

- In the Favorites list, switch to the **Subscriptions** service and select the subscription you need.

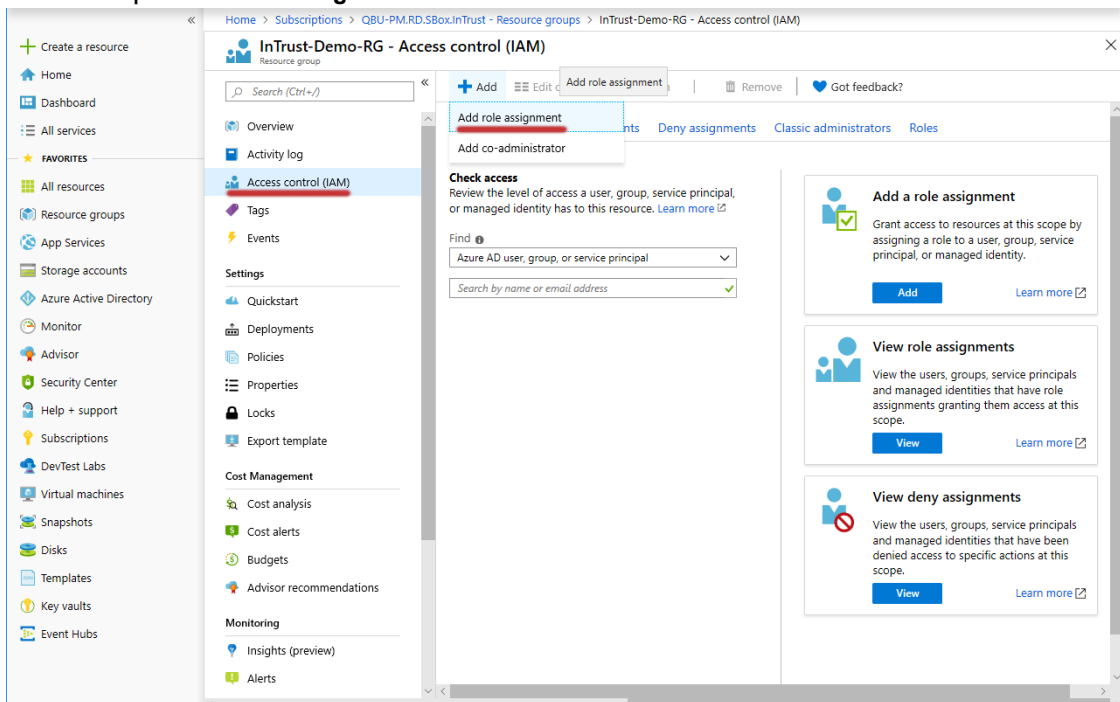


- In the menu pane, click **Resource groups**.

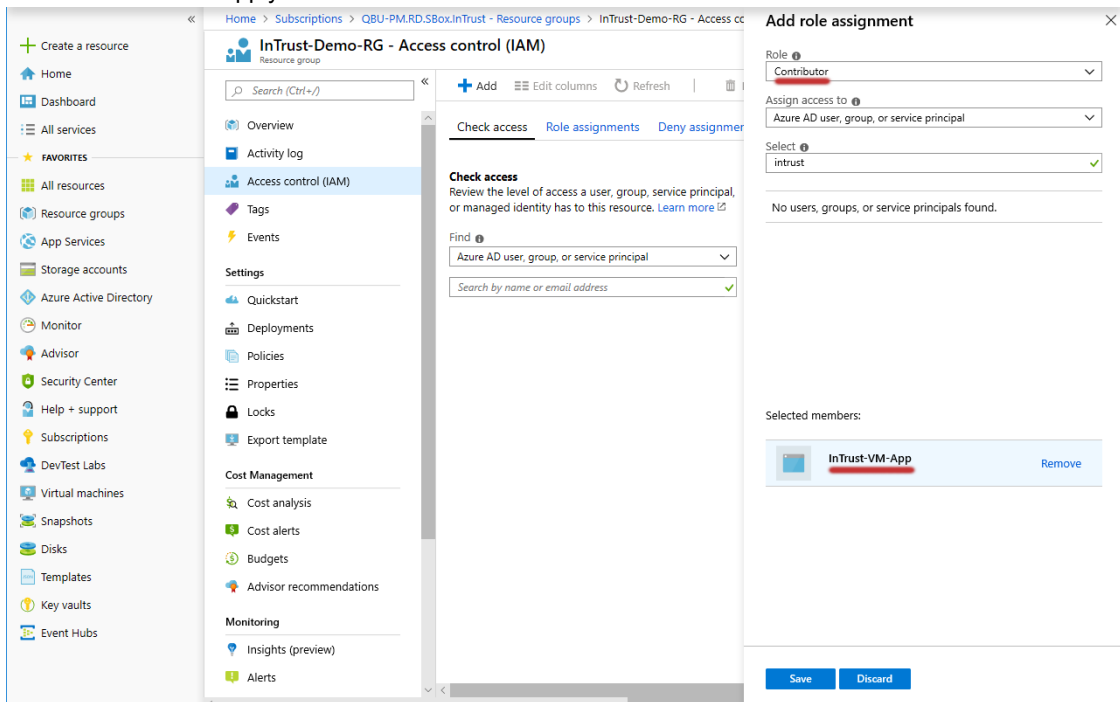
3. Select the resource group you need from the list that is displayed, or create a new resource group by clicking **Add**. You can leave the default settings for your new resource group.



4. In the menu pane for the resource group, click **Access control (IAM)**.
5. Click **Add | Add Role Assignment**.



- Under **Add Role Assignment**, find the necessary application, select the **Contributor** role for it and click **Save** to apply it.



- Likewise, add the **Virtual Machine Contributor** role to the same application.

Look Up the Subscription ID

- In the Favorites list, click **Subscriptions**.
- In the list of subscriptions that opens, locate the subscription you need.

- Copy the value in the **Subscription ID** column of the table and save it for later use.

The screenshot displays the Azure portal interface for a subscription. The left sidebar shows navigation options, with 'Subscriptions' highlighted. The main content area shows the details for the subscription 'QBU-PM.RD.SBox.InTrust'. The 'Subscription ID' is highlighted in red. Below the details is a 'Costs by resource' donut chart showing the following breakdown:

Resource	Cost (USD)
InTrust-agent	51.77
demoaagent1	44.50
Microsoftspace	36.54
Others	1,308.81

Look Up the Storage Account Connection String

- In the Favorites list, click **Storage accounts**.

The screenshot displays the Azure portal interface for the 'Storage accounts' page. The left sidebar shows navigation options, with 'Storage accounts' highlighted. The main content area shows a table of storage accounts with columns for Name, Type, Kind, Resource Group, Location, and Subscription. Two storage accounts are listed:

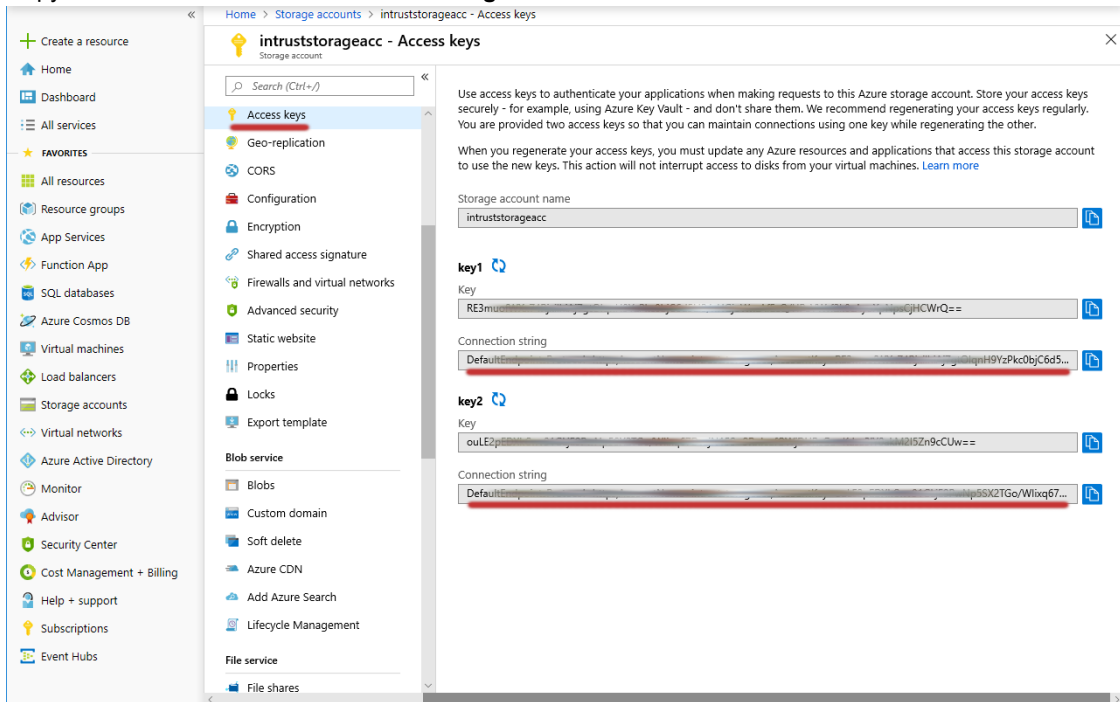
NAME	TYPE	KIND	RESOURCE GROUP	LOCATION	SUBSCRIPTION
intruststorageacc	Storage account	StorageV2	InTrust_Demo	Central US	QBU-PM.RD.SBox.InTr...
testintruststorageacc	Storage account	StorageV2	InTrust_Testing	Central US	QBU-PM.RD.SBox.InTr...

2. In the list of storage accounts that appears, select the one you need. Choose an account where:
 - **Resource group** is set to the resource group you need.
 - **Account kind** is set to an appropriate option:
 - For virtual machine auditing, select a kind that supports both blob storage and file storage; for example, **StorageV2 (general purpose v2)**.
 - For event hub auditing, it is sufficient to use a kind that supports only blob storage.

If such an account does not exist, create it by clicking **Add**.

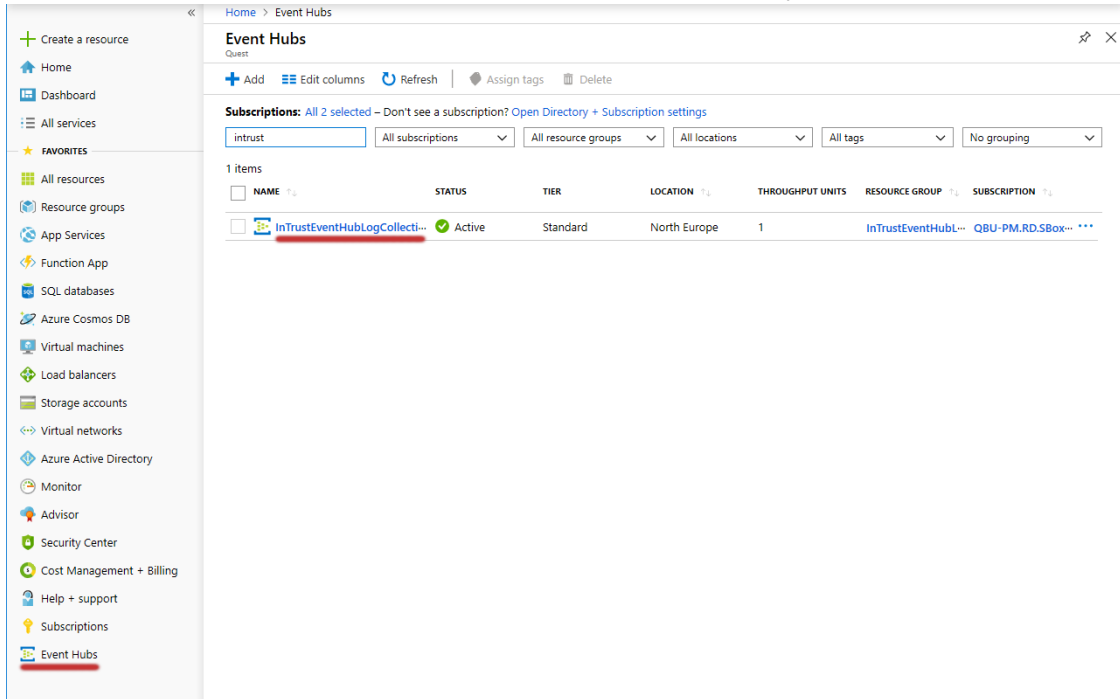
The screenshot shows the 'Create storage account' wizard in the Azure portal. The left sidebar contains navigation options like 'Home', 'Dashboard', 'All services', and 'FAVORITES'. The main content area is titled 'Create storage account' and has tabs for 'Basics', 'Networking', 'Advanced', 'Tags', and 'Review + create'. The 'Project details' section includes a description of Azure Storage and fields for 'Subscription' (QBU-PM.RD.SBox.InTrust) and 'Resource group' (InTrust-Azure-Pack-Demo). The 'Instance details' section includes a description of the deployment model and fields for 'Storage account name', 'Location' ((US) East US), 'Performance' (Standard), 'Account kind' (StorageV2 (general purpose v2)), 'Replication' (Read-access geo-redundant storage (RA-GRS)), and 'Access tier' (Hot). At the bottom, there are buttons for 'Review + create', '< Previous', and 'Next: Networking >'.

3. In the menu pane for the specified storage account, switch to **Access keys**.
4. Copy the values in the **Connection string** text boxes and save them for later use.



Look Up the Event Hub Connection Strings and Consumer Group

1. In the Favorites list, click **Event Hubs**.
2. In the list of event hubs namespaces that appears, select the one you need.



3. In the menu pane for the specified event hubs namespace, click **Event Hubs** (under **Entities**).

4. In the list of event hubs that appears, select the one you need.

[Home](#) > [Event Hubs](#) >

InTrustEventHubLogCollectionNS | Event Hubs

Event Hubs Namespace

Name	Status	Message Retention	Partition Count
insights-activity-logs	Active	7 days	4

5. In the menu pane for the specified event hub, switch to **Shared access policies**.
6. In the list of policies that appears, select the one you need. The properties of the policy are displayed.
7. Copy the values in the **Connection string–primary key** and **Connection string–secondary key** text boxes and save them for later use.
8. In the menu pane, switch to **Consumer groups** (under **Entities**).

9. Copy the name of the consumer group you need and save it for later use.

[Home](#) > [Event Hubs](#) > [InTrustEventHubLogCollectionNS | Event Hubs](#) >

insights-activity-logs (InTrustEventHubLogCollectionNS/insights-activity-logs) | Consumer g... ×
Event Hubs Instance

Search (Ctrl+/) << + Consumer group Delete Refresh

Overview
Access control (IAM)
Diagnose and solve problems

Settings

- Shared access policies
- Properties
- Locks
- Export template

Entities

- Consumer groups

Features

- Capture
- Process data

Support + troubleshooting

- New support request

Search to filter items... ×

Name	Location
\$Default	North Europe
preview_data_consumer_group	North Europe

Collecting Events from Azure Virtual Machines

Working with Azure virtual machine collections is similar to working with regular Windows collections, except that an Azure collection has additional settings for communication between Azure and the on-premises InTrust server.

In InTrust Deployment Manager, go to the Collections tab, click **New** and select **Azure Collection**.

On the Azure Virtual Machine Settings step, supply the Azure-specific configuration options:

- Resource group name
- Tenant ID
- Application ID
- Application key
- Subscription ID
- Connection string used by the storage account
If you are collecting events both from virtual machines and from event hubs, it is recommended that you have separate storage accounts for each purpose. For virtual machine auditing, use a storage account that supports file storage.

If you don't know where to get any of these items, see [Providing Access to Your Azure Environment](#).

i **TIP:** It is recommended that you create a dedicated application and resource group in your Azure subscription specifically for auditing purposes. This will give you better scalability and ensure problem-free coexistence with other Azure services. You will also be able to track and troubleshoot resource usage in a more precise way.

The remaining steps are the same as for regular Windows collections.

Azure Collection Specifics

- Only one Azure collection is allowed per InTrust organization.
- You cannot manually edit the membership of an Azure collection. It is populated automatically based on the contents of the Azure resource group that it is associated with. To collect from the right virtual machines, make sure you select the right resource group.

Collecting Events from Azure Event Hubs

Azure log (Event Hub) collections let you gather events that Azure objects direct to event hubs, including diagnostic events, activity logs and metrics.

To stream Activity log events to an event hub

1. In the Azure portal, navigate to **Monitor| Activity log**.
2. Select **Diagnostic Settings** and click **Add diagnostic setting**.
3. Under **Category details**, select the kinds of events that you want to export.
4. Under **Destination details**, select **Stream to an event hub**.
5. Select your subscription and namespace for the event hub.
6. Specify the **Event hub name** or leave it blank. If you omit it, Azure will use the predefined name "insights-activity-logs".
7. Select **RootManagedSharedAccessKey** as the policy.
8. Save the changes.

To create an Azure log (Event Hub) collection

In InTrust Deployment Manager, go to the Collections tab, click **New** and select **Azure log (Event Hub) Collection**. On the Specify Azure Subscriptions step, click **Add** and specify the event hub that you need. Supply the following options:

- **Event hub name**
This is either the name of the particular event hub, which you can look up in the Azure portal. Some event hub names are predefined. For example, if you need the event hub with Azure Activity log events, supply the name of an event hub to which the Activity log is streamed. However, you should first make sure that the event hub really exists in the correct event hubs namespace.
For details about setting up redirection of events to event hubs, see [Stream Azure monitoring data to an event hub](#). For details about Activity log events, see [To stream Activity log events to an event hub](#) above.
- **Consumer group name**
You should create a separate consumer group specifically for event hub auditing in advance.
- **Event hub connection strings**
- **Storage connection strings**
If you are collecting events both from virtual machines and from event hubs, it is recommended that you have separate storage accounts for each purpose. For event hub auditing, it is sufficient to use a storage account that supports only blob storage.

If you don't know where to get any of these items, see [Providing Access to Your Azure Environment](#) above.

i **TIP:** It is recommended that you create a dedicated event hub and consumer group in your Azure subscription specifically for auditing purposes. This will give you better scalability and ensure problem-free coexistence with other Azure services. You will also be able to track and troubleshoot resource usage in a more precise way.

The remaining steps are the same as for regular Windows collections.

Azure Log (Event Hub) Collection Specifics

- The members of an Azure log (Event Hub) collection are Azure event hubs not computers. You can have multiple Events Hubs in a single collection.
- Only one preselected non-editable "Azure Log" data source can be associated with this type of collection.
- If you collect Activity log events from an event hub, the scope of those events is the entire Azure subscription. If you are interested in just the resource group you are auditing with your Azure collection, be prepared to get Activity log events for a lot more than that.
- Due to the way these collections work, InTrust Deployment Manager may temporarily show valid errors about network connectivity that may have already been resolved. If such an error doesn't go away after a few minutes, you should investigate the situation, but you don't necessarily have to take immediate action as soon as you see the error.

Analyzing Azure Events

After you have made sure that InTrust collects data from Azure, use InTrust Repository Viewer to connect to the repository that stores the events and view them.

Events from Windows virtual machines in Azure are no different from on-premises Windows events, and all of your familiar Repository Viewer searches are compatible with them.

For events that originate in Azure rather than on Azure-hosted virtual machines, the Azure Knowledge Pack provides the following predefined Repository Viewer searches:

- All activity and diagnostic events
- All administrative events (RBAC changes) by who, what
- Key vault activity
- Resource-level events by subscription ID, resource group, provider
- Resource-level events by who, what, where
- SQL activity
- Tenant-level events by tenant ID, provider
- Tenant-level events by who, what, where

Use these searches directly or make customized copies of them to suit your needs.

Known Issues

The following issues are known at the time of the Azure Knowledge Pack technical preview for InTrust 11.4.1.

Table 1: Azure Knowledge Pack installation known issues

Known Issue	Issue ID
<p>The Azure Knowledge Pack technical preview is compatible only with the released version of InTrust 11.4.1 and incompatible with Update 1 for this version. You should be aware of the following related caveats:</p> <ul style="list-style-type: none">Do not install the Azure Knowledge Pack on servers where InTrust 11.4.1 Update 1 is applied.Do not apply InTrust 11.4.1 Update 1 on servers where the Azure Knowledge Pack is deployed.	IN-11509, IN-11611, IN-11513
<p>After you uninstall the Azure Knowledge Pack technical preview, some folders related to it may be left behind on disk.</p>	IN-9995
<p>During Azure Knowledge Pack technical preview installation, you may be taken to the Files in Use step, where the list of applications contains items you don't expect to interfere with the installation.</p>	IN-10408

Table 2: Azure Knowledge Pack general known issues

Known Issue	Issue ID
<p>The Azure Knowledge Pack technical preview supports only configurations with one resource group and one storage account per deployment. If you want to audit multiple resource groups, you need multiple deployments, each with its own resource group and storage account.</p>	IN-8943
<p>After you uninstall the InTrust agent from an Azure VM that is in a collection, InTrust Deployment Manager still shows the VM in the collection.</p>	IN-9073
<p>If you delete a VM from an Azure resource group that an Azure VM collection is associated with, you may get a temporary error message like the following in InTrust Deployment Manager:</p> <pre>Object reference not set to an instance of an object.</pre> <p>The error message goes away after a few minutes.</p>	IN-10514
<p>InTrust Deployment Manager versions released before the Azure Knowledge Pack don't hide Azure VM collections and don't disallow editing them. However, if you modify an Azure VM collection in an old InTrust Deployment Manager console, this causes the InTrust configuration to become invalid.</p> <p>If you use the Azure Knowledge Pack, make sure all instances of InTrust Deployment Manager are upgraded to a version that fully supports Azure VM collections.</p>	IN-10404
<p>InTrust Deployment Manager shows Azure VMs in collections even after agents have been uninstalled from the VMs.</p>	IN-8681

Known Issue	Issue ID
InTrust Manager doesn't show agents that are deployed on Azure VMs, which are available in InTrust Deployment Manager.	IN-10471
Agent installation fails for Azure VMs whose names contain non-ASCII characters, preventing real-time collection from such VMs.	IN-10011
When the agent is installed on an Azure VM, the AgentInstallDateTime VM tag specifies the wrong timezone. The tags says GMT instead of the local timezone.	IN-9377
After you delete an Azure VM collection, the configuration folder related to this collection is not deleted on the local file systems of the VMs from that collection.	IN-10330
When you manually uninstall the InTrust agent from an Azure VM, the accompanying Azure Proxy service is not automatically stopped and uninstalled.	IN-10231
InTrust fault-tolerance features are not supported for the Azure Knowledge Pack. The failover scenario doesn't work correctly for Azure VM collections audited by the Azure Knowledge Pack.	IN-10410
Changing the destination repository for a collection of Azure VMs causes the reconfiguration of the Azure Proxy service on the VMs. Events that occur during the reconfiguration are not collected.	IN-10449
Organization parameters are applied on agents on Azure VMs only after the reconfiguration of the Azure Proxy service, which happens after a collection is modified in InTrust Deployment Manager. On regular computers, they are applied almost immediately.	IN-10450
In some situations, an Azure VM in a collection may report a "Collecting" state even though the InTrust agent has stopped working on that VM. To check if the agent is functioning properly, see the last gathering time for it.	IN-10453
When you create an Azure collection, the items are configured one by one. Depending on the number of VMs, the collection configuration may take a long time.	IN-10478

Quest creates software solutions that make the benefits of new technology real in an increasingly complex IT landscape. From database and systems management, to Active Directory and Office 365 management, and cyber security resilience, Quest helps customers solve their next IT challenge now. Around the globe, more than 130,000 companies and 95% of the Fortune 500 count on Quest to deliver proactive management and monitoring for the next enterprise initiative, find the next solution for complex Microsoft challenges and stay ahead of the next threat. Quest Software. Where next meets now. For more information, visit www.quest.com.

Contacting Quest

For sales or other inquiries, visit www.quest.com/contact.

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