

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	
Get Your Shortcuts Handy	7
Look Up the Tenant ID, Application ID and Application Key	
Look Up the Storage Account Connection String	
Look Up the Event Hub Connection Strings and Consumer Group	
Collecting Events from Azure Virtual Machines	
Azure Collection Specifics	20
Collecting Events from Azure Event Hubs	
Azure Log (Event Hub) Collection Specifics	22
Analyzing Azure Events	
Known Issues	
About us	
Contacting Quest	
Technical support resources	

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.
- **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.

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.

Create a resource	All services 👂 event	×	
A Home	Everything	Event Hubs	*
i≣ All services	Compute	🕖 Event Grid Domains	*
All resources	Networking	🧟 Event Grid Subscriptions	*
Resource groups	Storage Web	Event Grid Topics	*
S App Services	Mobile	Event Hubs Clusters	*
SQL databases	Containers Databases	(Å) Management groups	*
Azure Cosmos DB Virtual machines	Analytics	∃ Time Series Insights event sources	*
Load balancers	AI + machine learning Internet of things	API Management services	*
Storage accounts ··· Virtual networks	Mixed reality	Cost Management + Billing	*
Azure Active Directory	Integration Identity	Monitor	*
🍽 Monitor 🐢 Advisor	Security	Keywords: events Identity Governance Keywords: Entitlement management	*
Security Center	Migrate	Azure AD Risk detections Keywords: Risk events	*
Help + support	Management + governance	Automation Accounts Keywords: inventory	*
Subscriptions	Other		
Event Hubs			

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.

**	Home > Quest - App registrations			
Create a resource	Quest - App registrations			\$ ×
🛧 Home	«	- New registration	Troubleshooting	
💷 Dashboard	D Search (Ctrl+/)		in a second second	
E All services	Overview	Welcome to the new and improved App	registrations (now Generally Available). See what's new	→
+ FAVORITES	💣 Getting started	Looking to learn how it's changed fro	m App registrations (Legacy)? Learn more	
All resources	Manage	sui want to use App registrations (Le	gacy)r Go back and tell us why	
🐑 Resource groups	🛓 Users	All applications Owned applications		
🔇 App Services	🚰 Groups	,∽ intrust		×
🦘 Function App	Organizational relationships	DISPLAY NAME	APPLICATION (CLIENT) ID CREATED ON	CERTIFICATES & SECRETS
👼 SQL databases	Roles and administrators			
🖉 Azure Cosmos DB	Enterprise applications	IN InTrust-App-For-Tests	670f5aaa-fd56-405c-ba 6/5/2019	🥝 Current
Virtual machines	Devices	IN InTrust-App-Test	bdc652b7-77b7-4cc1-8 8/6/2019	Current
🚸 Load balancers	App registrations	IN InTrust-VM-App	ea1e0359-8adb-41dd-a 2/28/2019	🔮 Current
Storage accounts	Identity Governance			
↔ Virtual networks	Application proxy			
Azure Active Directory	🔓 Licenses			
Monitor	Azure AD Connect			
🌪 Advisor	🕫 Custom domain names			
Security Center	Ø Mobility (MDM and MAM)			
💿 Cost Management + Billing	Password reset			
🚰 Help + support	Tompany branding			
📍 Subscriptions	User settings			
🗈 Event Hubs	H Properties			
	💄 Notifications settings 🗸			

- 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.

5. 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.

**	Home > Quest - App registrations > InTr	ust-VM-App			
+ Create a resource	InTrust-VM-App			Ŷ	\times
🛧 Home	«	n Delete A Endpoints			
🗔 Dashboard)> Search (Ctrl+/)				
E All services	III Overview	Welcome to the new and improved App registrations. Looking to	e learn how it's changed from App registrations (Legacy)? $ ightarrow$		
+ FAVORITES	📣 Quickstart	Display name InTrust-VM-App	Supported account types My organization only		Â
All resources	Manage	Application (client) ID	Redirect URIs Add a Redirect URI		
(🐑 Resource groups	📼 Branding	Directory (tenant) ID	Application ID URI		
🔇 App Services	Authentication	910-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-0-	http://InTrust-VM-App		
🦘 Function App	Certificates & secrets	Object ID 7a	Managed application in local directory InTrust-VM-App		
👼 SQL databases	-> API permissions	*			- 1
🖉 Azure Cosmos DB	Expose an API	Call APIs	Documentation		
Virtual machines	Owners		Microsoft identity platform		
4 Load balancers	Roles and administrators (Previ		Authentication libraries		
Storage accounts	0 Manifest		Code samples		
< inv line works	Support + Troubleshooting		Glossary		
Azure Active Directory	X Troubleshooting	Build more powerful apps with rich user and business data from Microsoft services and your own company's data	Help and support		
Monitor	New support request	sources.			
🌪 Advisor		View API Permissions			
Security Center					
Oost Management + Billing		Sign in users in 5 minutes			
Help + support		ris AB 49 11 🛋 AB 11 49			
Subscriptions					
🗈 Event Hubs		Use our SDKs to sign in users and call APIs in a few steps			
		View all quickstart guides			~
	1				100

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

*	Home > Quest - App registrations > InTru	ust-VM-App - Certificates & secrets					
- Create a resource	🔶 InTrust-VM-App - Certifica	ates & secrets				Ŷ	\times
A Home	«						
Dashboard	, Search (Ctrl+/)	Add a client secret					
E All services	Overview	Description					
* FAVORITES	📣 Quickstart						
All resources	Manage	Expires					
(🐑 Resource groups	🔤 Branding	In 2 years					
🔇 App Services	Authentication	 Never 					
Storage accounts	Certificates & secrets						
Azure Active Directory	→ API permissions	Add Cancel					
Monitor	Expose an API	THUMBPRINT	START DATE	EXPIRES			
🌪 Advisor	• Owners						
Security Center	Roles and administrators (Previ	Client secrets					
🚰 Help + support	Manifest	A secret string that the application uses t	o prove its identity w	hen requesting a token. Also can be referr	ed to as applicatior	1	
📍 Subscriptions	Support + Troubleshooting	password.					
🝨 DevTest Labs		+ New client secret					
Virtual machines	New support request	DESCRIPTION	EXPIRES	VALUE			
選 Snapshots		Demo password	2/28/2020	••}***************		Ŵ	
😁 Disks							
iemplates							
(†) Key vaults							
📴 Event Hubs							
	6						

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

«	Home > Quest - App registrations > InTr	ust-VM-App - Certificates & secrets				
+ Create a resource	🔶 InTrust-VM-App - Certific	ates & secrets			\$	×
+ Home	,> Search (Ctrl+/) «	Copy the new client secret value. You	won't be able to retrie	ve it after you perform another operation or leave t	his blade.	
All services FAVORITES	 Øverview Quickstart 	Credentials enable applications to identi location (using an HTTPS scheme). For a as a credential.	fy themselves to the higher level of assur	authentication service when receiving tokens a ance, we recommend using a certificate (instea	t a web addressable d of a client secret)	
All resources Resource groups App Services	Manage Branding Authentication	Certificates Certificates can be used as secrets to pro keys.	we the application's	identity when requesting a token. Also can be r	referred to as public	
Storage accounts	P Certificates & secrets	→ Upload certificate				
Azure Active Directory	- API permissions	No certificates have been added for this	application.			
Monitor	Expose an API					
🜪 Advisor	0wners	THUMBPRINT	START DAT	E EXPIRES		
Security Center	Roles and administrators (Previ					
Help + support	Manifest	Client secrets				
Subscriptions	Support + Troubleshooting	A secret string that the application uses	to prove its identity (when requesting a token. Also can be referred t	to as application	
nevTest Labs	X Troubleshooting	password.				
Virtual machines	New support request	+ New client secret				
選 Snapshots		DESCRIPTION	EXPIRES	VALUE		
🝔 Disks		Demo password	2/28/2020	···}**********************************	Copy to clipboard	
iemplates		Password uploaded on Mon Sep 30	12/31/2299	VK6BvNBYK4XNGhc8CA5.aTKuFErdI[
(*) Key vaults						
📴 Event Hubs						

To register an application with a subscription

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

*	Home > Subscriptions			
Create a resource	Subscriptions Do	ocumentation 🛛	Ż	\times
🛧 Home				
🗔 Dashboard				
E All services	Showing subscriptions in Quest. Don't see a subscription? Switch directories My role Status			
+ FAVORITES	8 selected V 3 selected		\sim]
All resources	Apply			
(🐑 Resource groups	Show only subscriptions selected in the global subscriptions filter 🛛			
🔇 App Services	\wp Search to filter items			
Function App	SUBSCRIPTION NAME 12 SUBSCRIPTION ID 12 MY ROLE 12 CURRENT COST STATUS			
👼 SQL databases	2 QBU-PM.RD.SBox.InTrust damaged and a contributor Contributor	ve		
🖉 Azure Cosmos DB	OBU-PM.RD.SBox.ITSearch	ve		
Virtual machines				
💠 Load balancers				
General Storage accounts				
 Virtual networks 				
🚸 Azure Active Directory				
Monitor				
🜪 Advisor				
Security Center				
📀 Cost Management + Billing				
Help + support				
Subscriptions				
Event Hubs				

2. 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).





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



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

Look Up the Subscription ID

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

13



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

Look Up the Storage Account Connection String

1. In the Favorites list, click Storage accounts.

Home > Storage accounts	
+ Create a resource Storage accounts	\$ ×
A Home Add == Erlit columns C Befrech Action tars	
Dashboard	
∃ All services Subscriptions: All 2 selected – Don't see a subscription? Open Directory + Subscription settings	
★ FAVORITES All tags ✓ All tags ✓ No groups	ing 🗸
All resources 2 items	
NAME to TYPE to KIND to RESOURCE GROUP to LOCATION to SUBSCRIPTION SUBSCRIPTION	
🐼 App Services Storage account StorageV2 InTrust_Demo Central US QBU-PM.RD	SBox.InTr··· ···
Function App Description App Desc	SBox.InTr··· ***
🐻 SQL databases	
2 Azure Cosmos DB	
👰 Virtual machines	
💠 Load balancers	
Storage accounts	
Virtual networks	
♦ Azure Active Directory	
(Monitor	
🜪 Advisor	
Security Center	
📀 Cost Management + Billing	
Belp + support	
Ŷ Subscriptions	
E Event Hubs	

- 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.

**	Home > Storage accounts > Create stora	age account						
+ Create a resource	Create storage account		×					
🛧 Home								
Dashboard	Basics Networking Advanced	Tags Review + create						
All services	Azure Storage is a Microsoft-managed serv	vice providing cloud storage that is highly available, secure, durable, scalable, and						
+ FAVORITES	redundant. Azure Storage includes Azure B	lundant. Azure Storage includes Azure Blobs (objects), Azure Data Lake Storage Gen2, Azure Files, Azure Queues, and Azure						
All resources	lables. The cost of your storage account de	epends on the usage and the options you choose below. Learn more						
	Project details							
(iii) Resource groups	Select the subscription to manage deploye	d resources and costs. Use resource groups like folders to organize and manage all						
🔇 App Services	your resources.							
Function App	* Subscription	QBU-PM.RD.SBox.InTrust						
🧟 SQL databases	* Resource group	InTrust-Azure-Pack-Demo						
🖉 Azure Cosmos DB		Create new						
Virtual machines	Instance details							
💠 Load balancers	The default deployment model is Resource	Manager, which supports the latest Azure features. You may choose to deploy using						
🧮 Storage accounts	the classic deployment model instead. Ch	oose classic deployment model						
Virtual networks	* Storage account name 🚯							
Azure Active Directory	* Location	(US) East US						
Monitor	Performance 👩	Standard Premium						
🌪 Advisor								
Security Center	Account kind	StorageV2 (general purpose v2)						
Oost Management + Billing	Replication 👩	Read-access geo-redundant storage (RA-GRS)						
Help + support	Access tier (default) 🕦	Cool 🖲 Hot						
💡 Subscriptions								
Event Hubs	Review + create < Pre	vious 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.

*	Home > Event Hubs							
+ Create a resource	Event Hubs							×
A Home	+ Add EE Edit columns	🕐 Refresh 🛛 🌒 Assigr	tags 💼 Delete					
🛄 Dashboard	-	Death see a subscription?	Directory I Subse	intion anttinue				
E All services	Subscriptions: All 2 selected	- Don't see a subscription? C	pen Directory + subsc	npuon setungs			N	
+ FAVORITES	Intrust	All subscriptions	All resource groups	 All locations 		gs 🗸	ivo grouping	
All resources	1 items							
(🐑 Resource groups	NAME 13	STATUS	TIER	LOCATION 1	THROUGHPUT UNITS	RESOURCE GROUP 1	SUBSCRIPTION 1	
🔇 App Services	InTrustEventHubLo	ogCollecti 🕑 Active	Standard	North Europe	1	InTrustEventHubL…	QBU-PM.RD.SBox…	
🦘 Function App								
👼 SQL databases								
🖉 Azure Cosmos DB								
Virtual machines								
4 Load balancers								
Storage accounts								
Virtual networks								
Azure Active Directory								
Monitor								
🌪 Advisor								
Security Center								
📀 Cost Management + Billing								
Help + support								
Subscriptions								
Event Hubs								

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 >

Evenerious Namespace					
	«	+ Event Hub 🖔 Refre	sh		
E Overview	^				
Activity log		- insignes-activity			
Access control (IAM)		Name	Status	Message Retention	Partition Count
Tags		insights-activity-logs	Active	7 days	4
Diagnose and solve problems					
🗲 Events					
Settings					
Shared access policies					
🗹 <u>Scale</u>					
Geo-Recovery					
🜮 <u>Networking</u>					
<u>Encryption</u>					
Properties					
A Locks					
Export template					
Entities					
Event Hubs					

InTrustEventHubLogCollectionNS | Event Hubs

- 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. <u>Home > Event Hubs > InTrustEventHubLogCollectionNS | Event Hubs</u> >

🛜 insights-activity-logs (InTrustEventHubLogCollectionNS/insights-activity-logs) | Consumer g... 🛛 🗡 + Consumer group 📋 Delete 🖒 Refresh ₽ Search (Ctrl+) ~ E Overview Search to filter items. ٦× R Access control (IAM) Name Location Diagnose and solve problems North Europe \$Default Settings preview_data_consumer_group North Europe Shared access policies **Properties** A Locks 🖳 Export template Entities Consumer groups Features Capture 🥬 Process data Support + troubleshooting R New support request

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.

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 "insightsactivity-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.

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
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:	IN-11509, IN-11611, IN-11513
 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. 	
After you uninstall the Azure Knowledge Pack technical preview, some folders related to it may be left behind on disk.	IN-9995
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.	IN-10408

Table 2: Azure Knowledge Pack general known issues

Known Issue	Issue ID
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.	IN-8943
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.	IN-9073
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:	IN-10514
Object reference not set to an instance of an object.	
The error message goes away after a few minutes.	
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.	IN-10404
are upgraded to a version that fully supports Azure VM collections.	
InTrust Deployment Manager shows Azure VMs in collections even after agents have been uninstalled from the VMs.	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