Tanium™ Interact User Guide

Version 2.15.112

July 10, 2023

The information in this document is subject to change without notice. Further, the information provided in this document is provided "as is" and is believed to be accurate, but is presented without any warranty of any kind, express or implied, except as provided in Tanium's customer sales terms and conditions. Unless so otherwise provided, Tanium assumes no liability whatsoever, and in no event shall Tanium or its suppliers be liable for any indirect, special, consequential, or incidental damages, including without limitation, lost profits or loss or damage to data arising out of the use or inability to use this document, even if Tanium Inc. has been advised of the possibility of such damages.

Any IP addresses used in this document are not intended to be actual addresses. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual IP addresses in illustrative content is unintentional and coincidental.

Please visit https://docs.tanium.com for the most current Tanium product documentation.

This documentation may provide access to or information about content, products (including hardware and software), and services provided by third parties ("Third Party Items"). With respect to such Third Party Items, Tanium Inc. and its affiliates (i) are not responsible for such items, and expressly disclaim all warranties and liability of any kind related to such Third Party Items and (ii) will not be responsible for any loss, costs, or damages incurred due to your access to or use of such Third Party Items unless expressly set forth otherwise in an applicable agreement between you and Tanium.

Further, this documentation does not require or contemplate the use of or combination with Tanium products with any particular Third Party Items and neither Tanium nor its affiliates shall have any responsibility for any infringement of intellectual property rights caused by any such combination. You, and not Tanium, are responsible for determining that any combination of Third Party Items with Tanium products is appropriate and will not cause infringement of any third party intellectual property rights.

Tanium is committed to the highest accessibility standards for our products. To date, Tanium has focused on compliance with U.S. Federal regulations - specifically Section 508 of the Rehabilitation Act of 1998. Tanium has conducted 3rd party accessibility assessments over the course of product development for many years and has most recently completed certification against the WCAG 2.1 / VPAT 2.3 standards for all major product modules in summer 2021. In the recent testing the Tanium Console UI achieved supports or partially supports for all applicable WCAG 2.1 criteria. Tanium can make available any VPAT reports on a module-by-module basis as part of a larger solution planning process for any customer or prospect.

As new products and features are continuously delivered, Tanium will conduct testing to identify potential gaps in compliance with accessibility guidelines. Tanium is committed to making best efforts to address any gaps quickly, as is feasible, given the severity of the issue and scope of the changes. These objectives are factored into the ongoing delivery schedule of features and releases with our existing resources.

Tanium welcomes customer input on making solutions accessible based on your Tanium modules and assistive technology requirements. Accessibility requirements are important to the Tanium customer community and we are committed to prioritizing these compliance efforts as part of our overall product roadmap. Tanium maintains transparency on our progress and milestones and welcomes any further questions or discussion around this work. Contact your sales representative, email Tanium Support at support@tanium.com, or email accessibility@tanium.com to make further inquiries.

Table of contents

Interact overview

Use Tanium Interact to issue questions to managed endpoints, analyze their answers, and deploy actions to the endpoints based on the answers. Although it is licensed as part of the Tanium Core Platform, Interact is a Tanium module, so you can update it separately from Tanium Console and the Tanium Server.

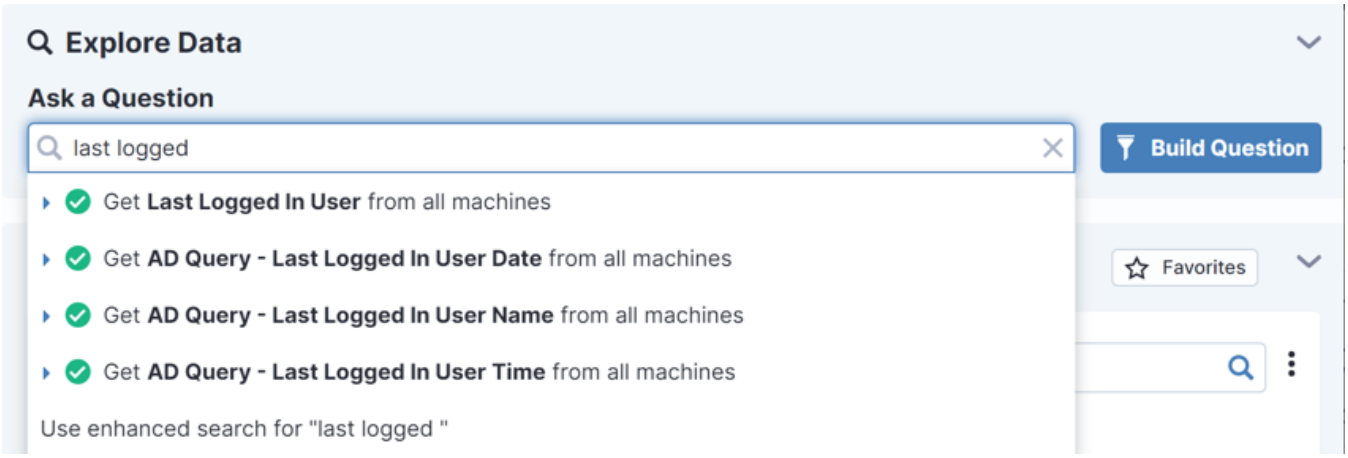
What is a question?

A Tanium *question* is a query that you issue from the Tanium Server to managed endpoints. A dynamic question is one that you create and issue through the **Ask a Question** or **Question Builder** features in Interact. A saved question is a configuration object that enables you to reissue a question without reconstructing it through those features.

The **Ask a Question** feature is built on a natural language parser that enables you to get started with natural questions rather than a specialized query language. You do not need to enter questions as complete sentences or particularly well-formed inquiries. Word forms are not case sensitive and can even include misspellings. The parser interprets your input and suggests a number of valid queries that you can use to formalize the question that is sent to Tanium Clients. Interact provides the **Ask a Question** feature as a field at the top of the Interact **Overview** page and the Tanium **Home** page. For details, see Issue a question through the Ask a Question field.

The following figure shows an example of how Interact uses the natural language parser to propose valid queries based on user input. First, the user enters the fragment `last logged in user` and clicks **Search**. In response, Interact returns a list of queries cast in valid syntax.

Figure 1: Natural language parser



Questions have a `get` clause that specifies the information to retrieve and a `from` clause that specifies the target endpoints. Basic questions include the following:

- One or more sensor names (such as `Last Logged In User`) in the get clause
- `From all machines` (all endpoints that host the Tanium Client) in the from clause

Advanced questions include reserved words or characters (such as `match` or `$`), regular expressions, filter clauses, the `in` operator, or advanced options.

For the steps to issue questions and view question history, see Asking questions and searching endpoints on page 41. For more information about question syntax, see Reference: Example questions on page 91 and Reference: Advanced question syntax on page 95.

What is a sensor?

A *sensor* is a script that runs on an endpoint to compute a response to a Tanium question. The Tanium Server distributes sensors to endpoints during Tanium Client registration. Sensors enable you to ask questions that collect information such as the following:

- Hardware and software inventory and configuration
- Running applications and processes
- Files and directories
- Network connections

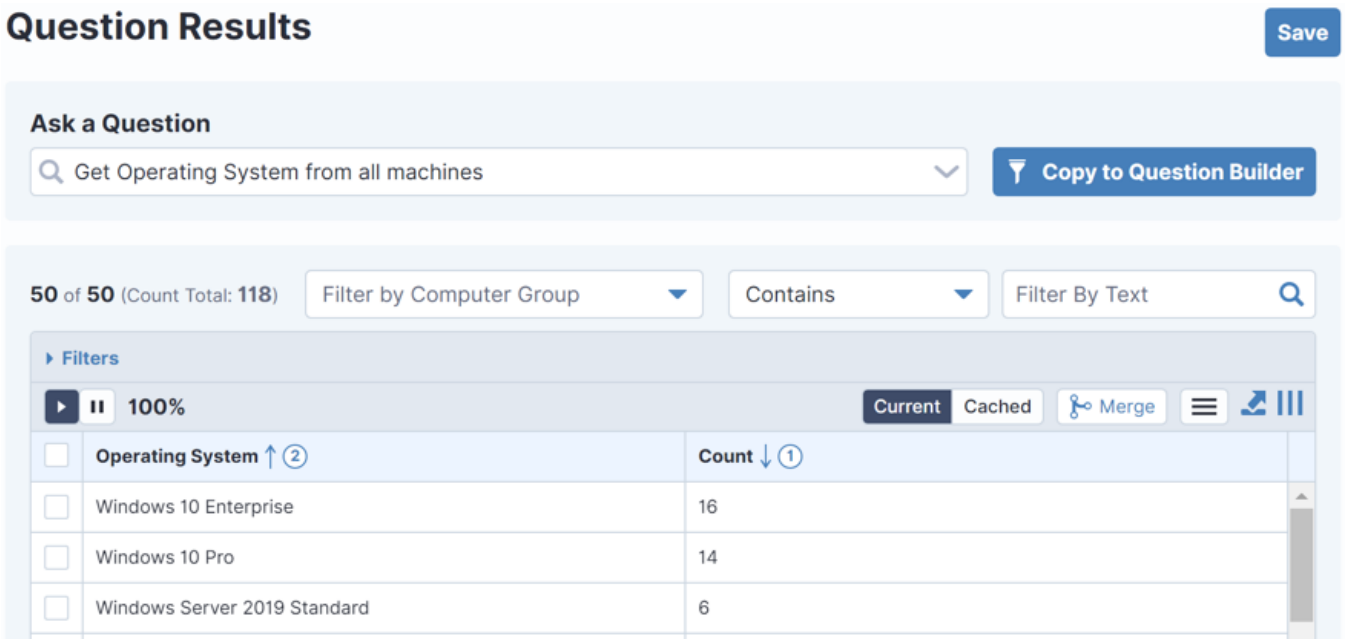
The Tanium Server automatically imports initial content that includes sensors for a wide range of common questions (see Tanium Console User Guide: Initial content). Other Tanium solutions that you import might provide more sensors. If you cannot find a sensor that you need within Tanium-provided content, you can create custom sensors.

For more information, see Tanium Console User Guide: Managing sensors.

Counting questions and non-counting questions

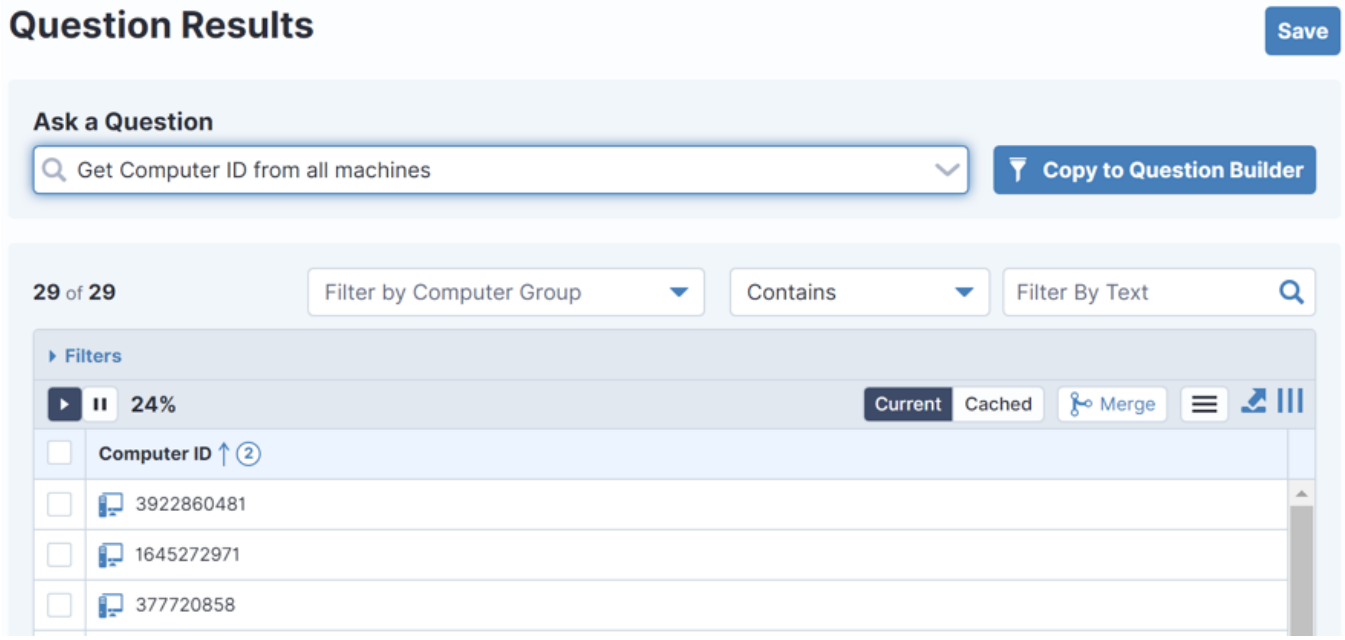
A *counting question* returns results in which it is possible for any particular answer string to be the same for multiple endpoints. The **Question Results** grid displays a **Count** column that indicates how many endpoints provided each common answer. A counting question can have only one sensor. `Get Operating System from all machines` is an example of a counting question, with a sensor that returns the operating system of managed endpoints. When an endpoint adds its answer to the answer message, it increments the tally of the answer that its value matches. The Tanium Server maintains a table of answer strings. In many cases, such as the operating system, many endpoints provide just a few common answers, so the question has a relatively small footprint on the Tanium Server.

Figure 2: Counting question



A *non-counting* question has sensors that return a unique answer string from each endpoint. For example, `Get Computer ID from all machines` returns unique answers. For a non-counting question, the Tanium Client adds a new string to the answer message instead of incrementing the tally for an existing string. Therefore, the data footprint for a non-counting question can be large on the Tanium Server.

Figure 3: Non-counting question



NOTE

If the **Count** column does not appear in the **Question Results** grid, click Customize Columns in the grid toolbar and select the **Count** check box to show the column. For more information on managing the **Question Results** grid, see Manage row sorting, column visibility, and text wrapping for question results.

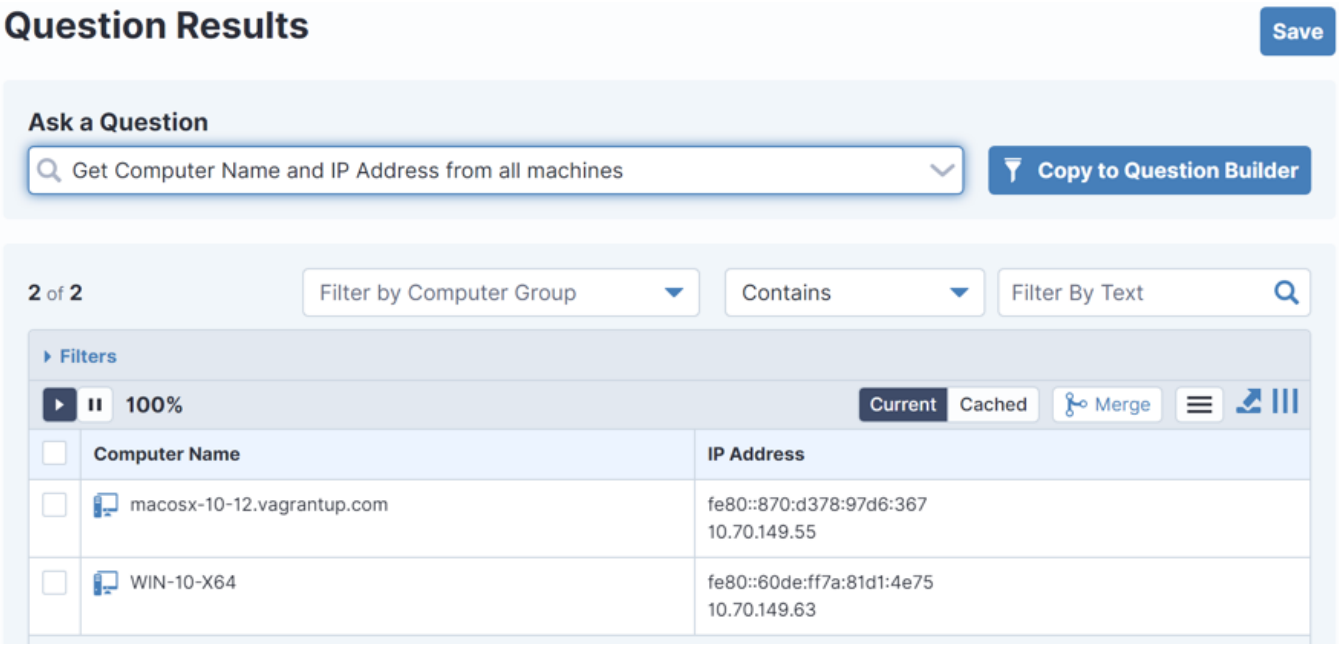
TIP

When using the **Question Builder** to construct a single-sensor question, you have the option to convert a counting question to a non-counting question for cases where a counting question returns the `[too many results]` answer. For details about that answer, see Tanium Console User Guide: Troubleshoot question results issues.

Questions with multiple sensors

When you construct a question, use the `AND` operator in the `get` clause to specify multiple sensors. The **Question Results** page groups results by the first sensor, then by the next sensor, and so on, as the following example illustrates.

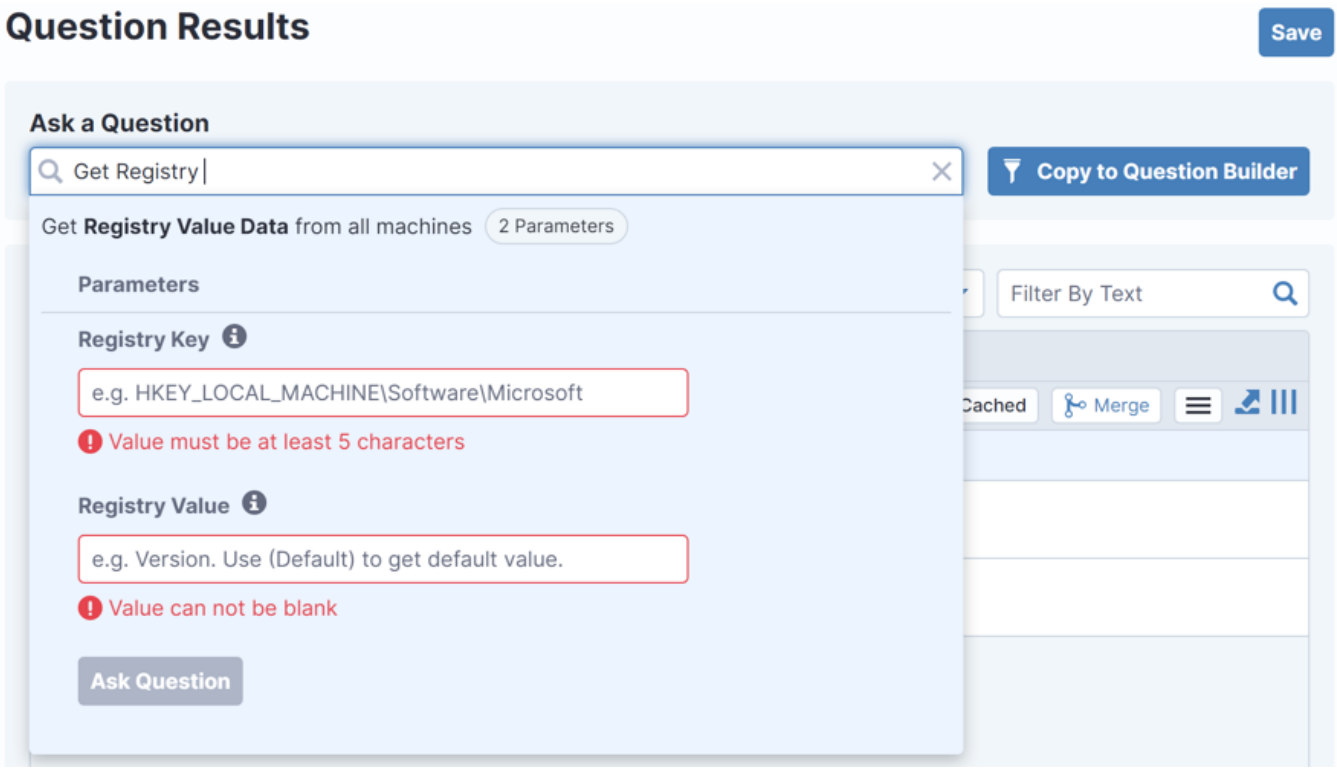
Figure 4: Question with multiple sensors



Questions with parameterized sensors

A *parameterized sensor* uses a value that you specify when entering the question in the **Ask a Question** field or **Question Builder**. The following example shows the Registry Value Data sensor. Tanium Console prompts you to specify a registry path and value.

Figure 5: Parameterized sensor



Another example is the High CPU Processes sensor. You can specify a parameter that is the number of CPU processes to return from each machine. For example, you might want to get the top 5 highest CPU utilizing processes. The question has the following syntax:

```
Get High CPU Process[5] from all machines
```

For sensors with multiple parameters, you can specify an ordered list of comma-separated parameters. For example, to see the first 10 lines from the action log for the action with ID 1, specify a parameter list as follows:

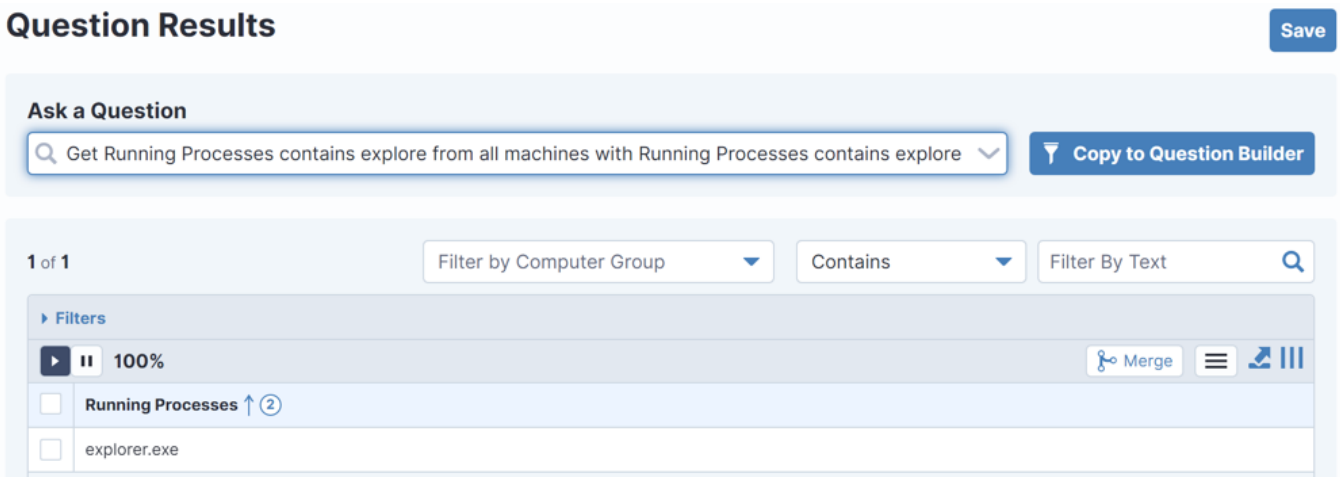
```
Get Tanium Action Log[1,10] from all machines
```

For more details, see Tanium Console User Guide: Example: Parameterized sensors.

Questions with filters

You can use filters to create questions that target fewer endpoints than the default `all machines`. For example, the following advanced question targets only endpoints that have a specific process name or value.

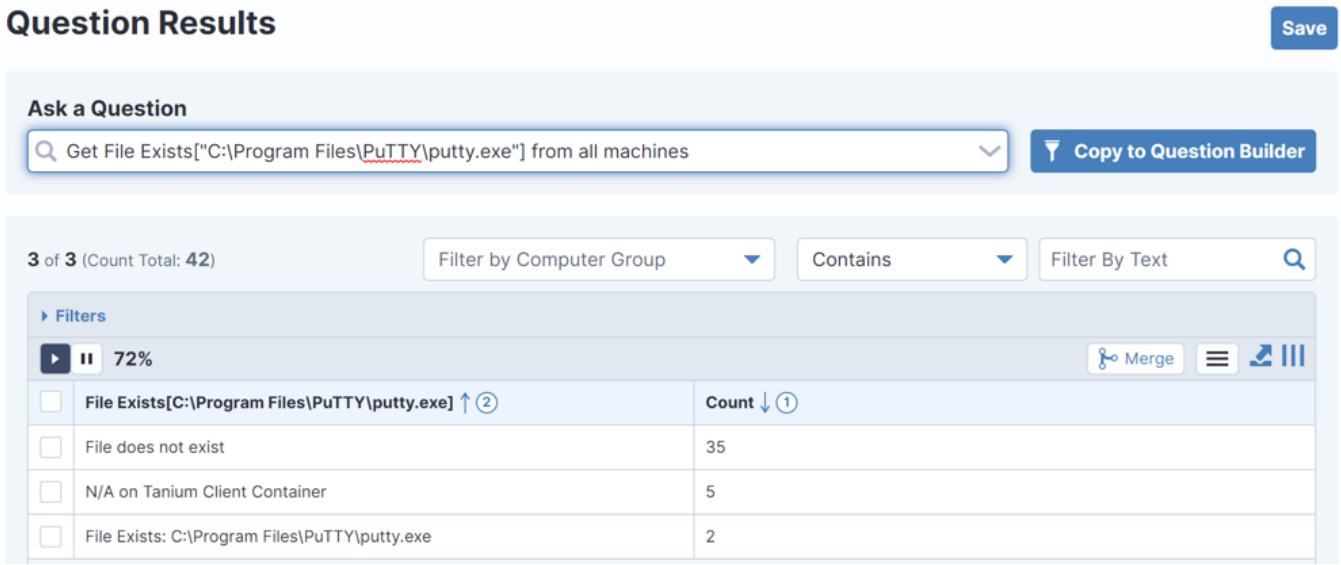
Figure 6: Question filter



The left side (`get` clause) is a complete and valid query; the right side contains a filter: the `from all machines with` expression. Filters in the `from` clause are the first part of a question that an endpoint processes. If the endpoint data does not match the filter, the endpoint does not process the question any further. If the question has multiple filters, the endpoint evaluates each filter. The filter expression must evaluate to a Boolean true or false. For example, the expression `from all machines with Running Processes contains explore` evaluates to true if the specified string matches the result string, or false if it does not. If a filter evaluates to true, the endpoint runs the sensors on the left side of the question and returns the results.

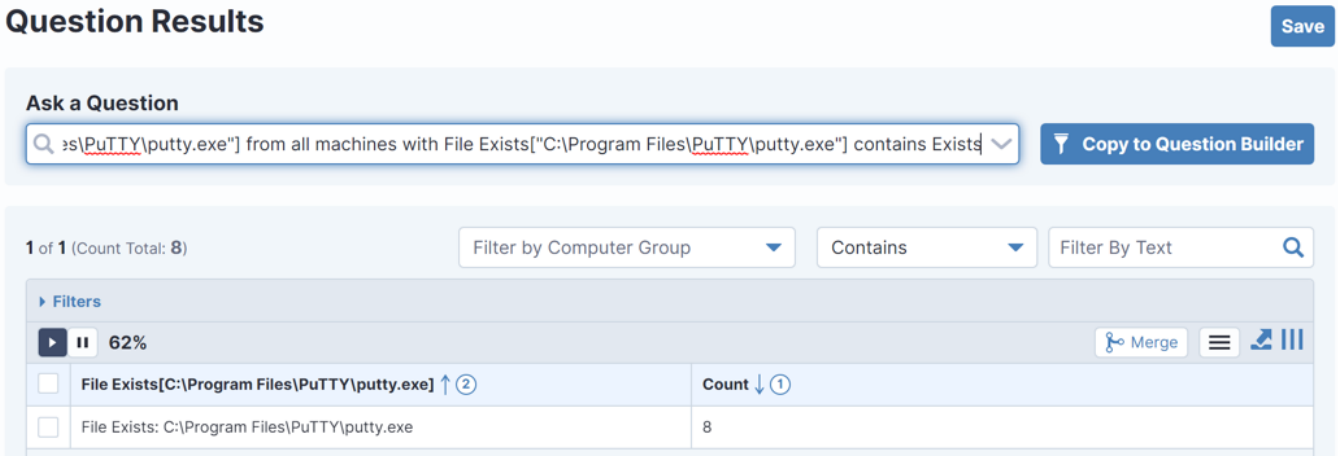
A parameterized sensor like `File Exists[]` returns the result `File Exists: Filename` or `File does not exist`, so be careful how you enter the sensor in a filter expression.

Figure 7: Example: Question with parameterized sensor



The filter expression `from all machines with File Exists["C:\Program Files\PuTTY\putty.exe"] contains "Exists"` evaluates to true when the result is `File Exists: C:\Program Files\PuTTY\putty.exe` and false when the result is `File does not exist`, so you can use it to filter the set of responses.

Figure 8: Example: Filter with parameterized sensor



Filter expressions can match strings or regular expressions. The following table describes the supported filter operators as they appear when you use the **Question Builder**. The table also describes how some operators are normalized after you load them from the **Question Builder** or enter the expressions in the **Ask a Question** field.

Table 1: Filter operators

Filter operator	Usage
contains	Sensor value contains the specified string. Example: `running processes contains "explore"`
does not contain	Sensor value does not contain the specified string.
starts with	Sensor value starts with the specified string. Example: `starts with "explore"` When you load the question, the expression is translated to a regular expression using the `matches` operator.
does not start with	Sensor value does not start with the specified string.
ends with	Sensor value ends with the specified string. Example: `ends with "explore.exe"` When you load the question, the expression is translated to a regular expression using the `matches` operator.
does not end with	Sensor value does not end with the specified string.
matches	Sensor value matches the specified regular expression (in Boost syntax).
does not match	Sensor value does not match the specified regular expression.

Table 1: Filter operators (continued)

Filter operator	Usage
in	Sensor value matches one of the specified strings. Use commas without spaces to separate the strings. When you load the question, the expression shown in the question field uses `equals` and `or` operators in place of `in`. Example: The filter `in "10.10.10.10,10.10.10.11"` in the Question Builder becomes `IP Address equals 10.10.10.10 or IP Address equals 10.10.10.11` when you load the question.
is equal to	Sensor value is equal to the specified value or string. When you load the question, the expression shown in the question field uses `equals` in place of `is equal to`.
is not equal to	Sensor value is not equal to the specified value or string. When you load the question, the expression shown in the question field uses `not equals` in place of `is not equal to`.
is less than	Sensor value is less than the specified value. When you load the question, the expression shown in the question field uses a symbol (`<`) in place of the operator words. Example: `installed application version[chrome] < 12`
is less than or equal to	Sensor value is less than or equal to the specified string. When you load the question, the expression shown in the question field uses symbols (`<=`) in place of the operator words. Example: `installed application version[chrome] <= 12`
is greater than	Sensor value is greater than the specified value. When you load the question, the expression shown in the question field uses a symbol (`>`) in place of the operator words. Example: `installed application version[chrome] > 12`
is greater than or equal to	Sensor value is greater than or equal to the specified string. When you load the question, the expression shown in the question field uses symbols (`>=`) in place of the operator words. Example: `installed application version[chrome] >= 12`

See Reference: Advanced question syntax on page 95 for examples of complex filter expressions, including questions with multi-column sensors.

Question expiration

When the Tanium Server issues a dynamic or saved question, it remains open (not expired) for 10 minutes on the targeted Tanium Clients. After a client returns values for the sensors in the question, if the values change while the question is open, that client returns the updated values. For example, if a client initially returns 50% for a question with the **CPU Consumption** sensor and consumption subsequently increases to 75% within the 10-minute interval, the client then returns 75%. Clients check every 10 seconds to determine whether sensor values have changed.

While a question is open, Tanium Clients evaluate the age of the results for each sensor to determine whether to return cached results or to reexecute the sensors for fresh results when answering subsequent questions that use the same sensors. See Maximum Data Age.

NOTE

The expiration interval is 30 minutes for questions that the Tanium™ Data Service issues to collect data for registered sensors. See Tanium Console User Guide: Manage sensor results collection.

For each question, the Tanium Server assigns an identifier (ID) that appears in the URL field of your browser when the **Question Results** page opens. For example, in the URL `https://10.20.30.40/#/interact/q/376`, the question ID is 376. The question and its ID expire 10 minutes after the question is issued, at which point the URL becomes invalid. This means you can refresh the page or share a link to its URL only within that 10-minute period. If you navigate to the URL after 10 minutes, Interact displays a `Question Expired` message and **Copy Question** button. Clicking the button reissues the question.

Saved questions

Saved questions are questions that you can reissue without reconstructing them in the Interact **Ask a Question** field. They are configuration objects for which you can define reissue intervals, access permissions, associated packages, and other settings. You can issue saved questions manually or based on a schedule. You can also issue saved questions through Tanium modules or through custom applications that use the Tanium XML API. For example, you can use Tanium™ Connect to periodically issue a saved question and send the results to an external server. You create saved questions by issuing a dynamic question through the **Ask a Question** field and saving it. Tanium solutions that you import also provide predefined saved questions. The Interact module organizes saved questions under dashboards and organizes dashboards under categories. Each category, dashboard, and saved question is assigned to one content set.

Dashboard

A *dashboard* is a group of saved questions that are related with respect to the information that they retrieve from endpoints. For example, the predefined **Hardware Inventory** dashboard contains questions that retrieve CPU, disk, memory, and BIOS information. You can issue all the questions in a dashboard simultaneously.

Category

A *category* is a group of dashboards. It serves as an umbrella term for questions that you use for a particular purpose. For example, the **Security** category includes multiple dashboards that contain security-related questions.

Content set

A *content set* is a group of saved questions, dashboards, categories, and other content to which you apply user role permissions to control access. Tanium solutions provide several predefined content sets. You can also create custom content sets. For details and related tasks, see Managing content sets.

Questions results

After you issue a dynamic question, the **Question Results** page opens and displays a grid with the answers (results) from endpoints. The page facilitates analyzing the results by providing display options such as live updates, filters, and charts. For details and related procedures, see Managing question results on page 50.

Actions

After you use Interact to issue a question, analyze the question results, and determine which endpoints require administrative action, you can deploy a package to those endpoints so that the Tanium Client can run the associated action. For the procedure, see Deploying actions on page 68.

Interoperability with other Tanium products

API Gateway

Interact includes Tanium Data Service, which is a service that enables you to see stored sensor results for endpoints that are offline at the moment you issue a question. You can use Tanium™ API Gateway to access data from the Tanium Data Service API. For information about what features are available through API Gateway, refer to the API Gateway schema reference.

- For information about how to access the schema reference, see Tanium API Gateway User Guide: Schema reference.
- For information about Tanium Data Service, see Tanium Console User Guide: Manage sensor results collection.

Reporting

Interact provides access to the Endpoint Details page in Tanium™ Reporting, where you can view comprehensive information about a single endpoint and manage the endpoint. To access the page, see Search endpoints on page 47. For more information about endpoint details, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

Getting started with Interact

Step 1: Review the requirements

Review the system, network, security, and user role requirements: see Interact Requirements on page 25.

Step 2: Sign in to Tanium Console

See Tanium Console User Guide: Sign in to Console.

Step 3: Install and configure Interact

See Installing Interact on page 37 and Configuring Interact on page 39.

Step 4: (Optional) Customize Interact

Customize the Interact **Overview** page: see Tanium Console User Guide: Customize Tanium module overview pages.

Step 5: (Optional) Configure Tanium Data Service

Configure the Tanium Server to automatically collect results for specific sensors so that you can see those results for endpoints that are offline when you issue questions: see Tanium Console User Guide: Manage sensor results collection.

Step 6: Ask questions and search endpoints

Issue dynamic questions to retrieve information about multiple endpoints in your network or display comprehensive information about a particular endpoint: see Asking questions and searching endpoints on page 41.

Step 7: Analyze and manage question results

For example, you can drill down into the question results with additional questions, filter the **Question Results** grid, and export its content: see Managing question results on page 50.

Step 8: Deploy ad-hoc actions or schedule recurring actions

Deploy ad-hoc actions or schedule recurring actions based on question results: see Deploying actions on page 68.

Step 9: Manage saved questions

For example, you can create saved questions, assign them to dashboards, assign the dashboards to categories, and assign saved questions to content sets based on RBAC requirements. See Managing saved questions on page 75.

Gaining organizational effectiveness

The three key organizational governance steps to maximizing the value that is delivered by Interact are as follows:

- Develop a dedicated change management process. See Change management on page 21.
- Validate cross-functional alignment. See Organizational alignment on page 21.
- Track operational maturity. See Operational metrics on page 21.

Change management

Develop a tailored, dedicated change management process for data consumption, taking into account the new capabilities provided by Tanium.

- Update SLAs with elevated expectations, including data consumption configuration and maintenance.
- Identify key resources in the organization to review and approve changes to data consumption to ensure minimal unexpected or unapproved changes.
- Identify maintenance windows for various data consumption scenarios to maximize uptime.
- Create a Tanium steering group (TSG) for data consumption activities, to expedite reviews and approvals of processes that align with SLAs.

Organizational alignment

Successful organizations use Tanium across functional silos as a common platform for high-fidelity endpoint data and unified endpoint management. Tanium provides a common data schema that enables security, operations, and risk/compliance teams to assure that they are acting on a common set of facts that are delivered by a unified platform.

In the absence of cross-functional alignment, functional silos often spend time and effort in litigating data quality instead of making decisions to increase awareness of data consumption at all levels of the organization.

Operational metrics

Interact maturity

Managing data consumption successfully includes operationalization of the technology and measuring success through key benchmarking metrics. The four key processes to measure and guide operational maturity of your Tanium Interact program are as follows:

Process	Description
Usage	How and when Tanium Interact is used in your organization

Process	Description
Automation	How automated Tanium Interact is
Functional Integration	How integrated Tanium Interact is, across IT security, IT operations, and IT risk/compliance teams
Reporting	How automated Tanium Interact is and who the audience of data consumption is

Use the following table to determine the maturity level for Tanium Interact in your organization.

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
Process	Usage	Interact is installed and one or more users have access and can ask basic questions	Saved questions created and in use / custom dashboards created that use saved questions / **Question Builder** in use for advanced questions Parameterized sensors understood and in use Visibility into real-time hardware and software inventory Leverage cache data through Tanium Data Service	Basic role-based access control (RBAC) configured Ad-hoc / scheduled actions in use / deploying actions Importing custom content for specific use cases Managing and registering sensors in Tanium Data Service	Optional: Action approval implemented (control before deploying an action) Advanced question syntax in use (such as the sensor column filter, 'in' operator, and regular expressions) Export RBAC details to audit user management	Custom RBAC implemented, as desired Authoring custom sensors and custom packages

		Level 1 (Initializing)	Level 2 (Progressing)	Level 3 (Intermediate)	Level 4 (Mature)	Level 5 (Optimized)
	Automation	Manual	Automated; Tanium Data Service data collection and purging	Automated; saved questions and scheduled actions	Automated; tuning Tanium Data Service purging of transient computers by computer group	Automated; tuning Tanium Data Service purging of transient computers by computer group
	Functional integration	Tanium Core with Tanium Interact is integrated across Security / Compliance / Operations				
	Reporting	Unused	Ad hoc; reporting tailored to stakeholders at request	Automated through Tanium Connect; reporting tailored to stakeholders on cadence	Automated through Tanium Connect; reporting tailored to stakeholders ranging from Operator to Executive	Automated through Tanium Connect; reporting tailored to stakeholders ranging from Operator to Executive

Interact Requirements

Review the requirements before you install and use Interact.

Core platform dependencies

Make sure that your environment meets the following requirements:

- Tanium™ Core Platform servers 7.4 or later

Solution dependencies

If you select **Tanium Recommended Installation** when you import Interact, the Tanium Server automatically imports all your licensed solutions at the same time. See Tanium Console User Guide: Import all modules and services.

Import specific solutions

If you select only Interact to import and are using Tanium Core Platform 7.5.2.3531 or later with Tanium Interact 3.0.72 or later, the Tanium Server automatically imports the latest available versions of any required dependencies that are missing. If some required dependencies are already imported but their versions are earlier than the minimum required for Interact, the server automatically updates those dependencies to the latest available versions.

If you select only Interact to import and you are using Tanium Core Platform 7.5.2.3503 or earlier with Tanium Interact 3.0.64 or earlier, you must manually import or update required dependencies. See Tanium Console User Guide: Import, re-import, or update specific solutions.

Required dependencies

Interact has the following required dependencies at the specified minimum versions:

- Tanium™ Core Content 1.3.100 or later
    - Core Content 1.8.5 or later requires Tanium™ Client Management
- Tanium™ Default Computer Groups 1.0.6 or later
- Tanium™ Default Content 8.4.29 or later
- Tanium™ RDB Service 1.2.151 or later
- Tanium™ System User Service 1.0.77 or later

For details about these content-only solutions, see Tanium Console User Guide: Initial content.

Feature-specific dependencies

If you select only Interact to import, you must manually import or update its feature-specific dependencies regardless of the Tanium Interact or Tanium Core Platform versions. Interact has the following feature-specific dependencies at the specified minimum versions:

- Tanium™ Reporting
  - 1.8.40 or later is required to display Reporting dashboards on the Tanium **Home** page. See Tanium Console User Guide: View dashboards.
  - 1.12 or later is required to access the Endpoint Details page from the Interact workbench. See Search endpoints on page 47.

Tanium Server computer resource and network requirements

Interact includes both the Interact workbench and Tanium Data Service. The Interact workbench installs and run on the Tanium Server, while Tanium Data Service installs and runs on the Module Server. The general resource specifications for the Tanium Server include the host computer resource and network requirements for Tanium Console and Interact. The impact of Tanium Data Service on the Tanium Module Server depends on usage. See the guide for your deployment for details.

- For general Module Server sizing guidelines in a Windows deployment, see Tanium Core Platform Deployment Guide for Windows: Host system resource guidelines.
- For Tanium Appliance specifications, see Tanium Appliance Deployment Guide: Tanium Appliance specifications.

Endpoints

Supported operating systems

Interact supports the same operating systems (OSs) for endpoints that the Tanium Client supports:

- Windows
- MacOS
- Linux
- AIX
- Solaris

For details about support for specific OS versions, see Tanium Client Management User Guide: Client version and host system requirements.

Disk space requirements

On managed endpoints, Interact requires at least 100 MB of disk space and another 100 MB of cache space for data files. The cache space includes the Tanium Client chunk cache and objects such as sensors and logs.

Processor requirements

On managed endpoints, Interact requires at least 10 MB of RAM and accounts for less than 0.5% of idle CPU usage.

Host and network security requirements

Specific ports and processes are needed to run Interact.

Ports

The following ports are required for Interact communication.

Source	Destination	Port	Protocol	Purpose
Module Server	Module Server (loopback)	17495	TCP	Internal purposes, not externally accessible

Configure firewall policies to open ports for Tanium traffic with TCP-based rules instead of application identity-based rules. For example, on a Palo Alto Networks firewall, configure the rules with service objects or service groups instead of application objects or application groups.

Security exclusions

Host and network security requirements for the Tanium Core Platform apply to Interact. For details, see Tanium Core Platform Deployment Reference Guide: Host system security exceptions.

User role requirements

Tanium has roles and permissions for both Interact and associated Tanium Data Service. To review a summary of the predefined roles, see Configuring Interact on page 39.

Interact module permissions

Interact has the following predefined module roles and associated module permissions.

Table 2: Interact user role permissions

Permission	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Ask Dynamic Questions[1] Issue questions through the Interact **Ask a Question** field and **Question Builder**.	SPECIAL	SPECIAL		

Table 2: Interact user role permissions (continued)

Permission	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Interact View the Interact workbench.	✓ SHOW	✓ SHOW	✓ SHOW	✓ SHOW
Interact Execute[2] Deploy actions in Interact.	✓ ACTION	✗	✗	✗
Interact Module[3,4] View, create, edit, or delete Interact content.	✓ READ WRITE	✓ READ WRITE	✓ READ	✗

[1] This permission applies to the Reserved content sets.

[2] The **Interact Execute** permission provides the following permissions:

- Platform content permissions: **Filter Group** read, **Sensor** read, **Saved Question** read, **Dashboard** read, **Dashboard Group** read, **Package** read, **Action** read, **Saved Question** write, **Dashboard** write, **Dashboard Group** write, and **Action** write. The **Dashboard** read and write permissions apply to Interact dashboards, not Reporting dashboards.
- Reporting module permissions: See Table 3.

[3] The **Interact Module** read permission provides the following platform content permissions: **Filter Group** read, **Sensor** read, **Saved Question** read, **Dashboard** read, and **Dashboard Group** read. The **Dashboard** read and write permissions apply to Interact dashboards, not Reporting dashboards.

[4] The **Interact Module** write permission provides the following permissions:

- Platform content permissions: **Filter Group** read, **Sensor** read, **Saved Question** read, **Dashboard** read, **Dashboard Group** read, **Saved Question** write, **Dashboard** write, **Dashboard Group** write. The **Dashboard** read and write permissions apply to Interact dashboards, not Reporting dashboards.
- Reporting module permissions: See Table 3.

The following table lists the provided platform content permissions and associated content sets (see the table footnotes) for the Interact permissions in Table 2.

Table 3: Provided platform content permissions for Interact

Permission	Permission Type	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Action	Platform Content	✓ READ WRITE	✗	✗	✗

Table 3: Provided platform content permissions for Interact (continued)

Permission	Permission Type	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Dashboard[1]	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Dashboard Group	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Filter Group	Platform Content	✓ READ	✓ READ	✓ READ	✗
Own Action	Platform Content	✓ READ	✗	✗	✗
Package	Platform Content	✓ READ	✗	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE	✓ READ EXECUTE
Saved Question	Platform Content	✓ READ WRITE	✓ READ WRITE	✓ READ	✗
Sensor	Platform Content	✓ READ	✓ READ	✓ READ	✗

To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.

[1]The **Dashboard** read and write permissions apply to Interact dashboards, not Reporting dashboards.

The **Interact Execute** action permission and **Interact Module** write permission each provide the following Reporting module permissions and associated content sets (see the table footnotes). These permissions enable users to access the Endpoint Details page in the Reporting workbench. For information about the Endpoint Details page, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

Table 4: Provided Reporting permissions for Interact

Permission	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Dashboard[1]	✓ READ	✓ READ	✗	✗

Table 4: Provided Reporting permissions for Interact (continued)

Permission	Interact Power User	Interact Basic User	Interact Read-Only User	Interact Show
Report[1]	✓ READ	✓ READ	✗	✗
Report API	✓ USER	✓ USER	✗	✗
Reporting Category	✓ READ	✓ READ	✗	✗
Reporting Settings	✓ READ	✓ READ	✗	✗

[1]The **Dashboard** and **Report** permissions apply to the Reporting content set. The Reporting **Dashboard** module permission is distinct from the platform content **Dashboard** permission that Table 2 references.

The following table summarizes the permissions required to perform specific tasks in Interact. Interact includes the Interact **Overview** page and **Question Builder** page. The **Administrator** reserved role has all the listed permissions. The table also indicates whether other reserved roles have permissions for the features.

Table 5: Required permissions to perform Interact tasks

Tasks	Roles and permissions
Install or uninstall Interact	**Administrator** reserved role only
All tasks in Interact	**Interact** show (module) permission is required for all Interact features, so be sure to assign a role with that permission to all Interact users.
View Interact content	**Interact Module** read (module) permission is required to view content in the Interact content set.
Manage Interact content	**Interact Module** write (module) permission is required to add, edit, or delete content in the Interact content set.
Deploy actions in Interact	**Interact Execute** (module) permission enables users to deploy actions in Interact. It implies the platform content permissions **Package** read, **Action** read, and **Action** write.

Table 5: Required permissions to perform Interact tasks (continued)

Tasks	Roles and permissions
Issue questions through the **Ask a Question** field and **Question Builder**	**Ask Dynamic Questions** (module) permission is required to issue questions through the **Ask a Question** field and **Question Builder**. You can assign the permission to any custom role. **Sensor** read content set permissions determine which sensors are available for you to select for questions. **Filter Group** read content set permissions determine which computer filter groups are available for you to view and select for questions and question results. Depending on whether Tanium™ Reporting, Tanium™ Asset, or both are installed, you require additional permissions to see endpoint details through the **Search Endpoints** field or the **Question Results** page. For more information, see View details for a single endpoint. The **Administrator** and **Content Administrator** reserved roles have all these permissions.
Save a question	**Saved Question** write permission is required to assign a saved question to content sets for which you have permission. **Saved Question** write is also required to create, edit, or delete saved questions. The **Sensor** read content set permissions determine the available sensors. **Filter Group** read content set permissions determine the available filter groups. In addition to the **Saved Question** write permission, users require the **Action** write and **Package** write permissions to add associated packages to a new saved question configuration. In addition to these three permissions, users require owner permissions for the question if they want to modify or delete the associated packages. The **Administrator** and **Content Administrator** reserved roles have all these permissions.
Use Interact Saved Questions	**Saved Question** read content set permissions determine the saved questions that you can see in Tanium Console, such as on the Interact **Overview** page, **Question Builder** page, and **Question Results** grid drill-down. **Sensor** read permission is required for the sensors specified in a saved question that you want to issue. **Filter Group** read content set permission is required for the filter groups specified in the saved question. **Ask Dynamic Questions** permission is required to use the drill down feature in the saved question results grid.
Use Interact Categories	**Dashboard Group** read content set permissions determine the categories that you can see in Tanium Console, such as on the Interact **Overview** page. **Dashboard Group** write permission is required to create, modify, or delete category configurations. **Dashboard** read content set permissions determine which Interact dashboards are available in categories. The **Administrator** and **Content Administrator** reserved roles can export and import categories.

Table 5: Required permissions to perform Interact tasks (continued)

Tasks	Roles and permissions
Use Interact Dashboards	**Dashboard** read content set permissions determine the Interact dashboards that you can see in Tanium Console, such as on the Interact **Overview** page. **Dashboard** write permission is required to create, modify, or delete Interact dashboard configurations. **Saved Question** read content set permissions determine which saved questions are available in dashboards. These **Dashboard** read and write permissions apply to Interact dashboards, not Reporting dashboards. The **Administrator** or **Content Administrator** reserved role can export and import Interact dashboards.
Deploy an action	**Action** write permission is required to see the **Deploy Action** button on the **Question Results** grid. **Package** read content set permissions determine which packages are available for you to select for actions. **Sensor** read and **Saved Question** read permissions on the **Reserved** content set are required to complete the deploy action workflow. During the workflow, these permissions allow special saved questions that the Tanium Server uses to track and report action status. The **Administrator** reserved role and **Interact Power User** role have all these permissions.
Use the Interact **Overview** page	To see the following sections of the Interact **Overview** page, users require the specified permissions: • **Overview**: **Dashboard Group** read, **Dashboard** read, and **Saved Question** read permissions control the summary counts. • **Favorite Categories**: **Dashboard Group** read permission • **Favorite Dashboards**: **Dashboard** read permission • **Favorite Saved Questions**: **Saved Question** read permission The **Dashboard** permissions apply to Interact dashboards, not Reporting dashboards. The **Administrator** reserved role has all these permissions.

Tanium Data Service permissions

Tanium Data Service has the following predefined module roles and associated module permissions.

Do not assign the **Tanium Data Service Account**, **Tanium Data Service Account - All Content Sets**, or **Data Collection Service Account** roles to users. These roles are for internal purposes only.

Table 6: Tanium Data Service user role permissions

Permission	Data Collection Administrator	Data Collection Operator
Ask Dynamic Questions A global permission that applies to all content sets. It enables issuing questions through the Interact **Ask a Question** field and **Question Builder**.	✗	✗
Data Collection OPERATOR: Access to configure data collection settings START: Manually start an unscheduled query to collect sensor results	✓ START	✓ OPERATOR START
Data Collection Administrator Unrestricted access to configure data collection	✓ ADMINISTER	✗
Data Collection API Identify Endpoint The following permissions are for internal purposes only and apply to the Tanium Data Service content set: READ: Read the results of the internal Endpoint ID sensor WRITE: Allocate Endpoint ID values to endpoints DELETE: Purge the sensor results of specific endpoints from Tanium Data Service based on Endpoint ID values	✓ READ WRITE DELETE	✓ READ DELETE
Data Collection Bundle Config View and edit configuration data for the next support bundle (internal purposes only)	✓ READ WRITE	✗
Data Collection EID Namespace Read and write endpoint ID namespaces (internal purposes only)	✗	✗
Data Collection Identify Endpoint The following permissions are for internal purposes only: READ: Resolve which sensors are used to determine the endpoint ID (EID) WRITE: Allocate the sensors that are used to determine the EID	✓ READ WRITE	✗

Table 6: Tanium Data Service user role permissions (continued)

Permission	Data Collection Administrator	Data Collection Operator
Data Collection Job Read and cancel pipeline jobs (internal purposes only)	✗	✗
Data Collection Metrics View the **Data Service Sensor Metrics** and **Data Service Database Metrics** charts in the Interact **Info** page	✓ READ	✓ READ
Data Collection Operator Settings View and edit Tanium Data Service settings (internal purposes only)	✓ READ WRITE	✓ READ WRITE
Data Collection Pipeline Read pipeline data (internal purposes only)	✗	✗
Data Collection Pipeline Write Write pipeline data (internal purposes only)	✗	✗
Data Collection Purge Purge data for specific sensors (internal purposes only)	✓ SENSOR	✓ SENSOR
Data Collection Rdb Connect to the Tanium™ RDB service (internal purposes only)	✗	✗
Data Collection Registration READ: View the Interact **Settings > Registration & Collection** page to see which sensors are registered for results collection WRITE: Register or unregister sensors for results collection, pause (disable) or resume (enable) collection, and purge results	✓ READ WRITE	✓ READ WRITE
Data Collection Sensor Write virtual sensor data (internal purposes only)	✗	✗

Table 6: Tanium Data Service user role permissions (continued)

Permission	Data Collection Administrator	Data Collection Operator
Data Collection Settings View and edit Tanium Data Service settings (internal purposes only)	✓ READ WRITE	✗
Data Collection Status View the **Data Service Status** chart in the Interact **Info** page	✓ READ	✓ READ
Data Collection Virtual Sensor Definition View and edit virtual sensors (internal purposes only)	✗	✗
Result Exclusion Read and write exclusions (internal purposes only)	✓ READ WRITE	✗
Result Expansion Read and write expansions (internal purposes only)	✓ READ WRITE	✗

Tanium Data Service roles also have the following administration and platform content permissions:

Table 7: Provided Tanium Data Service administration and platform content permissions

Permission	Permission Type	Data Collection Administrator	Data Collection Operator
Action Group	Administration	✗	✗
Client Status	Administration	✗	✗
Computer Group	Administration	✗	✗
Persona	Administration	✗	✗
User	Administration	✓ READ	✗
Action	Platform Content	✗	✗
Own Action	Platform Content	✗	✗
Plugin	Platform Content	✓ READ EXECUTE	✓ READ EXECUTE

Table 7: Provided Tanium Data Service administration and platform content permissions (continued)

Permission	Permission Type	Data Collection Administrator	Data Collection Operator
Saved Question	Platform Content	✗	✗
Sensor	Platform Content	✓ READ	✓ READ
To view which content set permissions are granted to a role, see Tanium Console User Guide: View effective role permissions.			

Installing Interact

Use the Tanium Console **Solutions** page to install Interact 2.1 or later and choose automatic or manual configuration:

- **Automatic configuration with dependencies**: Interact is installed with any required dependencies and other selected solutions. This option is the best practice for most deployments. For more information, see Import Interact with dependencies on page 37.
- **Manual configuration without dependencies**: Interact is installed without any required dependencies or other solutions. For more information, see Import Interact without dependencies on page 37.

In Tanium Core Platform versions earlier than 7.4.2.2063, the Tanium Server automatically imports the Interact workbench and Interact content set after you install the server and sign in to Tanium Console for the first time.

Before you begin

- Read the release notes.
- Review the Interact Requirements on page 25.
- Assign the correct roles to users for Interact. Review the User role requirements on page 27.
    - To import the Interact solution, you must be assigned the Administrator reserved role.

Import Interact with dependencies

No default settings are configured for Interact.

To import Interact with with required dependencies, be sure to select the **Apply Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Manage Tanium solutions. After the import, verify that the correct version is installed: see Verify the Interact version on page 38.

Import Interact without dependencies

To import Interact without any required dependencies, clear the **Apply All Tanium recommended configurations** check box while performing the steps in Tanium Console User Guide: Import, re-import, or update specific solutions. After the import, verify that the correct version is installed: see Verify the Interact version on page 38.

Upgrade Interact

For the steps to upgrade Interact, see Tanium Console User Guide: Manage Tanium solutions. After the upgrade, verify that the correct version is installed: see Verify the Interact version on page 38.

Verify the Interact version

After you import or upgrade Interact, verify that the correct version is installed:

1. Refresh your browser.
2. From the Main menu, go to **Modules > Interact** to open the Interact **Overview** page.
3. To display version information, click Info  .

Configuring Interact

The following sections describe the predefined user roles that you can use to set up Interact and Tanium Data Service users. To review specific permissions for each role, see User role requirements on page 27.

For more information about assigning user roles, see Tanium Core Platform User Guide: Manage role assignments for a user.

IMPORTANT On installation, Interact creates a **Tanium Data** user to automatically manage the service account for Tanium Data Service. Do not edit or delete the **Tanium Data** user.

Set up Interact users

Interact Power User

Assign the **Interact Power User** role to users who ask questions, manage content in the Interact content sets, and deploy actions through Interact.

Interact Basic User

Assign the **Interact Basic User** role to users who ask questions and manage content in the Interact content sets.

Interact Read-Only User

Assign the **Interact Read-Only User** role to users who ask questions and view content in the Interact content sets.

Interact Show

Assign the **Interact Show** role to users who view content in the Interact workbench. This includes users who need to view question results and saved question results in Interact.

Set up Tanium Data Service users

Data Collection Administrator

Assign the **Data Collection Administrator** role to users who manage the sensors from which to collect data for Tanium Data Service. This role can perform the following tasks:

- Purge data for specific sensors
- Register, unregister, enable, and disable sensors for collection
- Configure data collection settings (unrestricted access)

Data Collection Operator

Assign the **Data Collection Operator** role to users who manage the sensors from which to collect data for Tanium Data Service. This role can perform the following tasks:

- Purge data for specific sensors
- Register, unregister, enable, and disable sensors for collection
- Configure data collection settings

Do not assign the **Tanium Data Service Account**, **Tanium Data Service Account - All Content Sets**, or **Data Collection Service Account** roles to users. These roles are for internal purposes only.

Asking questions and searching endpoints

Use Tanium Interact to ask questions and retrieve information from endpoints. For example, you can ask a question that determines if any endpoints are missing critical security patches. Based on the question results that the endpoints return, you can then deploy actions, such as installing security patches. You can also use the Interact **Search Endpoints** feature to quickly retrieve comprehensive information about a single endpoint instead of constructing a long question with many sensors.

For an overview of questions and related concepts, see Interact overview on page 9. For the user roles and permissions required to ask questions, see User role requirements on page 27.

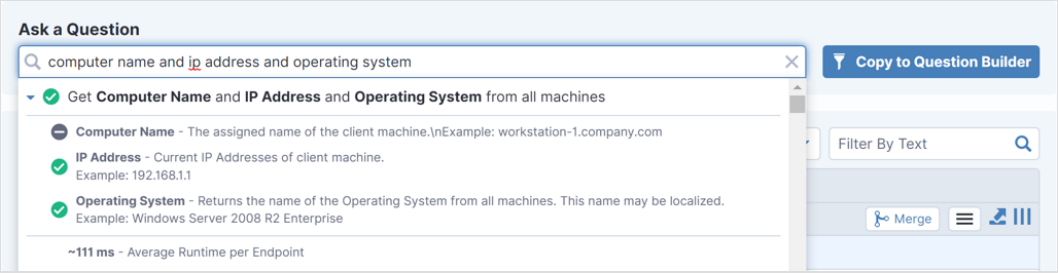
Issue a question through the Ask a Question field

Use the Interact **Ask a Question** field to quickly construct dynamic questions. The field is particularly useful when you want to issue simple questions, or when you understand Tanium question syntax sufficiently to manually enter advanced questions that involve filters, regular expressions, or operators.

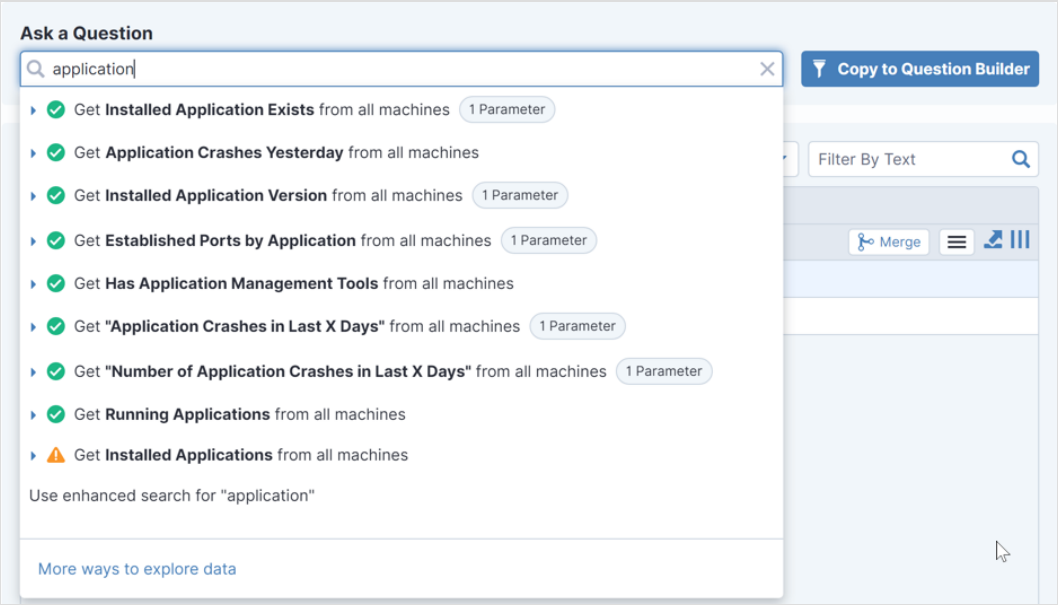
If you want guidance while creating questions, see Issue a question through the Question Builder on page 43. For details on question syntax, including how to handle reserved words and characters in question text or sensor names, see Reference: Advanced question syntax on page 95.

1. Go to the Tanium **Home** page or Interact **Overview** page.
2. In the **Ask a Question** field, enter your question and press **Enter**, or just move your cursor to the field to open a dropdown list from which to select a recently asked question. Note the following options and behaviors for the field:
    - Interact uses a natural language parser to interpret your entry. The question text can be in natural English and does not require complete sentences, case sensitivity, or strictly correct spelling.
    - Unless you specify a `from` clause in the question, Interact uses the default `from all machines`. This default value specifies that all managed endpoints that are members of computer groups assigned to your user account answer the question.
    - For new users, the dropdown list contains a list of common questions. When you return to the **Ask a Question** field for subsequent questions, the dropdown list shows your most recent questions.

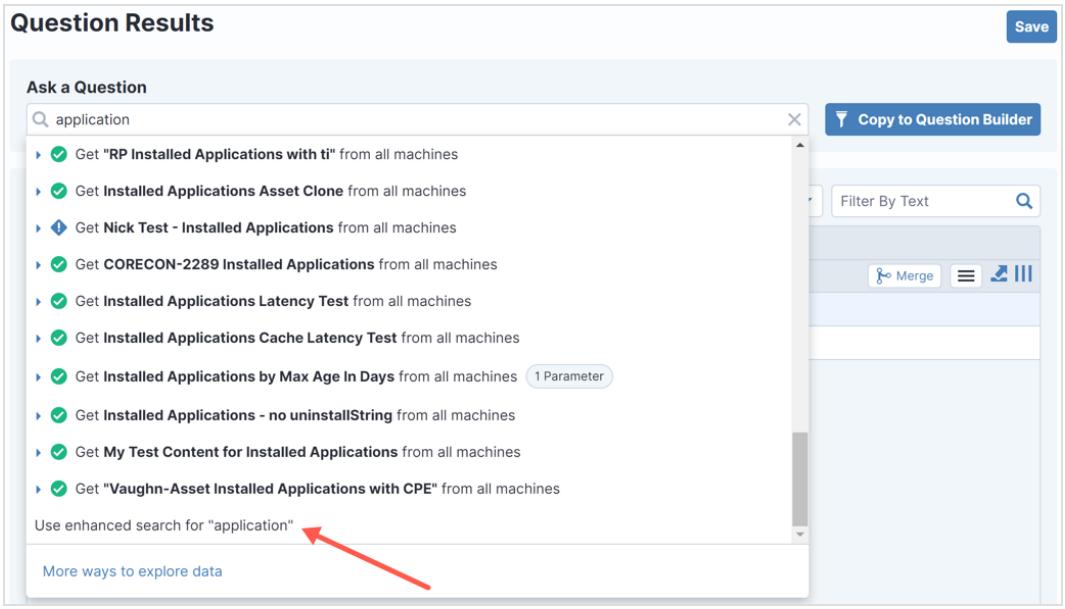
- Expand a question in the dropdown list to show details for that question, including the average runtime on endpoints and which sensors are used.



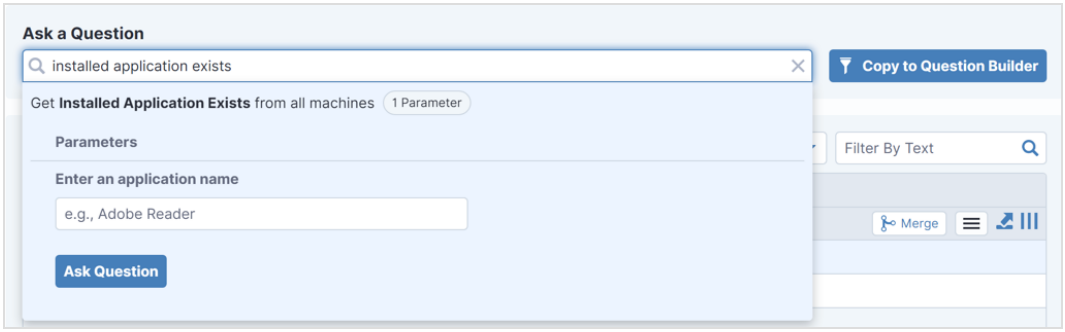
- When you enter a question, the dropdown list displays a set of proposed questions in valid syntax, listed in the order of how closely they approximate your question text. If the proposed questions do not match your entry, add quotation marks around the sensor names (see Use reserved words or characters). Alternatively, click **More ways to explore data** in the dropdown list to open the **Question Builder**, which shows how to properly format question text.



- If your question does not appear in the dropdown list, select the **Use enhanced search for** option. The natural language parser then examines the question text and shows additional questions.



- If your question text includes a parameterized sensor, Interact prompts you for the parameters.



After you press **Enter** or select a question in the dropdown list, the **Question Results** page opens to show answers from endpoints.

TIP

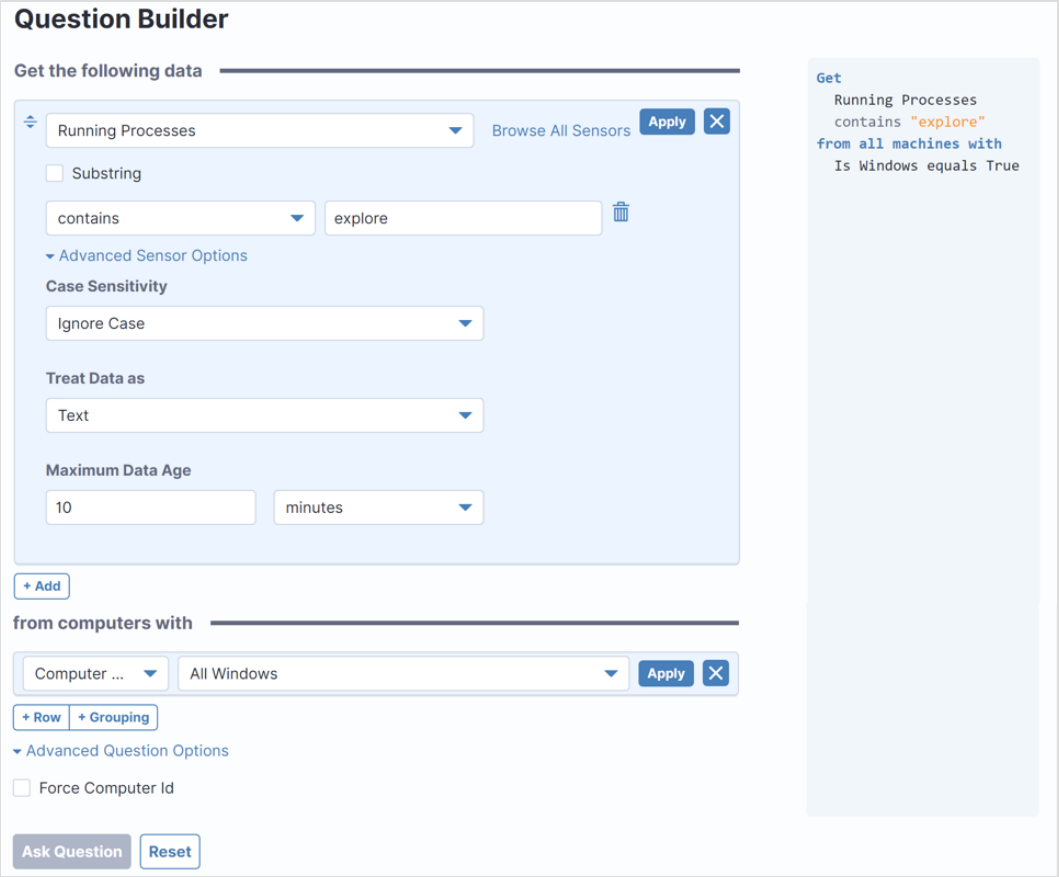
For examples of questions that you can enter in the **Ask a Question** field, see Reference: Example questions on page 91.

For details and tasks relating to question results, see Managing question results on page 50.

Issue a question through the Question Builder

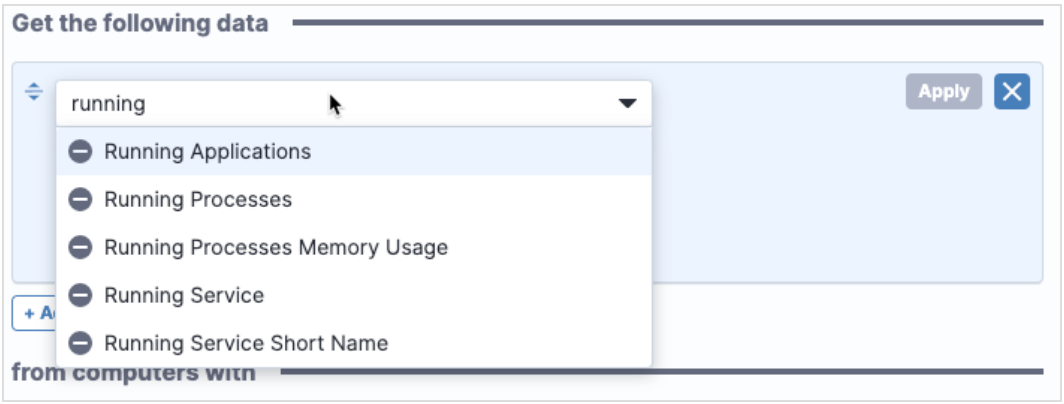
The **Question Builder** provides a guided method for creating a dynamic question. It has form fields to help you complete the `get` statement and the `from` clause, including any filters.

Figure 9: Question Builder

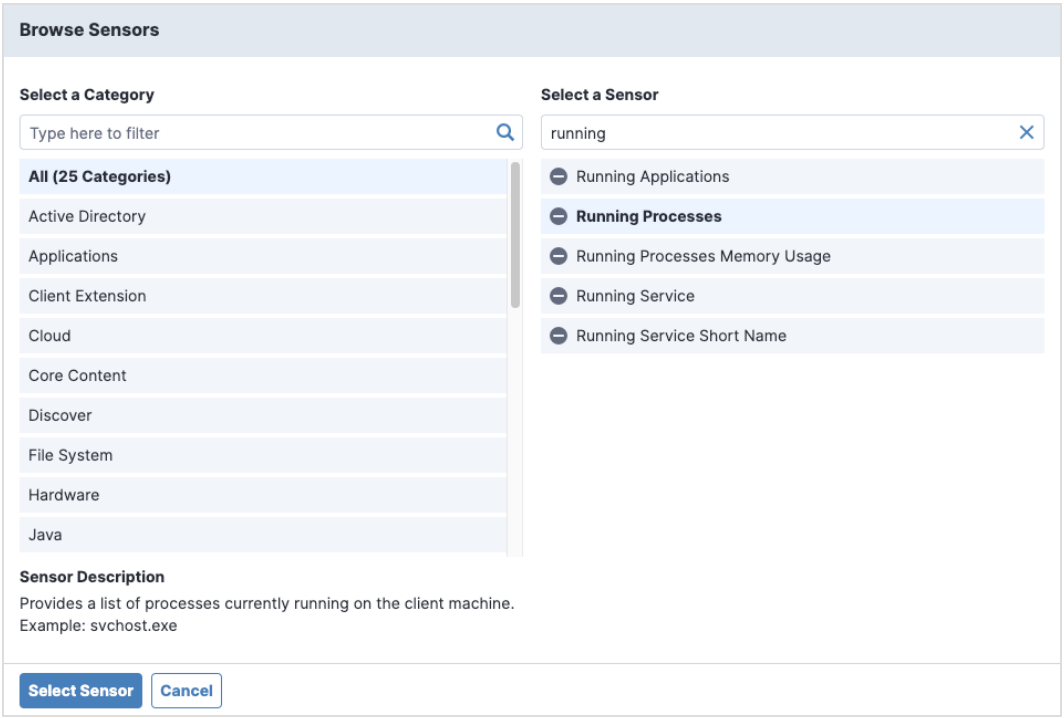


1. Open the **Question Builder** page:
    - To create a new question, click **Build Question** beside the **Ask a Question** field on the Tanium **Home** page.
    - To refine a question that you already issued, click **Copy to Question Builder** next to the question field on the **Question Results** page.
    - You can also access the **Question Builder** page from the Interact menu, and through the **More ways to explore data** option in the **Ask a Question** field.
2. Click **+ Add** below **Get the following data** to create the get statement. A row appears with a text field for entering a sensor name.

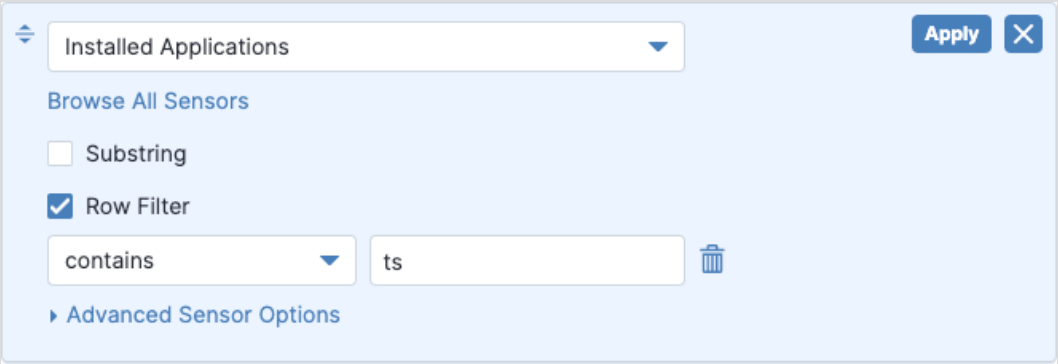
3. Start typing in the sensor name field, use the typeaheads to select a sensor, and click **Apply**.



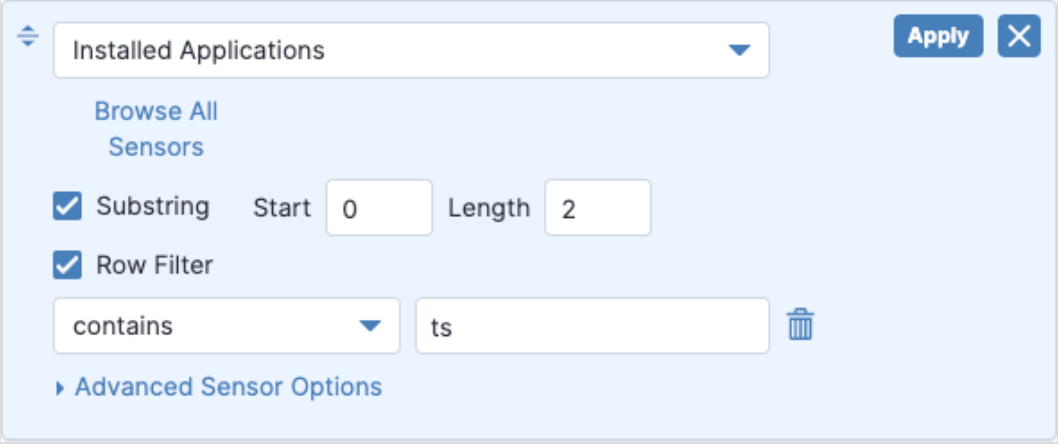
Alternatively, click **Browse All Sensors** below the sensor name field to open the **Browse Sensors** dialog and select a sensor. The bottom of the dialog displays the **Sensor Description**.



4. For a sensor that produces data across multiple **Question Results** columns, you can add filters based on column data matches. In the **Question Builder**, click **Add filter** below the sensor field to configure a filter. By default, filter matching applies to a single column, which you select in the first dropdown list below the sensor name. Note that single-column filtering works only if the sensor definition specifies column delimiters with a single character (such as "`|`"), not multiple characters (such as "`|:`"). To apply matching to all the columns for a sensor, select **Row Filter**.



You can select matching operators and specify regular expressions to match strings. To match on substrings, select the **Substring** box and specify a **Start** position (where `0` is the first position) and number of characters (**Length**).



5. (Optional) If you add a filter in the **Get the following data** or **from computers with** sections, you can click **Advanced Sensor Options** below the filter to configure additional settings. See Reference: Advanced sensor options.

6. To create the `from` clause, click one of the following buttons below **from computers with** and then click **Apply**:

   - **+ Add**: Add one or more conditions that endpoints must match. You can base the matching (**Select Attribute**) on a **Sensor** or **Computer Group** (management group or filter group).
   - **+ Grouping**: Select this option to nest a Boolean operator and then use **+ Add** to build the nested expression.

   You can configure multiple filters, including nested filters. For example, to investigate the web browsers installed on computers, you can select the Boolean **AND** or **OR** in the `from` clause to target modern browsers.

7. (Optional) Click **Advanced Question Options** and enable **Force Computer Id** if you want to convert a single-sensor, counting question into a non-counting question by forcing Tanium Clients to include the computer ID in their answers. Note that the **Question Results** page does not include the computer ID results when you select this option. Converting to a non-counting question is a workaround that resolves cases where a counting question returns the `too many results` answer. For details, see Enable or disable live updates on page 51.

8. Click **Ask Question** to issue the question.

   The **Question Results** page opens to show the answers from endpoints.

> NOTE For details and tasks relating to question results, see Managing question results on page 50.

Search endpoints

Use the Interact **Search Endpoints** field to view comprehensive information about a single endpoint as an alternative to issuing a long, complex question. Interact quickly retrieves and displays information for the **Search Endpoints** feature, even for endpoints that are currently offline, because most of the sensors that collect the information are registered by default with Tanium Data Service.

> NOTE The permissions that are required to use the **Search Endpoints** field are available to the **Administrator** reserved role, **Interact Power User** role, and **Interact Basic User** role.
>
> The **Search Endpoints** field requires Interact 2.13 or later and Reporting 1.12 or later.

The **Search Endpoints** field provides two levels of information:

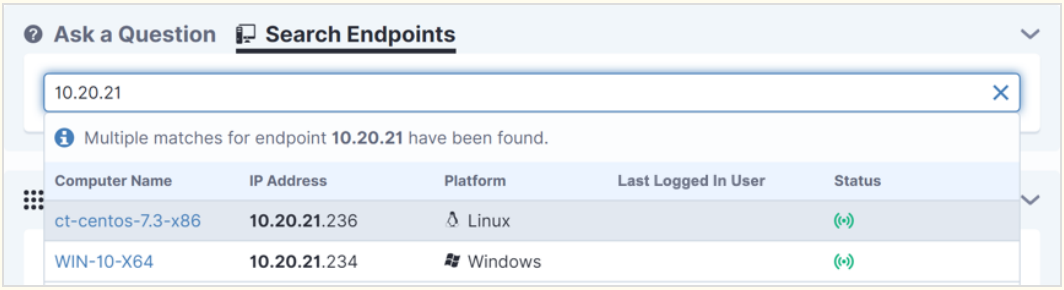
- **Basic information**: This includes the results of the following sensors: **Computer Name**, **Tanium Client IP Address**, **OS Platform**, **Last Logged in User**, and **Online** status (online or offline).
- **Detailed information**: You can open a page that shows a single endpoint view with comprehensive details from dozens of sensors. In addition to the basic information, the detailed information include data about the endpoint operating system, hardware, primary user, Tanium Client version, processors, installed applications, logical disks, network adapters, and physical disks. If the endpoint is online, you can deploy an action to it from the endpoint view page.

> TIP You can also access this information through the **Question Results** page. See View details for a single endpoint.

1. Go to the Tanium **Home** page and click **Search Endpoints**.
2. Display basic information about an endpoint by typing its computer name, Tanium Client IP address, or last logged-in user name without pressing **Enter**.

   TIP

   Type a partial string to see basic information about multiple endpoints. For example, if you type `10.20.21`, a dropdown list shows information about all the endpoints with an IP address that contains those digits.

3. Click the **Computer Name** to open the Endpoint Details page, which contains detailed information and provides additional options for exploring or managing the endpoint.

   For information about using the Endpoint Details page, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

View question history

Use the **Question History** page to manually reissue questions or view a chronology of issued questions, as well as their syntax and other details (such as issuer and expiration time stamp). By default, the **Question History** page shows questions that were issued in the past 24 hours. You can change the date range to show more entries, or apply filters to limit the entries that appear.

By default, question **Expiration** date-times are based on the **Local Time** of the system that you use to access Tanium Console, but you can switch to Coordinated Universal Time (**UTC**).

NOTE

Users require a role with the **Question History** read permission to see the **Question History** page. For the permissions that are required to load questions from the page, see Question history.

Reissue a question

To reissue a question, select the question in the grid and click **Load**. Tanium Console displays the results in the **Question Results** page.

Export question history

Export information from the **Question History** grid as a CSV file to view the information in an application that supports that format. If you have the **Administrator** reserved role, you can also export the information as a JSON file.

1. From the Main menu, go to **Administration > Content > Question History**.
2. Select rows in the grid to export information only for specific questions. If you want to export information for all questions, skip this step.
3. Click Export  .
4. (Optional) Edit the default export **File Name**.

   NOTE The file suffix (`.csv` or `.json`) changes automatically based on the **Format** selection.
5. Select an **Export Data** option: export information for all **All** questions in the grid or just for the **Selected** questions.
6. Select the file **Format**: **CSV** (default) or **JSON** (**Administrator** reserved role only).
7. Click **Export**.
   The Tanium Server exports the file to the downloads folder on the system that you used to access Tanium Console.

Copy question history details

Copy question history details to your clipboard to paste them into a message, text file, or spreadsheet. Each row in the grid is a comma-separated value string.

1. From the Main menu, go to **Administration > Content > Question History**.
2. Perform one of the following steps:
   - **Copy row information**: Select one or more rows and click Copy  .
   - **Copy cell information**: Hover over the cell, click Options  , and click Copy  .

Managing question results

Question results overview

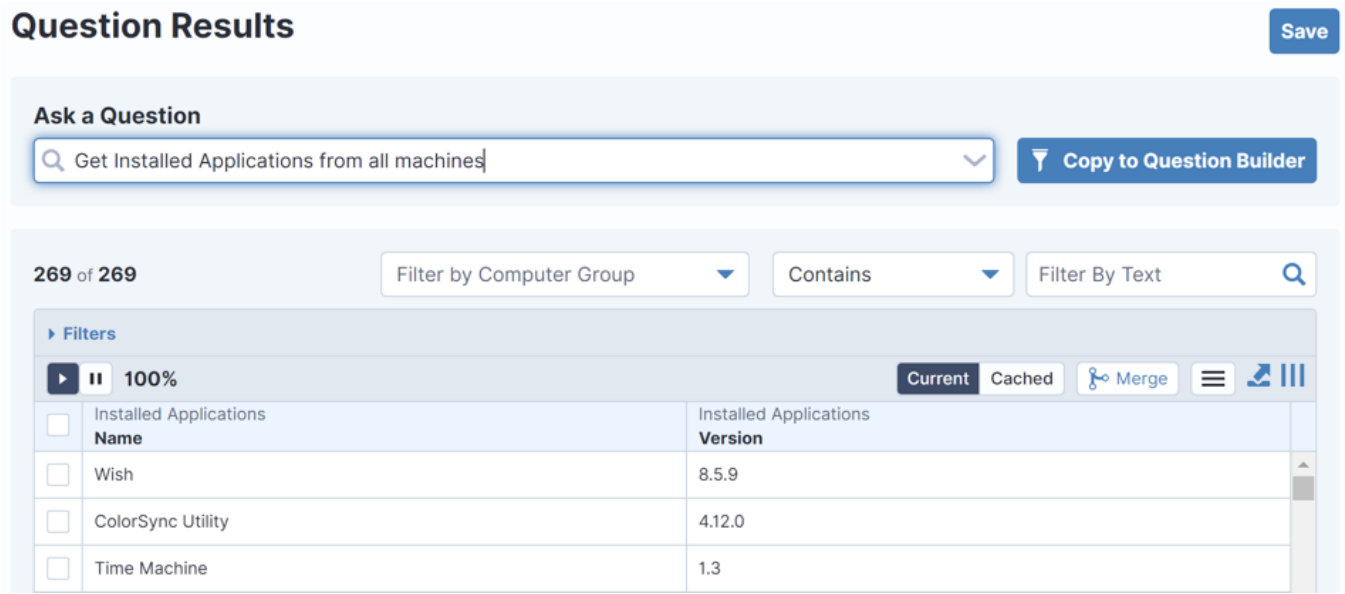
After you use Tanium Interact to issue a dynamic question, the **Question Results** page opens and displays a grid with the answers (results) from endpoints. The page facilitates analyzing the results by providing display options such as live updates, cached results, and filters. You can also use the page to retrieve additional information from endpoints by merging questions and by drilling down into the results.

Each row in the results grid is an aggregation of the endpoints that reported the same answer. For counting questions, the **Count** column shows the number of Tanium Clients with that answer, as shown in Figure 10 (for details, see Counting and non-counting questions).

When you issue a saved question or a dashboard of questions, Tanium Console opens the saved question results page or dashboard results page respectively. These pages resemble the **Question Results** page but have additional options. See Issue a saved question and Issue a dashboard of saved questions.

TIP If Tanium Clients do not answer questions, see Tanium Console User Guide: Troubleshoot question results issues.

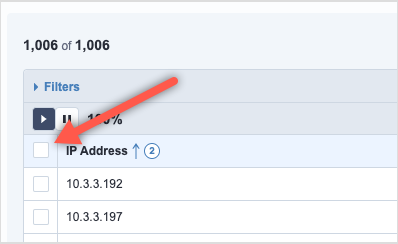
Figure 10: Question Results grid



Selecting rows

After you manipulate the grid to show the results that you want, you can deploy actions to the associated endpoints by selecting some or all of the result rows and clicking **Deploy Action**. For the full procedure, see Deploying actions.

- You can select up to 100 rows in the grid.
- To quickly select multiple consecutive result rows for drilling down, copying, exporting, or deploying actions, click the check box in the first row to include, hold down the **Shift** key, and then click the check box in the last row to include.
- Click the check box next to the header row to select 100 rows, starting with the first row that displays on the screen. If you already have rows selected, Interact only selects rows to reach the 100 limit. Click the check box again to clear any selected rows.



Enable or disable live updates

The top left of the **Question Results** grid toolbar shows the percentage of Tanium Clients that reported results. The live updates feature is enabled by default, which means Tanium Console updates the grid as more Tanium Clients report results.

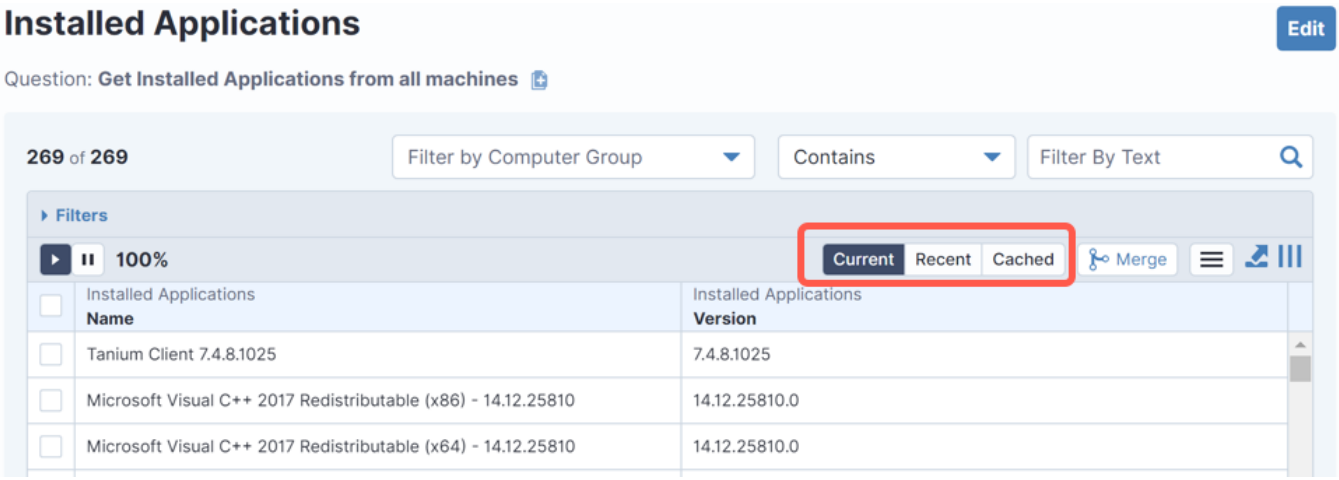
Click Pause ❚❚ to stop the grid from updating and click Play ▶ to resume updating.

TIP Even after 100% of Tanium Clients have reported, some answer rows might indicate incomplete results. To investigate incomplete results, see Troubleshoot question results issues on page 87.

Display results for online and offline endpoints

When the **Question Results** page opens, it initially displays only current results, which are answers from endpoints that were online at the moment you issued the question. However, you can also display recent or cached results that the Tanium Server stored when it queried endpoints that were previously online but are currently offline.

Figure 11: Current, recent, and cached results



The option to display stored results enables you to have a more complete view of your managed endpoints. For example, to evaluate the security state of both online and offline endpoints, you can display both current and stored results for questions about which endpoints have a critical patch applied or a particular third-party application installed. Click the button for the type of results that you want to display:

- **Current**: By default, the grid displays results only from endpoints that are currently online.
- **Recent** (saved questions only): In addition to results from online endpoints, this option includes results from offline endpoints if those results still reside on the Tanium Server after the last time the server issued that question. The server stores the results of saved questions for seven days by default. Note that the server associates recent results with specific saved questions, not with sensors. This means that even if multiple saved questions share the same sensor, the results grid might show different recent results for that sensor based on which question you issue and your computer management group permissions. Only users who have the permissions to create saved questions can view recent results.
- **Cached**: The grid displays results that the Tanium Server collects by periodically querying all managed endpoints for specific sensors. The option appears only for questions in which all the sensors are registered for collection. The server stores the results for 30 days by default. Because the server saves the results on a per-sensor basis, the grid displays the same results for a particular sensor when you issue any dynamic or saved question that uses that sensor. The grid displays only the most recent collected results. Only users with the **Data Collection Registration** write permission can register sensors. For details, see Manage sensor results collection.

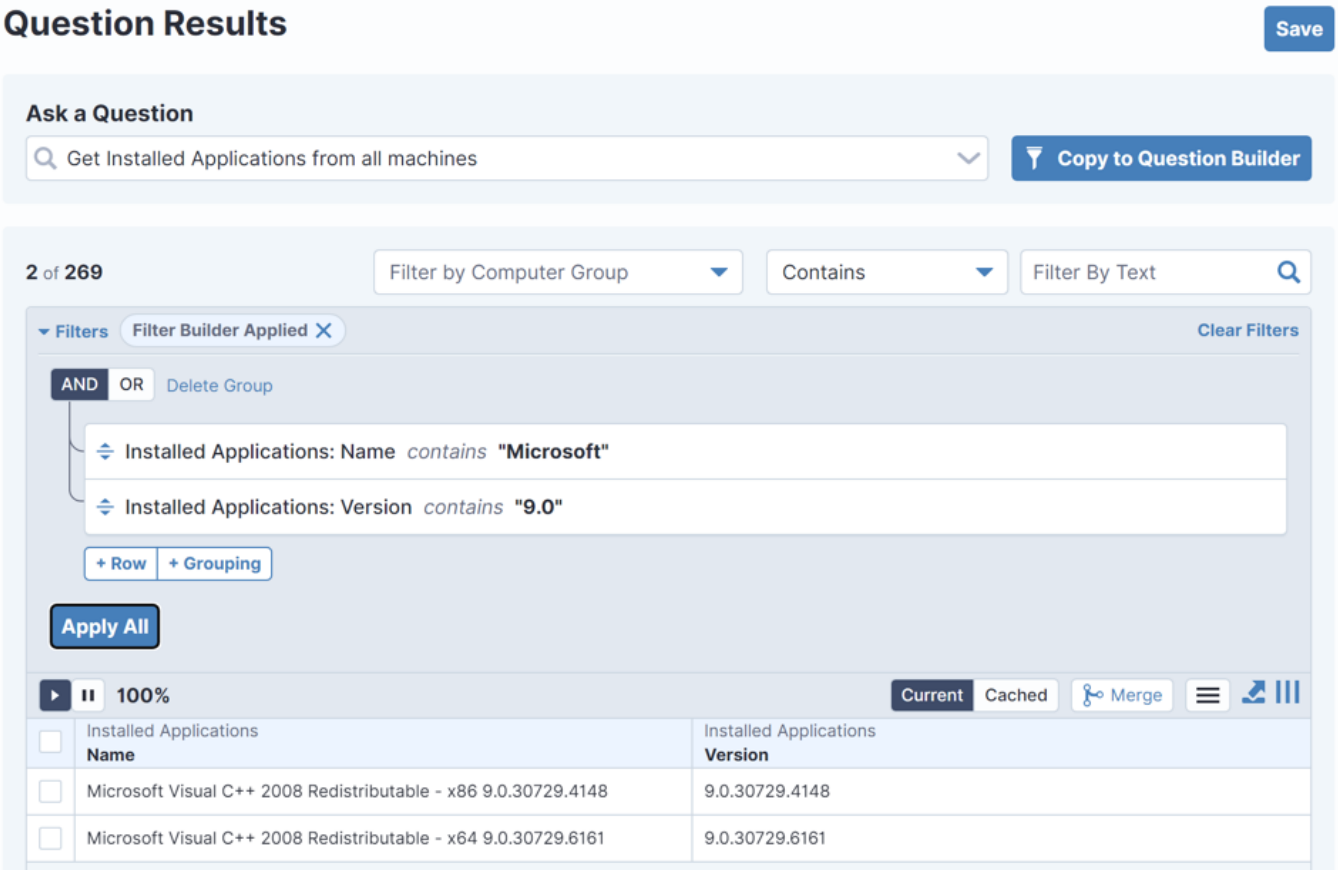
BEST PRACTICE

For offline endpoints, view **Cached** results instead of **Recent** results. For cached results, the Tanium Server more accurately identifies the responding endpoints, allows all users to view the results, and returns results for both dynamic and saved questions.

Filter question results

Use the filter controls in the header of the **Question Results** grid to display only results that match the criteria you specify.

Figure 12: Question Results grid filters



NOTE

The **Question Results** grid includes multiple grid filters. The Tanium Server combines the filters with a Boolean AND. For example, if you select a computer group filter and also configure an advanced filter, the server combines the logic of both filters.

Use a text filter

Use the **Filter By Text** field to filter the **Question Results** grid based on values in pertinent grid columns. The Tanium Server filters the grid without reissuing the question. Select the **Contains** or **Does not contain** operator, enter a search string, and click Search .

TIP

For most questions, the text filter shows matching results in any grid column. If you filter on certain cached results, values in the **Count** column are ignored by the text filter.

Use a computer group filter

After you select an entry in the **Filter by Computer Group** drop-down, the Tanium Server issues a new question with the added filter. Select **All Computers**, **No Computers**, or a user-configured computer group. If the list of computer groups is long, you can use the text filter within the **Computer Group** drop-down to filter by group name. If you save the question, the question text includes the **Computer Group** filter but not the text filter within the drop-down.

NOTE

The **Filter by Computer Group** drop-down displays only the groups that are available to your user account through assignment or inheritance (management groups) or that are assigned to a content set for which your account has role permissions (filter groups). For details, see Managing computer groups.

Use an advanced filter

Use advanced filters to filter question results based on match conditions, including column values.

1. In the header of the **Question Results** grid, click **Filters**.
2. Click one of the following buttons to add filter conditions:
   - **+ Row**: Add one or more conditions and click **Apply**.
   - **+ Grouping**: Select this option to nest a Boolean operator. Use **+ Row** or **+ Grouping** to build the nested expression and then click **Apply**.

   After you click **Apply All**, the grid refreshes.

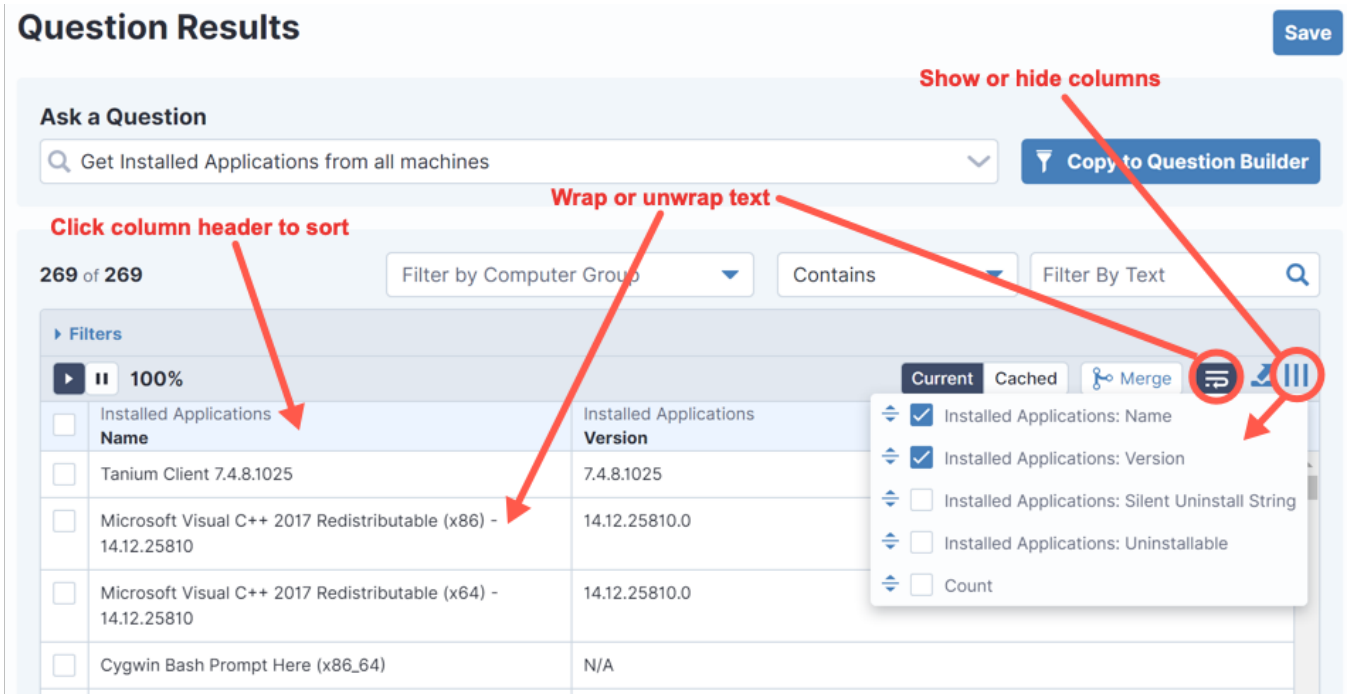
Manage row sorting, column visibility, and text wrapping for question results

To sort rows alphabetically or numerically in the **Question Results** grid based on the values in a specific column, click the column header. To perform a secondary sort, press the **Shift** key and click another column header.

To change which columns are visible in the grid, click Customize Columns in the grid toolbar and select (show) or deselect (hide) the column check boxes.

To toggle text wrapping, click Wrap or Unwrap in the grid toolbar.

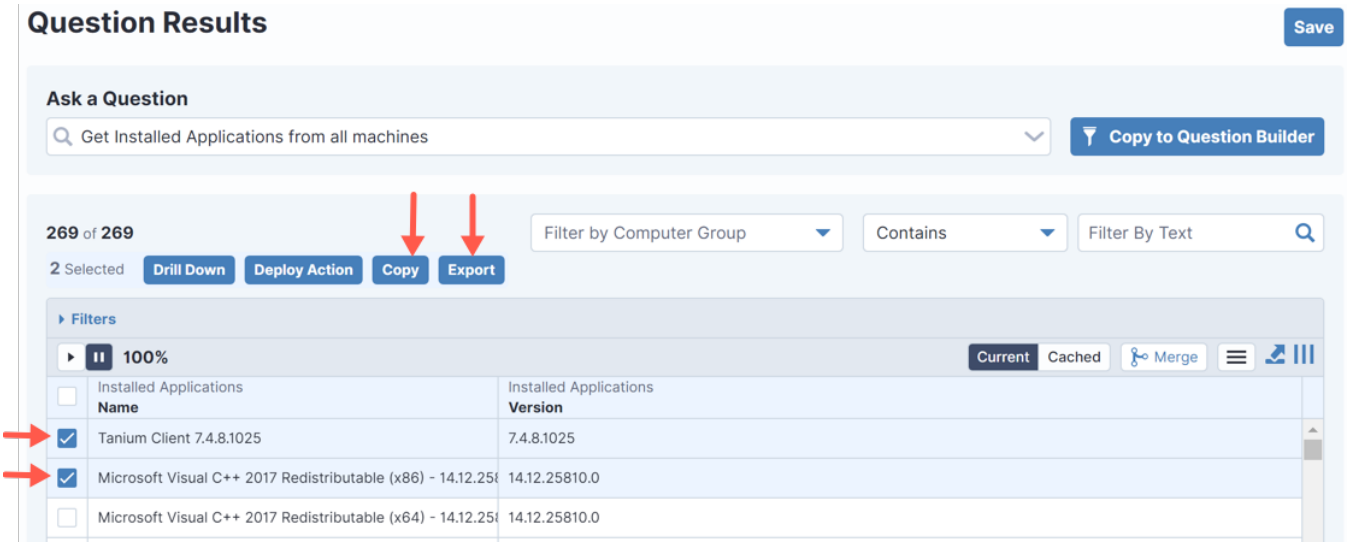
Figure 13: Question Results grid sorting, column visibility, and text wrapping controls



Export and copy question results

The **Question Results** page provides several options for copying and exporting the results grid contents. To export all results, click Export on the right side of the grid toolbar. You can also select specific results and click **Copy** or **Export** above the grid.

Figure 14: Copy or export question results



Copy question results to the clipboard

You can copy question results to the clipboard in text format. To include sensor names (displayed in the grid as column headers) in the copied text, see Set Tanium Console user preferences.

- To copy specific results, select the corresponding check boxes and click **Copy**.
- To copy the contents of a grid cell, hover over the cell, click Options, and click Copy Cell Value.
- To copy the contents of a grid cell, press the **Alt** key (Windows) or **Option** key (macOS) and click in the grid cell. Tanium Console then displays a message indicating that the clipboard has a copy of the cell contents. This operation works for most grids in Tanium Console.

Export question results

You can export question results to a CSV file.

1. Select one of the following export options:
   - To export specific results, select the corresponding check boxes and click **Export**.
   - To export the complete results, click Export in the header of the grid.
2. Enter a **File Name** for the CSV file.
3. To include sensor names (grid column headers) in the .csv file, select **Include headers in export**.
   If you selected only a subset of the results to export, click **Export** and skip the remaining steps, which describe options that are available only if you are exporting the complete results.
4. Select how the CSV file displays results for questions where one sensor generates multiple results for each responding endpoint. As an example, for the question `Get Computer Name and High CPU Processes[5] from all machines`, the High CPU Processes sensor returns five processes for each endpoint. By default, the file displays one row for all the results that the sensor generated for an endpoint. For the example question, this would mean each row lists all the top five processes for each endpoint (identified by Computer Name).

Computer Name	High CPU Processes[5]
SQL1.tam.local	sqlservr.exe TaniumClient.exe cmd.exe conhost.exe cscript.exe
TS1.tam.local	TaniumReceiver.exe chrome.exe svchost.exe cmd.exe conhost.exe

To display a row for each result that a sensor generates, select **Flatten rows**. For the example question, a flattened export results in five rows per endpoint: one row for each process that the High CPU Processes sensor returned. Note that this option works only if just one sensor in the question has multiple results.

Computer Name	High CPU Processes[5]
SQL1.tam.local	sqlservr.exe
SQL1.tam.local	TaniumClient.exe
SQL1.tam.local	cmd.exe
SQL1.tam.local	conhost.exe
SQL1.tam.local	cscript.exe

If you select **Flatten rows**, the **Fail on errors** check box appears. Selecting **Fail on errors** causes the export to fail for all results if any result includes multiple columns (sensors) with more than one value. In the example, it would be an error if a single endpoint returned multiple results for both Computer Name and High CPU Processes. By default, **Fail on errors** is disabled, which means the export proceeds despite such errors. However, the output includes errors without flattening the affected results; the output does not use separate lines to account for multiple columns with multiple values.

5. Click **Export**.

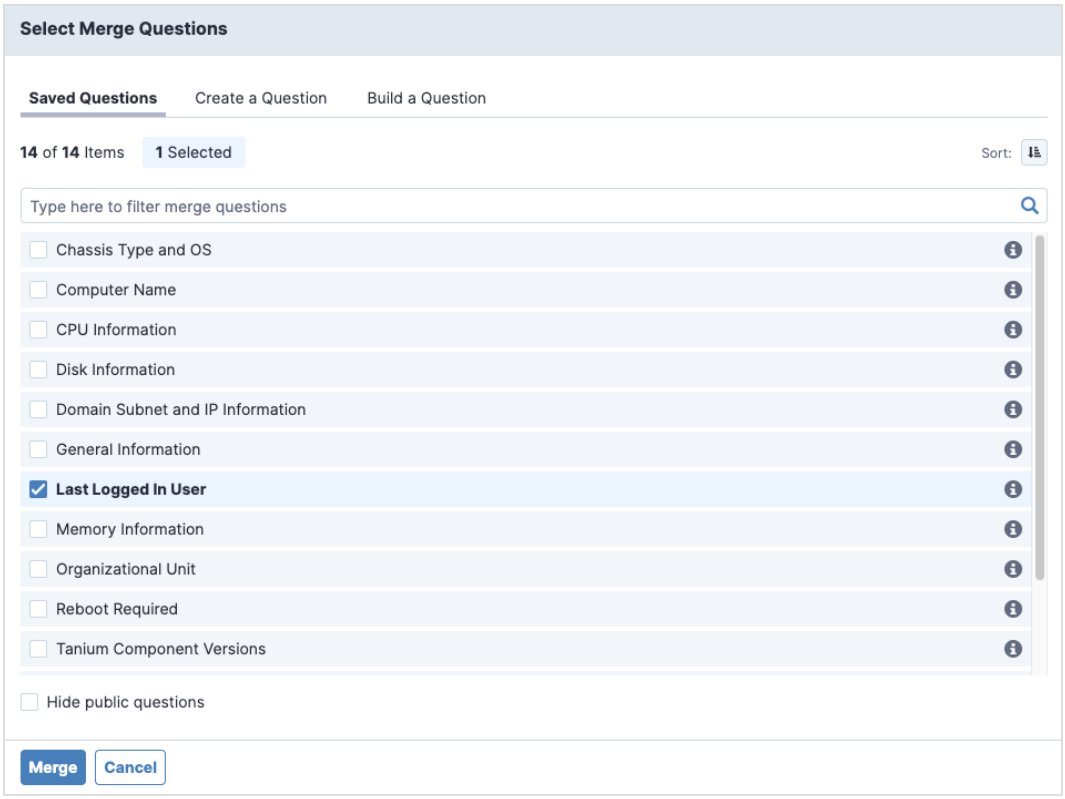
Merge questions

Question results often lead to additional questions. For example, the results of a question that returns computer names and running processes might indicate that some endpoints are running a suspicious process. You can *merge* the initial question with another question to learn more information, such as the last logged-in user. The Tanium Server issues the merge question in the background, and Tanium Console re-displays the **Question Results** grid with one or more additional columns containing results for the sensors that the merge question specified.

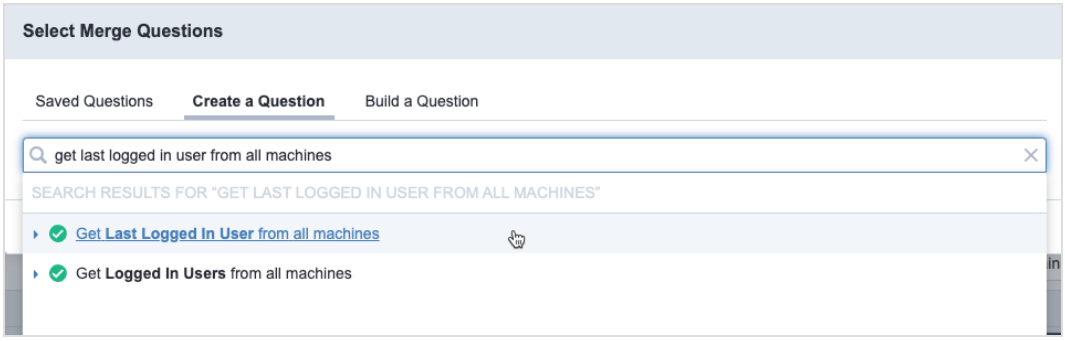
Merge operations automatically apply to all results. You do not need to select grid rows before merging.

1. Click **Merge** on the right side of the **Question Results** grid toolbar to open the **Select Merge Questions** dialog.
2. Use one of the following tabs to add questions and then click **Merge**:
   - **Saved Questions**: Lists saved questions that are assigned to content sets for which you have **Saved Question** read permission. The questions must also have the Display this question in the list of questions that are available to merge setting enabled.

To filter the list so that it includes only saved questions with **Visibility** is set to **Only the Owner and Admins can see this object**, select **Hide public questions**.

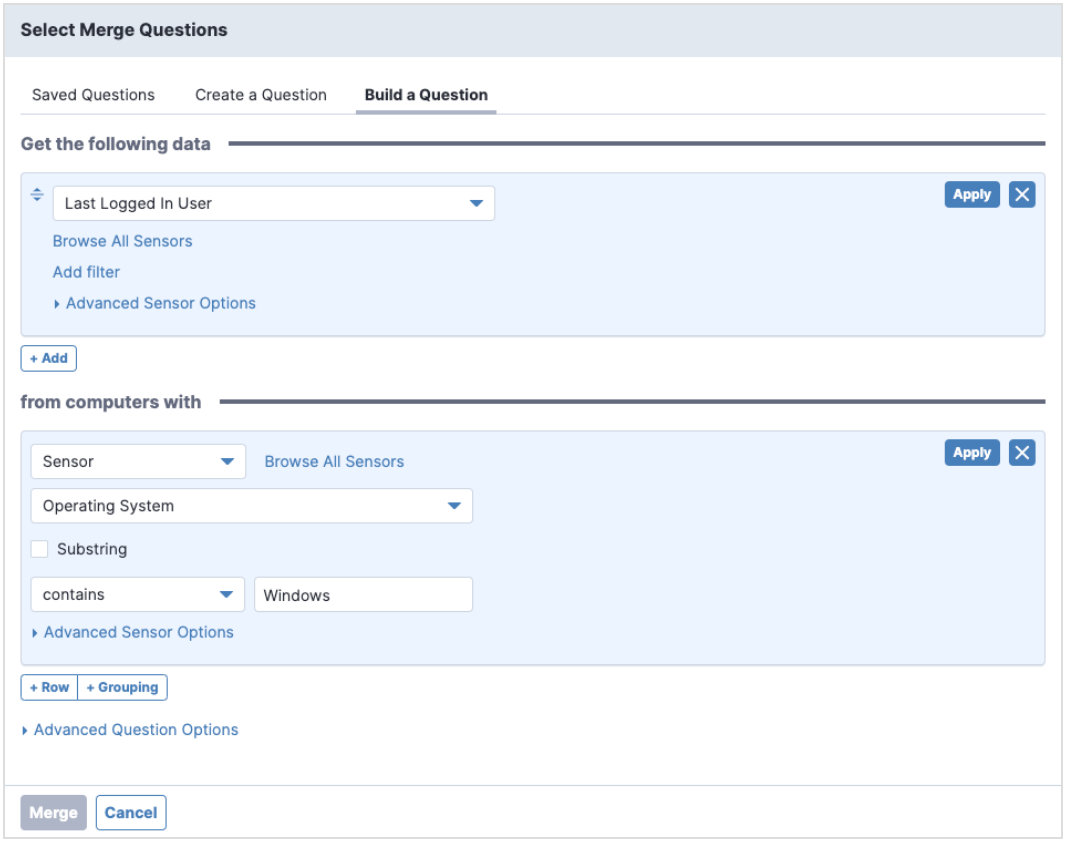


- **Create a Question**: Enter a question using the same syntax as in the Interact **Ask a Question** field (see Issue a question through the Ask a Question field).

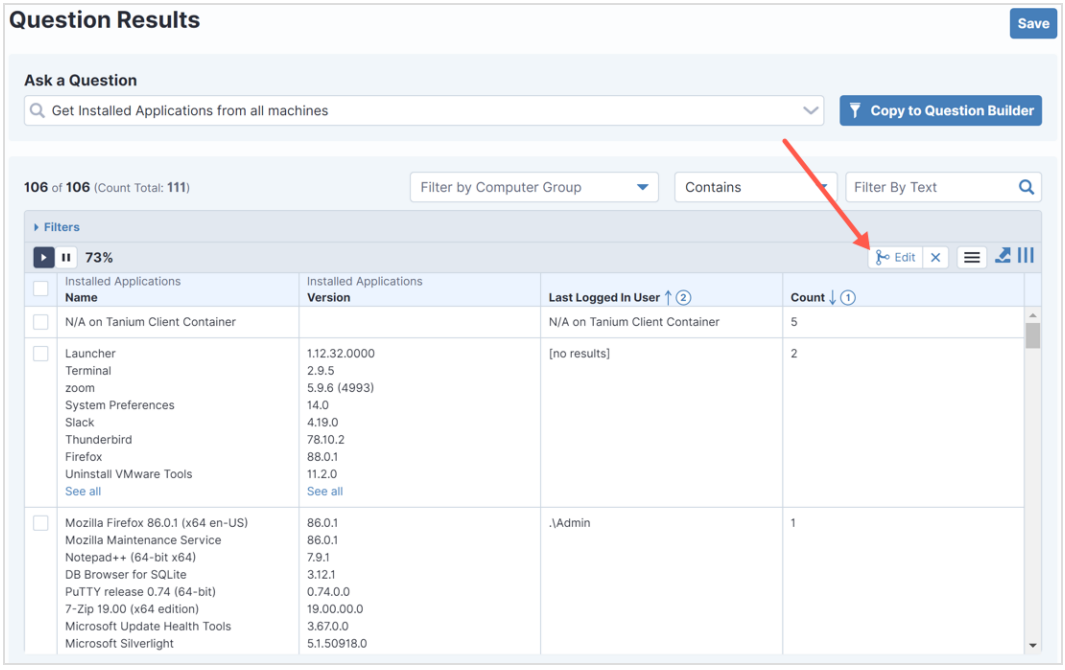


- **Build a Question**: Construct a question using the same fields as in the Interact **Question Builder** (see Issue a question through the Question Builder).

  Notice that you add sensors to the `get` clause but you do not add filters to the `from` clause. The `from` clause is automatically based on the rows that you selected in the **Question Results** grid when you clicked **Merge**.



After you click **Merge**, the **Question Results** grid displays the updated results. You can use the **Edit** button in the grid header to modify the merge settings.



Drill down

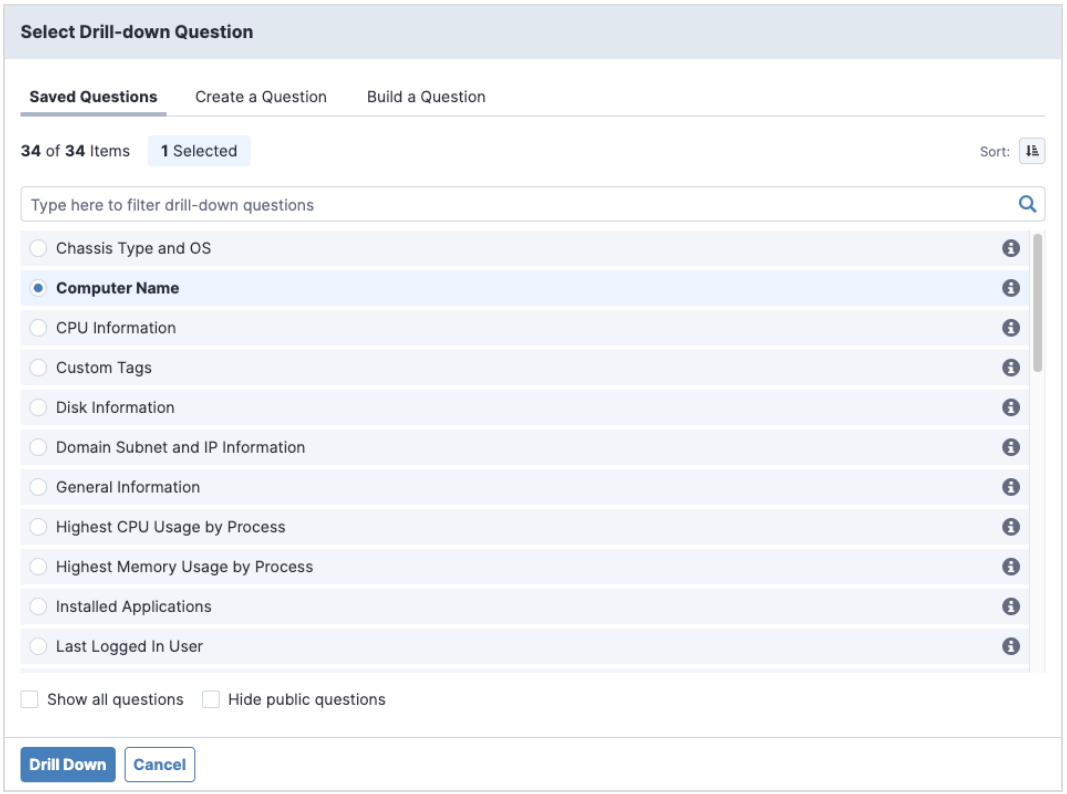
In the **Question Results** grid, you can drill down into selected results to retrieve more information from the associated endpoints. Adding a drill-down question effectively means using its sensors to filter the selected results. A typical use case is targeting a smaller group of endpoints for an action. For example, you might initially issue a question that returns a list of chassis types and operating systems for all endpoints. To see the identities of endpoints that return specific results, you can drill down into those results with the **Computer Name** sensor.

1. In the **Question Results** grid, select the results for which you want more information and then click **Drill Down**.
2. Use one of the following tabs to specify a drill-down question and then click **Drill Down**.

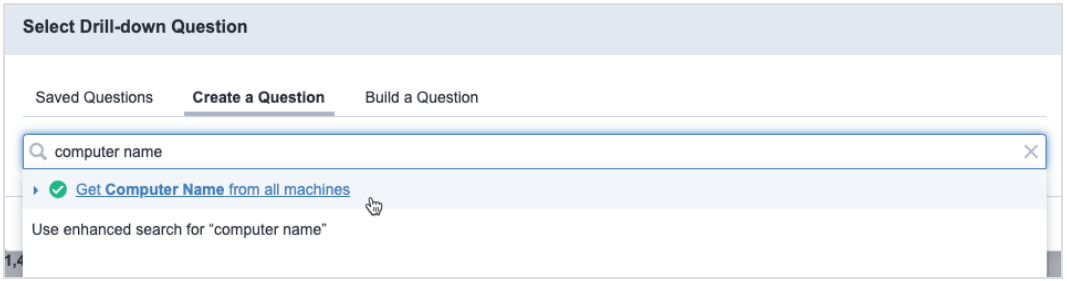
> TIP
> If the selected **Question Results** include the value of a parameterized sensor and your drill-down question uses a sensor with a matching parameter, the **Select Drill-down Question** dialog automatically populates that parameter with the value from the selected results.

- **Saved Questions**: Lists saved questions that are assigned to content sets for which you have **Saved Question** read permission. By default, the list includes only questions that have the Display this question in the list of questions that are available for drilling down setting enabled. To include questions that do not have the setting enabled, select **Show all questions**.

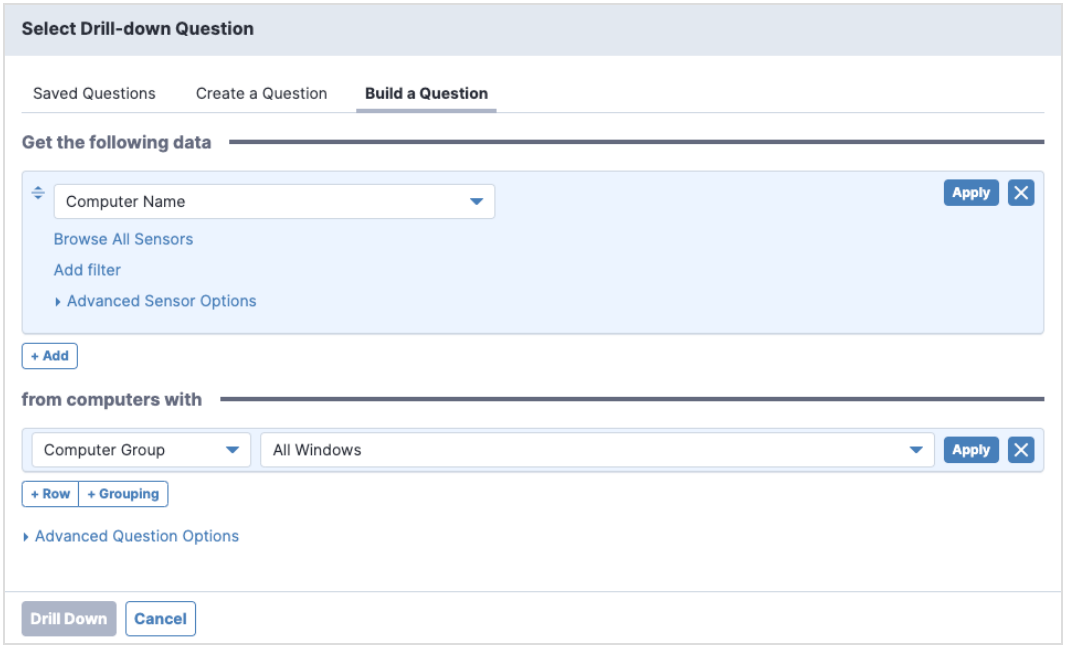
TIP To filter the list so that it includes only saved questions with **Visibility** is set to **Only the Owner and Admins can see this object**, select **Hide public questions**.



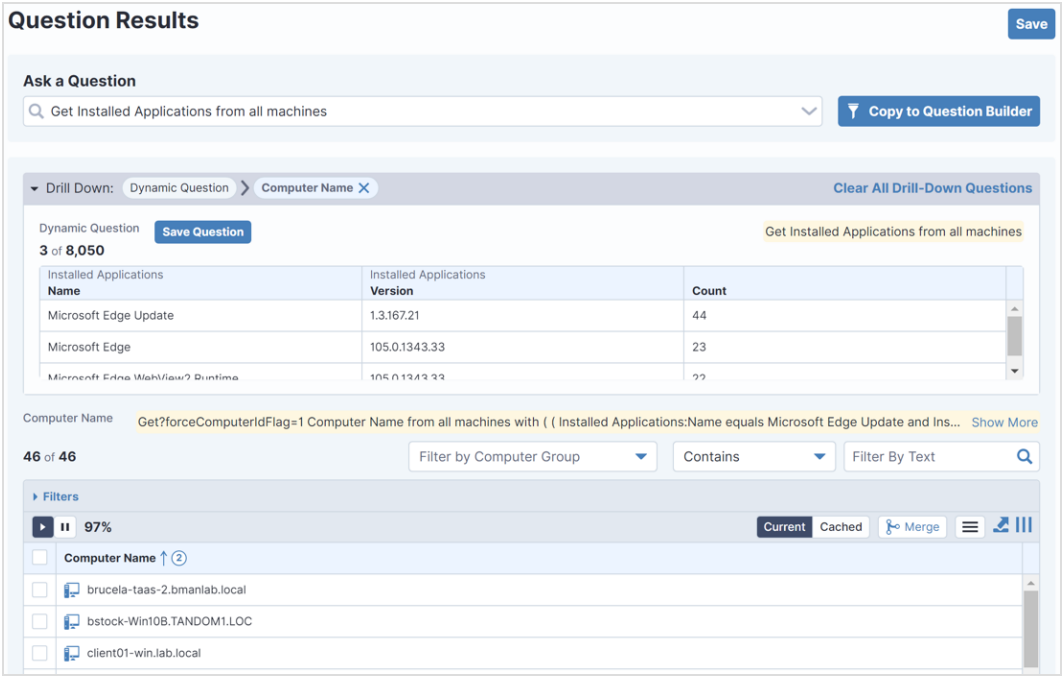
- **Create a Question**: Enter a question using the same syntax as in the Interact **Ask a Question** field (see Issue a question in natural language).



- **Build a Question**: Construct a question using the same fields as in the Interact **Question Builder** (see Issue a question through the Question Builder).



After you click **Drill Down**, Interact shows the progression of results, including a new **Question Results** grid for the drill-down question. You can then drill down further, deploy an action, save the question, or click **Copy to Question Builder** for further refinement.



View details for a single endpoint

When you analyze question results from endpoints, you might want to explore additional information about a particular endpoint. For example, if an endpoint returns `100%` for a question with the **CPU Consumption** sensor, you might want to see details about the processors on that endpoint. Interact provides a single endpoint view feature that quickly retrieves and displays the information, even for endpoints that are currently offline, because most of the sensors that collect the information are registered by default with Tanium Data Service.

NOTE

The endpoint details that are available for viewing depend on the installed Tanium solution versions:

- View endpoint details through Reporting on page 63: Requires Interact 2.13 or later and Reporting 1.12 or later.
- View endpoint details through Asset on page 65: Requires Asset 1.7 or later and a minimum Interact version of 2.1.

If Interact, Reporting, and Asset are all at the required versions, the endpoint details are available only through Reporting, not Asset.

View endpoint details through Reporting

From the **Question Results** page, you can access two levels of information about an endpoint:

- **Basic information**: This includes the results of the following sensors: **Computer Name, Tanium Client IP Address**, **OS Platform**, **Last Logged in User**, and **Online** status (online or offline).
- **Detailed information**: You can open a page that shows a single endpoint view with comprehensive details from dozens of sensors. In addition to the basic information, the detailed information include data about the endpoint operating system, hardware, primary user, Tanium Client version, processors, installed applications, logical disks, network adapters, and physical disks. If the endpoint is online, you can deploy an action to it from the endpoint view page.

NOTE

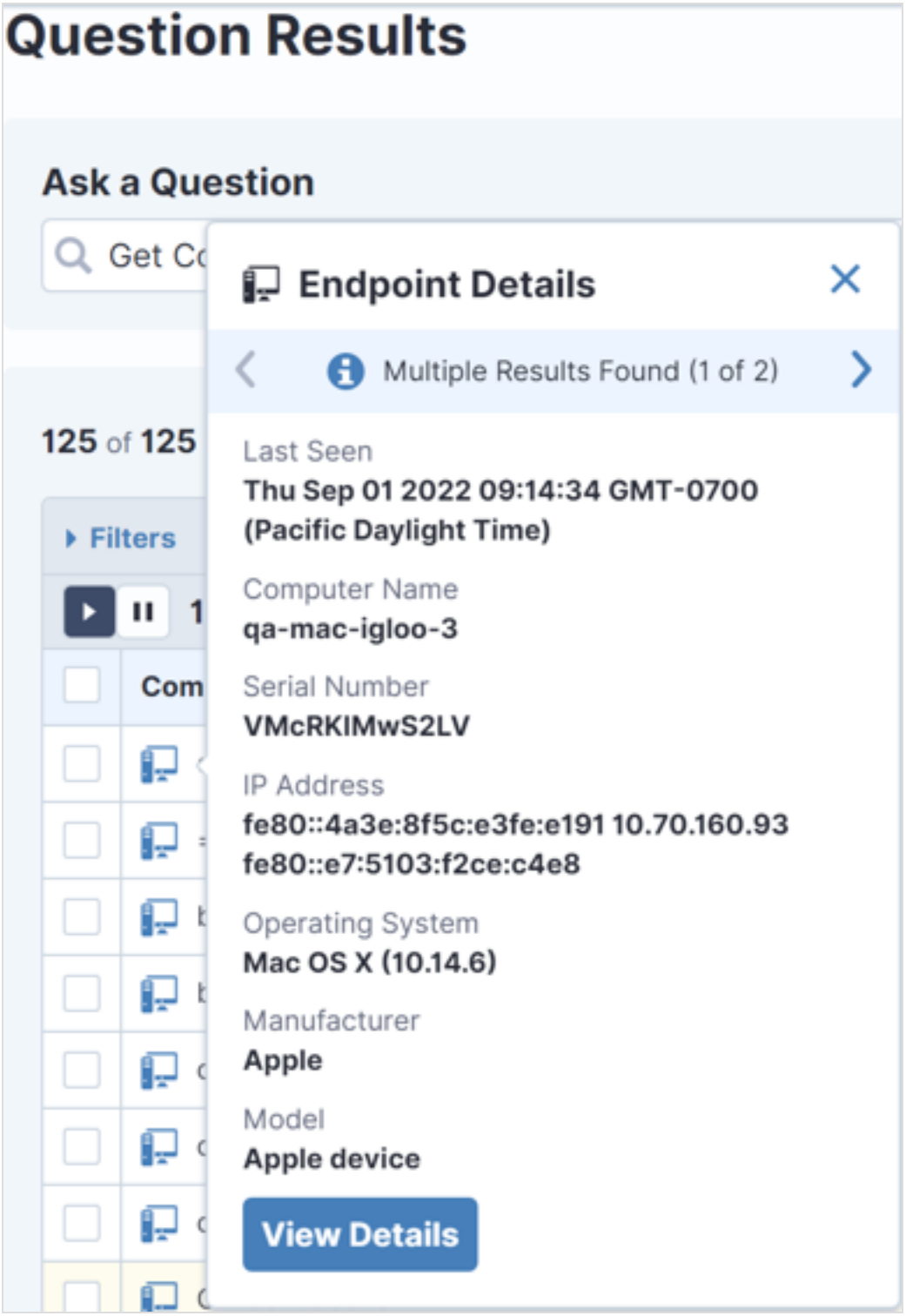
The permissions that are required to view endpoint details through Reporting are available to the **Administrator** reserved role, **Interact Power User** role, and **Interact Basic User** role.

TIP

To access this information without issuing a question, use the **Search Endpoints** field on the Tanium **Home** page. See Search endpoints.

1. Issue a question that includes the **Computer Name, Computer ID, or Tanium Client IP Address** sensor.
2. In the **Question Results**, click an endpoint icon to see the details for that endpoint.
   An **Endpoint Details** dialog opens to display the basic information. If multiple endpoints have the same **Computer Name**,

Tanium Client IP Address, or **Last Logged in User**, click Previous ❮ or Next ❯ in the **Multiple Results Found** banner to find the details for a specific endpoint.



3. Click the **View Details** to open the Endpoint Details page, which contains detailed information and provides additional options for exploring or managing the endpoint.

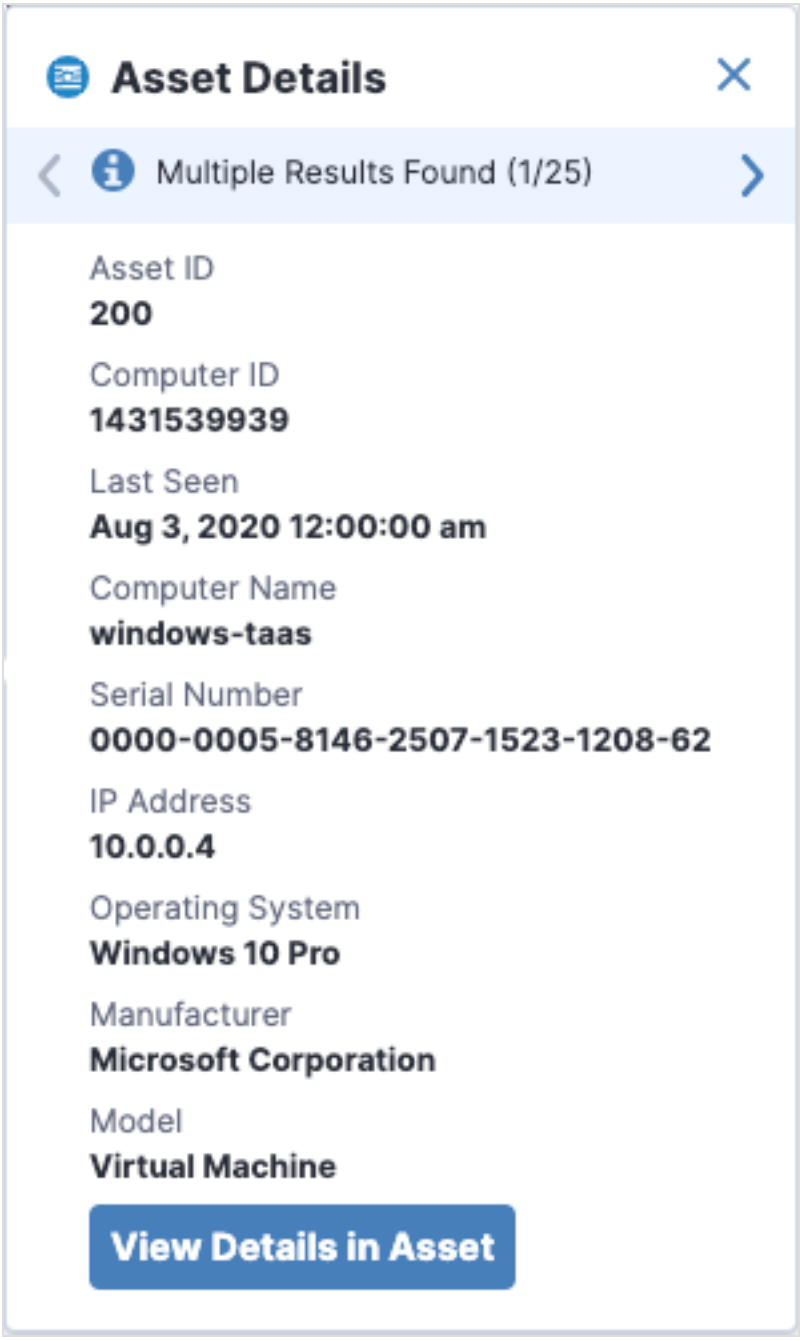
   For information about using the Endpoint Details page, see Tanium Reporting User Guide: Viewing and managing a single endpoint.

View endpoint details through Asset

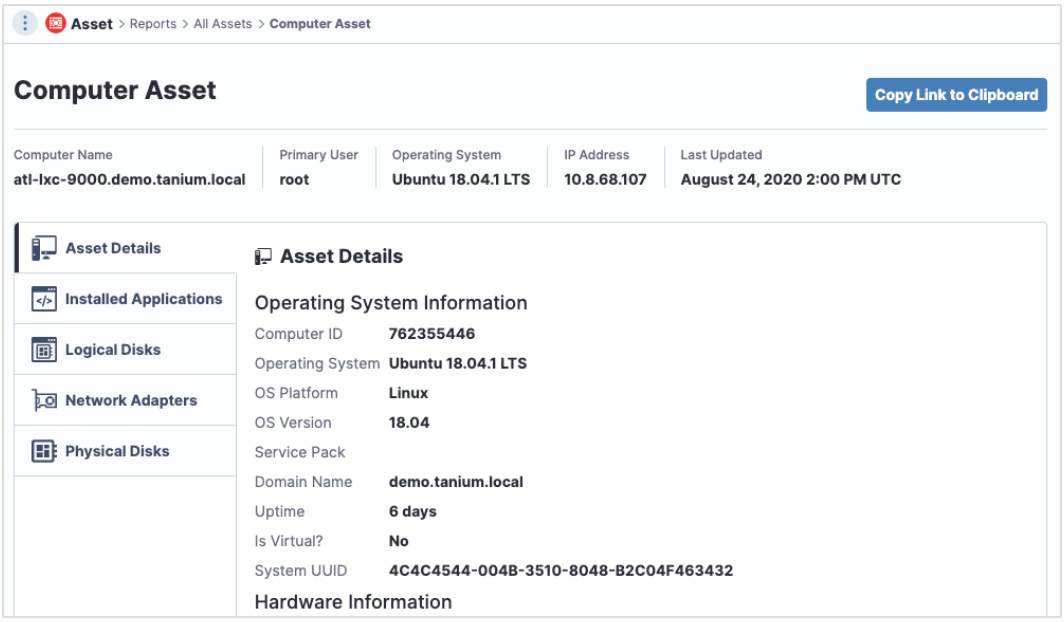
Tanium™ Asset stores numerous details about each endpoint that might be useful for your operational or monitoring activities. For example, you might want to see CPU and storage details about an endpoint before deploying an action to it. If you installed Asset version 1.7 or later and you sign in to Tanium Console as a user with the **Asset Report** read permission, you can see those details through the **Question Results** grid without issuing additional questions that consume more bandwidth and processor resources.

1. Issue a question that includes any of the following sensors:
   - Computer Name
   - Computer ID
   - Tanium Client IP Address
   - Asset Computer Serial Number
   - Asset Primary User Details
2. Click the Asset icon for an endpoint in the **Question Results.**

An **Asset Details** dialog opens to display a summary of the Asset details for that endpoint. If the Asset database has multiple entries for the same endpoint, click Previous or Next in the **Multiple Results Found** banner to find the details for a specific endpoint.



3. Click **View Details in Asset** to see all the Asset details for an endpoint. Asset then opens the **Computer Asset** report for the endpoint.



Deploying actions

After you use Tanium Interact to issue a question, analyze the question results, and determine which endpoints require administrative action, you can deploy actions to those endpoints.

NOTE For the user role permissions required to deploy actions, see User role requirements on page 27.

IMPORTANT Do not deploy an action unless you completely understand its scope, impact on an individual endpoint, and impact on the environment given the number of targeted endpoints. Furthermore, be sure your organization has authorized you to perform the action. Some organizations require a second user to review and approve actions. See Tanium Console User Guide: Managing action approval.

1. Select a method to initiate action deployment based on how many actions you want to issue, whether they are recurring (scheduled) or non-recurring (unscheduled), and whether they have similar settings:

   - **Issue a new action**: You can deploy only one new action at a time. To start, issue a dynamic question (see Issue a question through the Ask a Question field on page 41) or Reissue a saved question on page 81 (required for a policy action). Then select rows (up to 100) in the **Question Results** page for the endpoints that require the action, click **Deploy Action**, and proceed to the next step.

     NOTE You can also deploy a new action from other Tanium Console pages:

     - **Administration > Configuration > Client Status** page: See Tanium Console User Guide: Deploy actions to remediate client registration or connectivity issues.
     - **Administration > Permissions > Packages** page: See Tanium Console User Guide: Deploy actions from the Packages page.

     For details about policy actions, see Tanium Console User Guide: Policy action.

   - **Issue existing actions**:

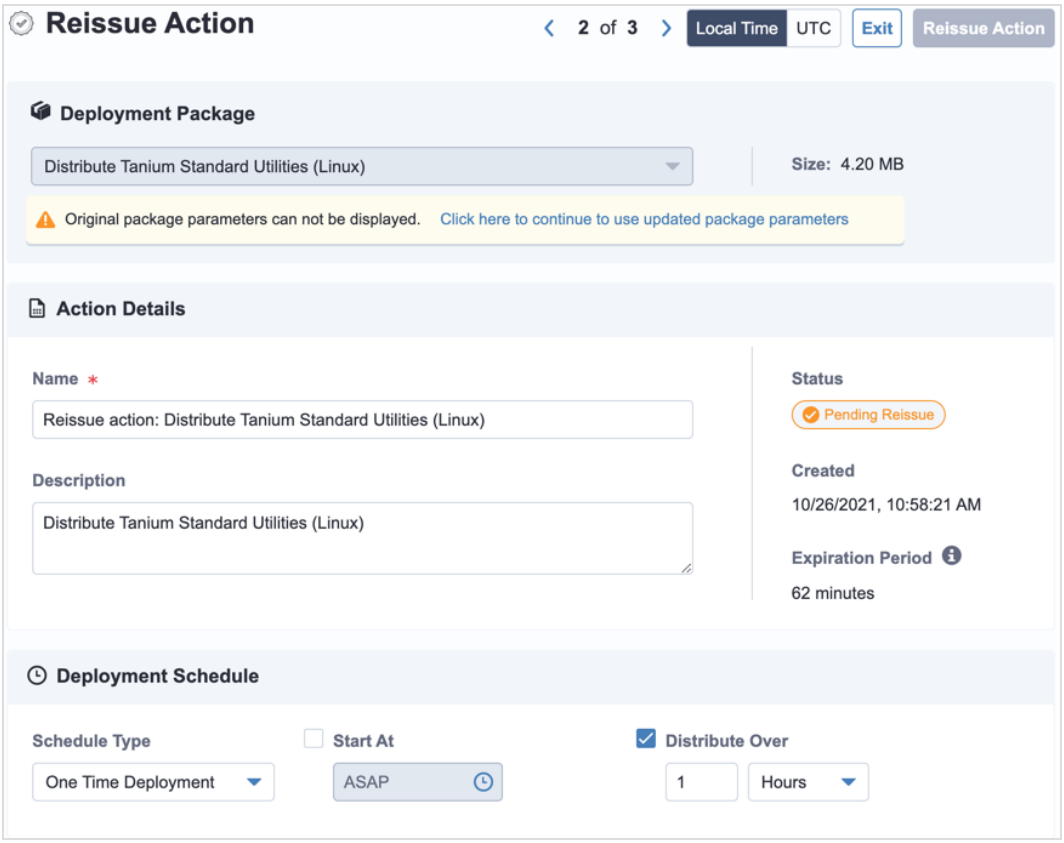
     a. Go to the **Administration > Actions** page that lists the actions you will issue:

        - To issue scheduled or unscheduled actions that were previously issued, go to **Administration > Actions > Action History**.
        - To immediately issue scheduled actions that are configured with a future start date, go to **Administration > Actions > Scheduled Actions**.

b. Select one or more actions and perform one of the following steps:

- To re-issue a single action, or to re-issue multiple actions that each require a different start time or distribution period, click **Reissue** and proceed to the next step.
- To re-issue multiple actions with the same start time and distribution period, select **More > Bulk Reissue**, specify the time standard (**Local Time / UTC**), **Start At**, and **Distribute Over** values (see Table 8), click **Confirm**, and skip the remaining steps. This option is for a one-time deployment only. If you select multiple recurring actions, the Tanium Server creates copies of the actions with their **Schedule Type** set to **One Time Deployment**.

2. Configure the following settings. If you are issuing multiple actions, use the ‹ and › widgets to navigate among the pages for each action.



NOTE

If you save an action with **Start At** and **Re-issue every** values and subsequently clear those settings instead of specifying new values, the Tanium Server discards the changes. To stop deploying an action, disable or delete it. See Tanium Console User Guide: Manage scheduled actions.

Table 8: Action settings

Settings	Guidelines
Deployment Package	Select a package from the dropdown list or enter a search string to find a package by name. You might have to configure additional settings based on your selection: • **Parameterized package**: Configure any package parameters. For example, if you select the **Set Tanium Server Name List** package, you must enter the **Server Name List**. For details, see Tanium Console User Guide: Example: Parameterized packages. • **Sensor-sourced package**: If the package has a sensor variable in its name, the Tanium Server creates a separate action for each unique value that the sensor returns among the question results that you selected for the action. For example, if the package name includes the sensor **Computer Name**, the action deployment workflow automatically creates an action for each endpoint in the selected results. For details, see Tanium Console User Guide: Package settings. • **Updated package**: If you are re-issuing or editing an action, you cannot change the **Deployment Package** and any package parameters are read-only by default. However, if the package settings changed after the action was last issued or saved, clicking **Update Source Package** makes the action use the latest version of the package and enables you to update parameter values. Click **Revert Source Package** if you want to revert to the default behavior of using the same package version and parameter values as when the action was last issued or saved. If Console cannot show the original package settings, a link below the **Deployment Package** prompts you to **Click here to continue to use updated package parameters**. For more information, see Tanium Console User Guide: Update action packages.
Local Time / UTC	Select a time standard for the **Start At** and **End At** date-times: • **Local Time** (default) is local to the system that you use to access Tanium Console. • **UTC** is Coordinated Universal Time.
Name	Specify a name to identify the action. The name appears in the record for the action on the **Scheduled Actions**, **Action History**, and action approval pages.
Description	(Optional) Enter a description helps other users understand the purpose of the action.
Status	This read-only setting appears when you create or reissue an action, and indicates whether the action is **New** or **Pending Reissue**.
Created	This read-only setting appears when you reissue or edit an action, and indicates the date and time when the action was created.

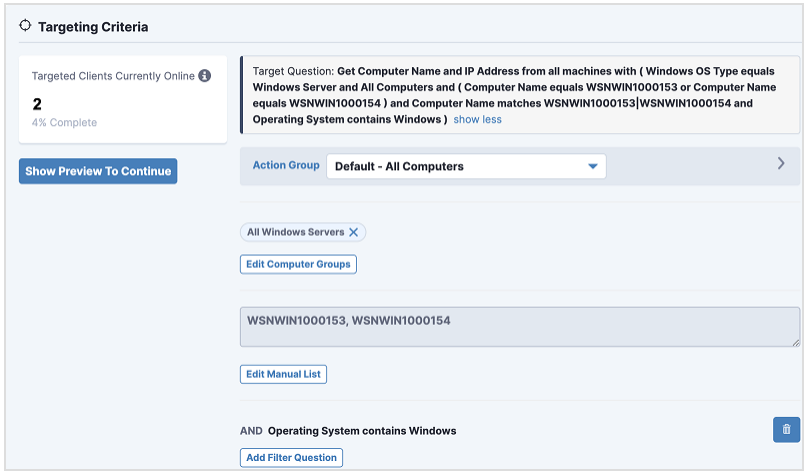
Table 8: Action settings (continued)

Settings	Guidelines
Expiration Period	This read-only setting indicates when the action expires. The value is the larger result of the following calculations: • The sum of the command and download timeout values in the selected package. See Tanium Console User Guide: Command Timeout and Download Timeout. • The sum of the package **Command** timeout and optional Distribute over on page 72 action setting. The expiration applies to each deployment of a recurring action but does not change the schedule settings (**Reissue Every**, **Start At**, and **End At**).
Schedule Type	Select one of the following options: • **One Time Deployment**: Deploy the action only once. • **Recurring Deployment**: Schedule the action to deploy at intervals (**Re-issue every**) over a specified period (from the **Start At** to **End At** date-times). This option is required for policy actions.
Re-issue every	This setting appears only if you set the **Schedule Type** to **Recurring Deployment**. Scheduling the action to repeat at intervals is useful when: • Action approval is required and you are not certain that an approver will approve the action before its initial deployment expires. • You want to deploy software or configuration updates to endpoints that might not be online during the initial deployment but that you expect to be online at some point between the **Start At** and **End At** dates. • The action is a continual hygiene practice. For example, you want to check periodically that a Tanium Client service is running or a client configuration has a particular value. Specify a number and unit: **Minutes**, **Hours**, **Days**. NOTE The **Re-issue every** interval must exceed the action **Expiration Period**.

Table 8: Action settings (continued)

Settings	Guidelines
Start At / End At	By default, actions that do not require approval deploy as soon as you click **Deploy Action** at the bottom of the **Action Deployment** page, but you can set a **Start At** date-time to override the default. For example, you might want deployment to start during a maintenance window for the targeted endpoints. Note the following behavior when action approval is enabled (see Tanium Console User Guide: Enable or disable action approval): • If you omit a **Start At** time, the action deploys immediately after it is approved, provided other action conditions do not preclude the Tanium Server from deploying it. • If you specify a **Start At** time, the action deploys at the next start time following approval. For example, if you set the action to deploy daily at 1:00 am and a user approves it at 2:00 am, the action deploys the next day at 1:00 am. The **End At** setting appears only if you set the **Schedule Type** to **Recurring Deployment**. Configure the setting if you do not want to re-deploy the action indefinitely. For example, you might want to stop deployment before the end of a maintenance window for the targeted endpoints. BEST PRACTICE Specify an **End At** date-time unless you are sure that you want to re-deploy the action indefinitely. If you are not sure, configuring the schedule to end in six months is better than running indefinitely.
Distribute over	The Tanium Server distributes actions to endpoints in batches. The **Distribute Over** option randomizes the distribution over the specified period to prevent spikes in network traffic or other resource consumption. For example, an action that depends on a sensor that queries Active Directory (AD) might cause a flood of traffic to the AD server unless the action is distributed over time. Similarly, an action that targets endpoints in a virtual machine farm might exhaust the shared CPU or memory resources if all endpoints simultaneously run a resource-intensive program. Specify a number and unit: **Minutes**, **Hours**, **Days**.

Table 8: Action settings (continued)

Settings	Guidelines
Targeting Criteria	Configure which endpoints to target for the action. By default, the action targets all endpoints that match: • The **Target Question**, which is initially based on the rows that you selected in the **Question Results** page when you clicked **Deploy Action** there. The **Target Question** updates automatically when you change other targeting criteria. • The predefined **Default - All Computers** action group, which includes all managed endpoints unless you changed the group membership before initiating the action deployment. You can also select a different **Action Group**. Optionally, refine the targeting by adding: • **Computer groups**: Click **Add Computer Groups**, select one or more computer groups, and click **Save**. • **Manual list**: Enter a comma-separated list of endpoints by computer name or IP address and click **Save**. • **Filter question**: Enter a question to target endpoints that return results and click **Save**. The Tanium Server applies a Boolean AND to the criteria that you specify. For a recurring action, only the endpoints that match the latest results of the **Target Question** will perform the action. 

3. Click **Show Preview to Continue** and review the affected endpoints.
4. Perform one of the following steps:
    - If you are issuing or reissuing the action, click **Deploy Action**.
    - If you are editing the action, click **Save Action**.

5. If the number of **Estimated clients affected** exceeds the configured threshold (the default is 100), enter the estimated number and click **Confirm**. The Tanium Server enforces this confirmation step to ensure that you understand the impact that an action will have on your network.

   TIP To change the threshold that controls whether Tanium Console prompts users for the **Estimated clients affected**, go to **Administration > Configuration > Settings > Platform Settings** and edit the **Prompt Estimate Threshold** setting. Note that changing the value to 0 causes Tanium Console to prompt users whenever they deploy actions regardless of the number of affected endpoints.

6. Perform one of the following steps to review the action status based on if the action requires approval.

   - **Approval not required**: Confirm that the action produces the expected results on the **Action Status** page, which opens automatically unless you specified a future **Start At** value in the action configuration. An action with a future **Start At** value appears in the **Scheduled Actions** page. For scheduled actions, wait until deployment starts and then check the status in the **Action History** page.
   - **Approval required**: Confirm that the action appears in the **Scheduled Actions** page. The action remains in a pending state until a user approves it, as described in Tanium Console User Guide: Approve pending actions. After the action is approved and deployment starts, check the action status in the **Action History** page.

   NOTE For details about the **Action Status** page and the steps to access it from the **Action History** page, see Tanium Console User Guide: View action status.

   Non-recurring actions that you deploy immediately appear only in the **Action History** page, not the **Scheduled Actions** or action approval pages. See Tanium Console User Guide: Manage actions that are completed or in progress.

TIP On the **Scheduled Actions** page, the **Policy** column displays `Yes` for a policy action. To show the column, click Customize Columns and select **Policy**. The **Next Issue Time** column, which is visible by default, displays `if applicable` for a policy action because that type of action deploys only if one or more endpoints returns results for the associated saved question at the next interval.

To troubleshoot action deployment issues, see Tanium Console User Guide: Monitor actions.

Managing saved questions

Saved questions are questions that you can store on the Tanium Server as configuration objects and reissue without entering them in the Interact **Ask a Question** field or **Question Builder**. For an overview of saved questions and related concepts, see Saved questions on page 17.

Use the Interact **Overview** page to perform the following actions:

- View, issue, create, and edit saved questions.
- Move questions between content sets.
- Define categories and dashboards, and assign saved questions to them.
- View and select favorite categories, dashboards, and saved questions.

For details about the user roles and permissions required to manage saved questions, see User role requirements on page 27.

User-specific saved questions

When multiple users work with the same saved question, the following factors control which users can see the question, and which question settings and results the users can see:

- **User role permissions**: To view and edit a saved question, a user must have the required role permissions for the content set to which the question is assigned (see Manage saved questions). Additionally, the **Visibility** setting in the question determines whether the question is visible only to the owner (question creator) or to any user who has the required role permissions.
- **User-specific configuration changes**: When a user saves changes to the question configuration, the Tanium Server saves a copy of the question. When users sign in to the server, the users see only the copy with their own changes.
- **Computer group management rights**: The computer groups assigned to users, user groups, and personas determine the visibility of the saved question **Reissue** interval and recent question results.

For details, see Tanium Console User Guide: User-specific saved questions.

Create a saved question

1. Use the Interact Ask a Question field or **Question Builder** to ask a dynamic question.
   The **Question Results** page shows the results.
2. Click **Save** above the question field and configure the following settings:

Table 9: Saved question settings

Settings	Guidelines
Name	Enter a name to identify the saved question in lists that appear in Tanium Console workflows.
Content Set	Assign the question to a content set. The list is populated with all content sets for which you have **Saved Question** write permission.
Tags	To add tags for filtering lists of saved questions in Tanium Console, click **Add tags**, enter a **Name** to identify the tag, and enter the tag **Value**. Add + a **Name**-**Value** pair for each additional tag. NOTE In the **Sensors** page, the **Tags** column is hidden by default. To show the column, click Customize Columns and select **Tags**.
Visibility	• **According to RBAC**. Users must have the **Saved Question** read permission for the content set to which the saved question belongs to see the saved question. • **Only the Owner and Admins can see this object**. Only the question owner and users with the **Administrator** reserved role can see the saved question. By default, the user who creates the question is the owner. NOTE If the user account of the initial owner is deleted, ownership of the question might transfer to another user. See Delete, undelete, or lock out a user.

Table 9: Saved question settings (continued)

Settings	Guidelines
Reissue	If you want to periodically reissue the question, select **Reissue this question every** and specify a number and unit for the reissue interval: **Minutes**, **Hours**, **Days**. The Tanium Server first issues the saved question immediately after you save the configuration. Tanium Clients that are online at that time respond with their answers. You can use the reissue option to account for clients that are currently offline but will be online later. For example, employee laptops that are offline at the moment you save the saved question configuration might be online at least once during an eight-hour reissue interval. If you configure reissuing, the Tanium Server reissues the saved question in the background at the specified interval. For example, if you save the saved question configuration at 9:00 a.m. local time and specify a reissue interval of every eight hours, the the server reissues the saved question at 5:00 p.m., 1:00 a.m., 9:00 a.m., and so on. By default, the server caches responses for seven days, and displays the cached responses in the **Question Results** grid for endpoints that are offline when the server issues the question. You can use the Question History to verify that the server issues the saved questions based on the specified reissue interval. NOTE If you specify an eight-hour reissue interval, the Tanium Server reissues the question exactly every eight hours, regardless of time changes due to daylight savings time. Which users can see the reissue interval for a saved question depends on the computer groups assigned to those users. For details, see Tanium Console User Guide: User-specific saved questions.
Show this question in the list of questions that are available for drilling down	Enable this option to include the question in the list that users see when selecting a question for a drill-down operation on question results. For details, see Drill down into results.
Show this question in the list of questions that are available to merge	Enable this option to include the question in the list that users see when selecting a question for a merge operation on question results. Only non-counting questions provide this option. For details, see Merge questions. NOTE You cannot change this setting after you save a new saved question configuration. Enabling this option automatically enables the **Yes, turn into non-counting question** option.

Table 9: Saved question settings (continued)

Settings	Guidelines
Do not turn into non-counting question Yes, turn into non-counting question	The option to convert the question to a non-counting question is available only if the question has one sensor in the `get` clause. Converting to a non-counting question enables the Tanium Server to store the answers as recent data, which the server uses when live data is unavailable, such as when the answering endpoints are offline. For details, see Display current or recent question results. NOTE: You cannot change this setting after you save a new saved question configuration. Non-counting questions consume more disk storage because the Tanium Server maintains the answer strings for each endpoint (based on computer ID).
Save these settings for myself and other users with no prior settings saved Save these settings for my view only	Select whether the **User Settings** values that you configured are visible to other users who might view the saved question configuration. This visibility option is useful when you want a question to initially have the same **User Settings** values for everyone until individual users specify their own values. • **Save these settings for myself and other users with no prior settings saved**: The **User Settings** that you configured appear to all users who view the question configuration. If a user subsequently edits the settings, only that user will thereafter see the values that the user configured instead of the values that you initially configured. • **Save these settings for my view only**: When users other than yourself view the question configuration, the **User Settings** have no values until individual users specify values.
Associated Packages	Optionally, select the packages that you want to appear at the top of the **Deployment Package** dropdown list in the **Action Deployment** page when users deploy an action based on the question. By default, the **Deployment Package** selection is set to the first package that you add to the **Associated Packages**. As an example, for a question that returns the logging level of Tanium Clients on Windows endpoints, you might want to add **Set Windows Tanium Client Logging Level** as an **Associated Package**. For details, see Deploying actions and Example: Saved questions with associated packages.

3. Expand the **Preview** section to preview the results of the saved question, and then click **Save**.

The question appears in the **Administration > Content > Saved Questions** page.

IMPORTANT: When you save a question that has a parameterized sensor, the sensor definition, including the substituted values, is saved in an object called a *temporary sensor*. On the endpoint, the Tanium™ Client runs the temporary sensor when it computes answers to a saved question that calls it. A saved question that is reissued according to a schedule continues to use the temporary sensor even if the sensor from which it was based is updated. Therefore, if a sensor is updated, and you want the saved question to use the updated code, you must re-create the saved question.

Edit a saved question

As a best practice, do not edit saved questions that are provided through Tanium content packs (for details, see Tanium Console User Guide: Best practices for resolving import conflicts (Tip 4)). If you need to edit Tanium-provided questions, review User-specific saved questions on page 75 and contact Tanium Support. For more information, see Contact Tanium Support on page 90.

Alternatively, you can create copies of Tanium-provided questions and edit the copies. You can also edit custom saved questions that you created from scratch. To edit a saved question:

1. From the Interact **Overview** page, find the question in the **Saved Questions** panel, mouse over the question, click Options ..., and select **Edit Properties**.
2. Configure the settings described in Create a saved question on page 75 and save your changes.

> **NOTE** If you create a saved question based on a parameterized sensor and then modify the sensor, the saved question behavior reflects the original sensor definition. Only after you modify the saved question will it behave as expected with the new sensor definition. For details on parameterized sensors, see Questions with parameterized sensors on page 12.

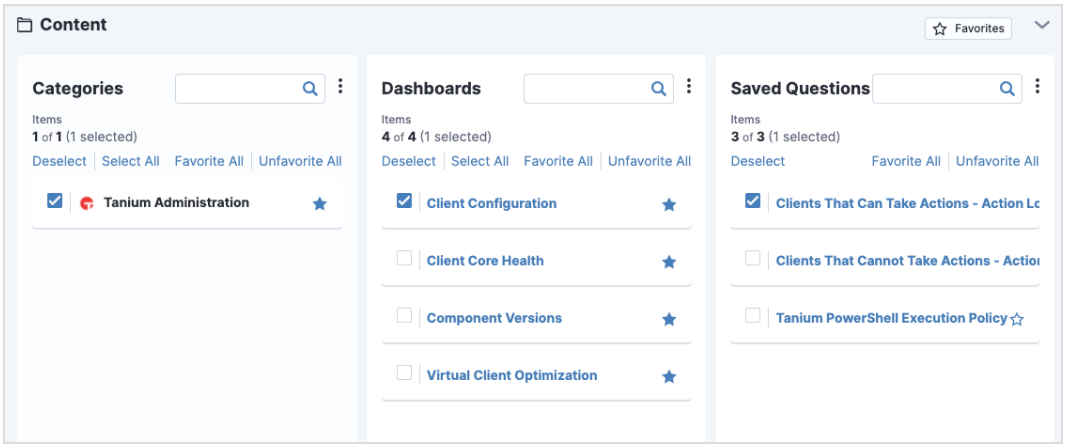
Filter saved questions

The number of saved questions tends to increase as your team uses the Tanium system more. To find specific questions when the Interact **Overview** page has too many to scan quickly, you can filter by text strings, categories, dashboards, and favorites.

Filter by categories and dashboards

In the Interact **Overview** page, you can select check boxes in the panels so that only items belonging to the selected categories or dashboards appear. You can apply multiple filters. Click **Deselect** in a panel header to deselect all its filters.

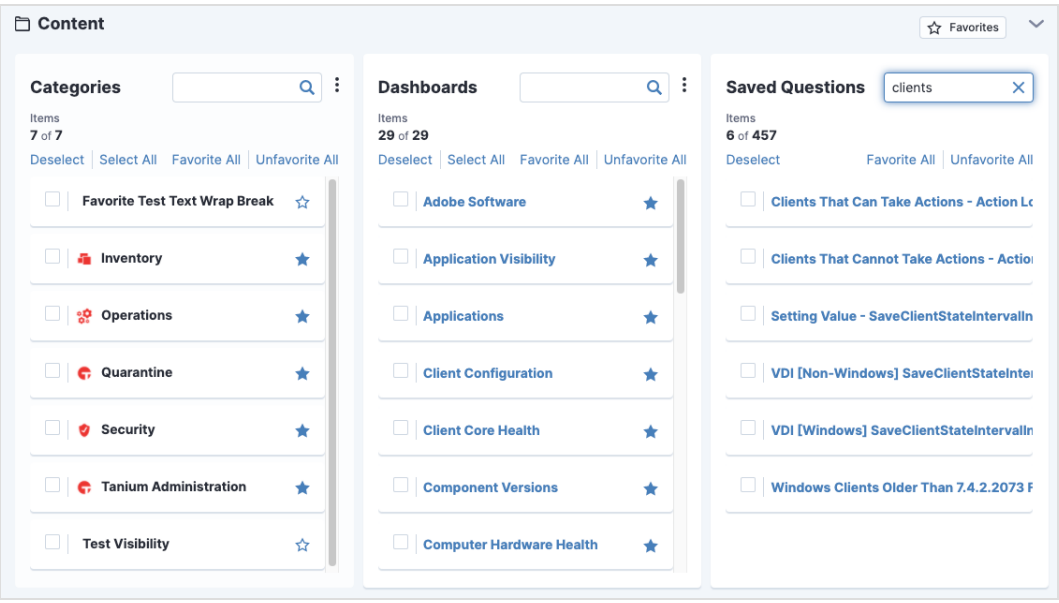
Figure 15: Interact content filters



Filter by text strings

In the Interact **Overview** page, use text filters in the panels to find items that match a specified string. Click the **x** in the text search box to deselect the filter.

Figure 16: Text filters



Filter by favorites

A *favorite* is a category, dashboard, or saved question that you want to appear on the Interact **Overview** page. You can also use favorites as an optional filter on the Interact **Overview** page. The Tanium Server saves favorites as a user-specific setting; your favorites selections do not apply to other users.

Items that you select as favorites before upgrading to Interact 2.0 or later remain favorites after upgrading. If you did not have favorites before an upgrade or before you install a new Tanium Server, all categories and dashboards for which you have read permission are set as favorites anyway.

To configure the display of favorite content, perform the following steps:

1. From the Main menu, go to **Modules > Interact**.

   TIP

   On the Tanium **Home** page, click the Favorites icon for an item to deselect it as a favorite and remove it from the page. However, the Tanium **Home** page does not provide the option to show items that are not favorites, so you cannot restore favorite status to items on that page.

2. Click the Favorites icon next to the name of a category, dashboard, or saved question to select or deselect that item as a favorite.

   TIP To reduce clicks, click **Favorite All** or **Unfavorite All** in a panel header and then toggle on or off individual items in that panel.

3. To view only favorite categories, dashboards, and saved questions, click **Favorites** in the upper right of the **Content** section. The button changes to a dark background to indicate that the panels display only favorites. Click **Favorites** again to toggle off the filter.

   TIP After you find and select your favorite **Categories** or **Dashboards**, you might want to toggle off the **Favorites** filter so that the **Saved Questions** panel displays both favorite and non-favorite questions.

Reissue a saved question

After you save a question, you can manually reissue it anytime by performing one of the following steps:

- From the Interact **Overview** page, click the question name in the **Saved Questions** panel.
- If the question is selected as a favorite, go to the Tanium **Home** page, scroll to the **Favorite Interact Categories**, expand the corresponding category and dashboard, and click the question name.

Tanium Console displays the results in the saved question results page. This page provides the option to see recent results from offline endpoints if those results still reside on the Tanium Server after the last time the question was issued. The server stores the results of saved questions for seven days by default. For details, see Display results for online and offline endpoints on page 51.

TIP If you want the Tanium Server to automatically reissue a saved question, edit the question configuration and set the **Reissue** interval: see Edit a saved question on page 79.

If you want to simultaneously issue all the questions in a dashboard, see Issue a dashboard of saved questions on page 81.

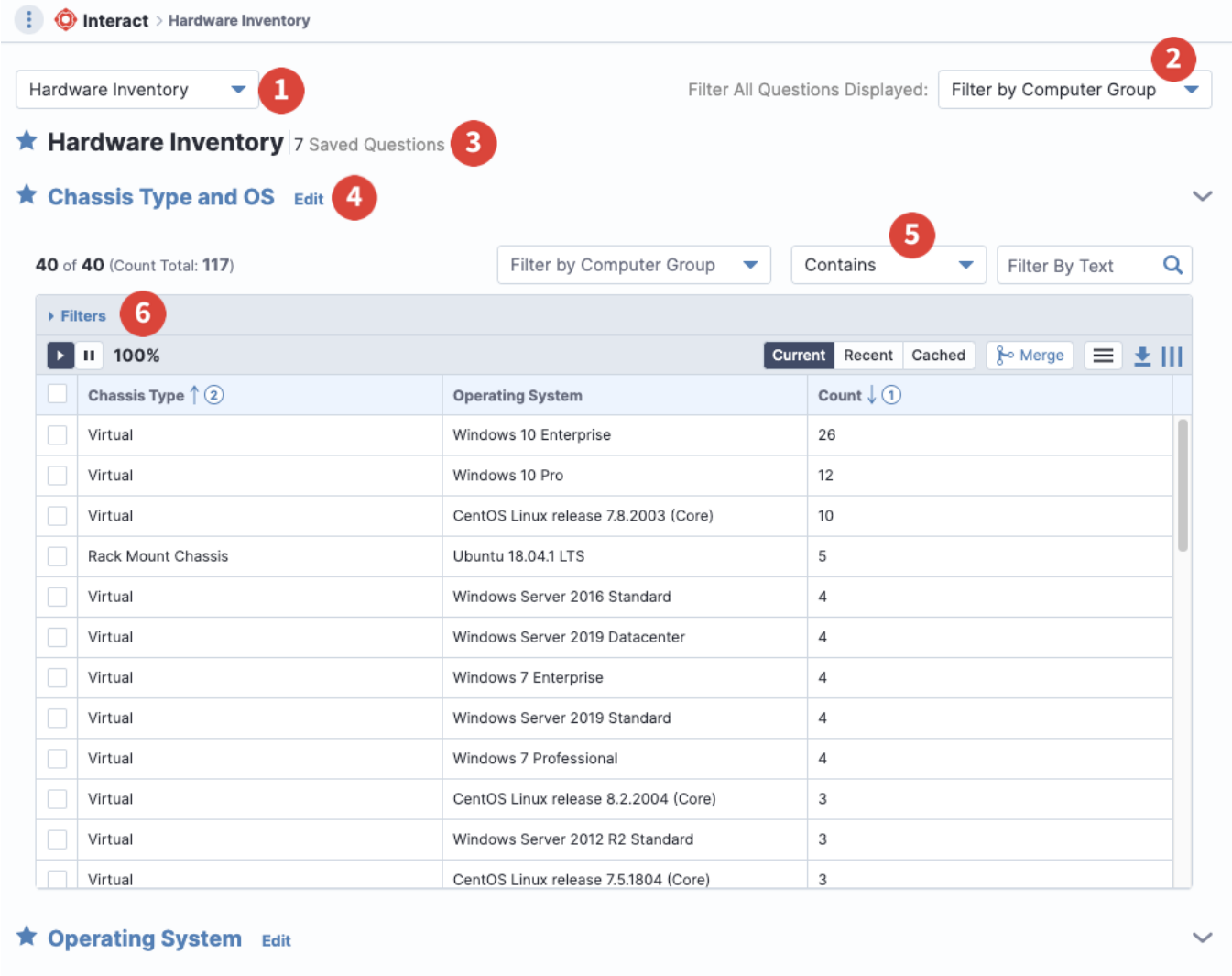
Issue a dashboard of saved questions

In some cases, it is useful to issue several saved questions that are related based on the kind of information they retrieve from endpoints. In such cases, you can group the questions in a single dashboard and issue them simultaneously. For example, the predefined **Hardware Inventory** dashboard contains questions that retrieve chassis type, operating system, monitor, CPU, disk, memory, and BIOS information.

To issue all the questions in a dashboard:

1. From the Main menu, go to **Modules > Interact**.
2. In the **Dashboards** panel, click the dashboard name.
   The dashboard results page appears, which shows a results grid for each saved question in the dashboard.

Figure 17: Dashboard results page



For each question, the dashboard results page provides all the features that are available in the saved question results page, such as viewing **Current**, **Recent**, or **Cached** results (see Managing question results on page 50). The dashboard results page also has the following features (matching the numbers in Figure 17):

1 Use the dashboards dropdown list to issue a different dashboard.

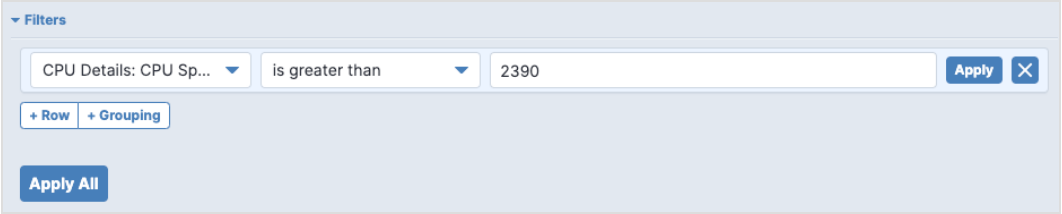
2 Use the **Filter All Questions Displayed** drop-down to filter all the results grids by computer group.

3 The page shows the dashboard name, favorite status (★ for favorite, ☆ for non-favorite), and number of saved questions in the dashboard. Click the favorite icon ★/☆ to toggle the favorite status of the dashboard.

4 For each results grid, the page shows the question name and favorite status. Click the favorite icon ★/☆ to toggle the favorite status of the question. Click the question name to reissue the question. Click **Edit** to change the question settings. See Edit a saved question on page 79.

5 Filter by computer group or text.

6 Apply additional filters to a specific results grid.



Manage categories and dashboards

Tanium solutions that you import provide predefined dashboards as containers for organizing saved questions. The solutions also provide predefined categories as containers for dashboards. You can create custom categories and dashboards, and assign saved questions to them based on how you set up role-based access control (RBAC) for your Tanium deployment. You perform all the following tasks on the Interact **Overview** page.

Create a category

1. In the **Categories** panel heading, click Options and select **New Category**.
2. Specify a **Name**, **Content Set**, Icon, and **Visibility** option, and click **Save**.

Create a dashboard

1. In the **Dashboards** panel heading, click Options and select **New Dashboard**.
2. Specify a **Name**, **Filter Group**, **Content Set**, and **Visibility** option, and click **Save**.

Assign dashboards to a category

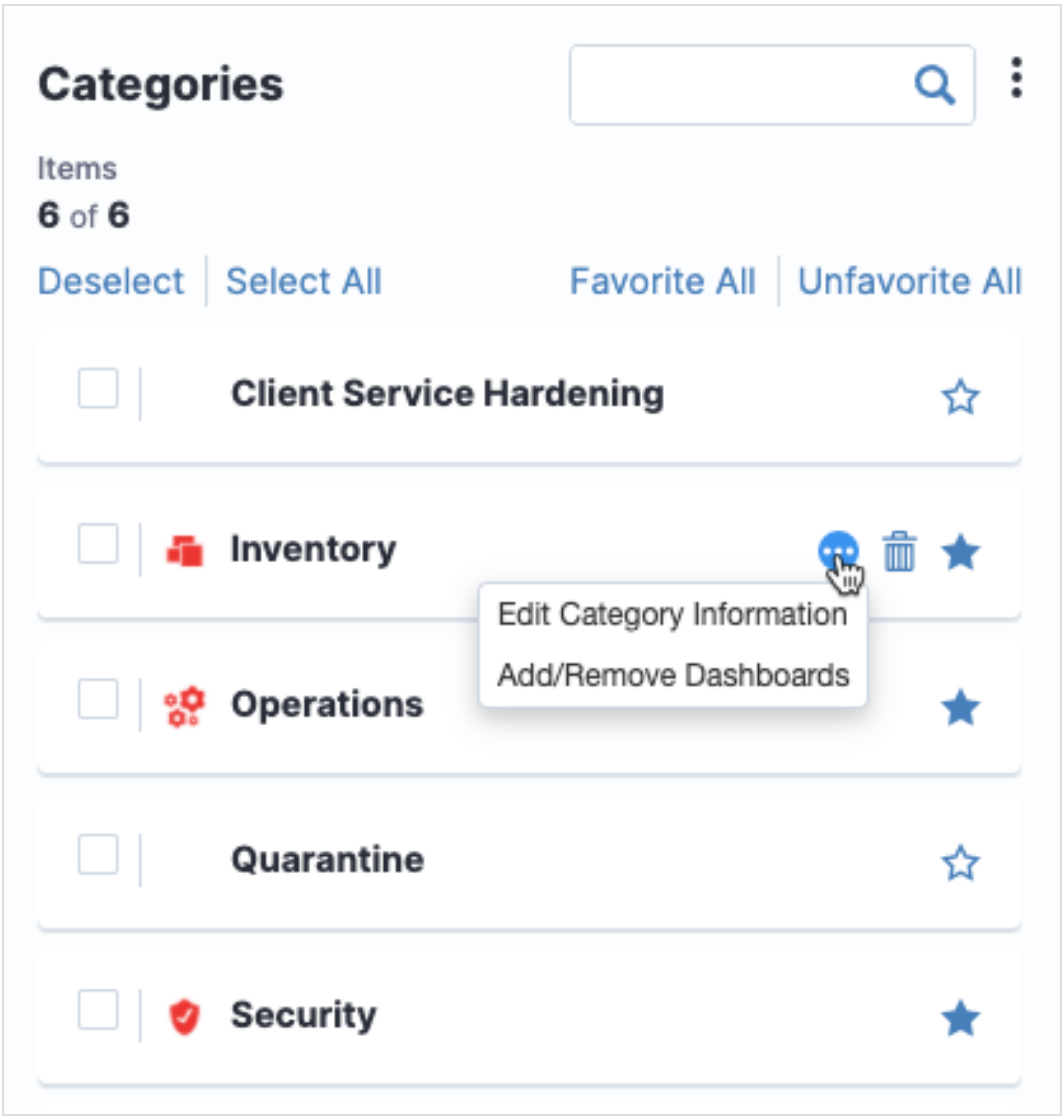
1. In the **Categories** panel, mouse over the category, click Options, and select **Add/Remove Dashboards**.
2. In the **Dashboards** panel, select the dashboards to include in this category and click **Apply**.

Assign saved questions to a dashboard

1. In the **Dashboards** panel, mouse over the category, click Options, and select **Add/Remove Saved Questions**.
2. In the **Saved Questions** panel, select the saved questions to include in this dashboard and click **Apply**.

Edit category or dashboard settings

1. In the **Categories** or **Dashboards** panel, mouse over the category or dashboard, click Options, and select **Edit Category Information** or **Edit Dashboard Information**.



2. Edit the settings and save the configuration.

TIP To edit saved questions settings, see Edit a saved question on page 79.

Export categories, dashboards, or questions

If you are assigned a role with the **Export Content** permission, you can export category, dashboard, and saved question configurations as a JSON file. The **Administrator** reserved role has that permission.

1. Click Options in the panel header and select the export option.
2. Select items to export or **Select all**.
3. Click **Export**, optionally modify the **File Name**, and click **Export** again.

The JSON file is saved to the downloads folder on the computer that you use to access Tanium Console.

Delete a category or dashboard configuration

When you delete a category, the Tanium Server does not assign its dashboards to any other category. When you delete a dashboard, the server does not assign its saved questions to any other dashboard.

1. In the **Categories** or **Dashboards** panel, mouse over the category or dashboard and click Delete.
2. Confirm that you want to delete the configuration.

> NOTE
> You cannot delete a saved question configuration from the Interact **Overview** page, only from the **Administration > Content > Saved Questions** page.

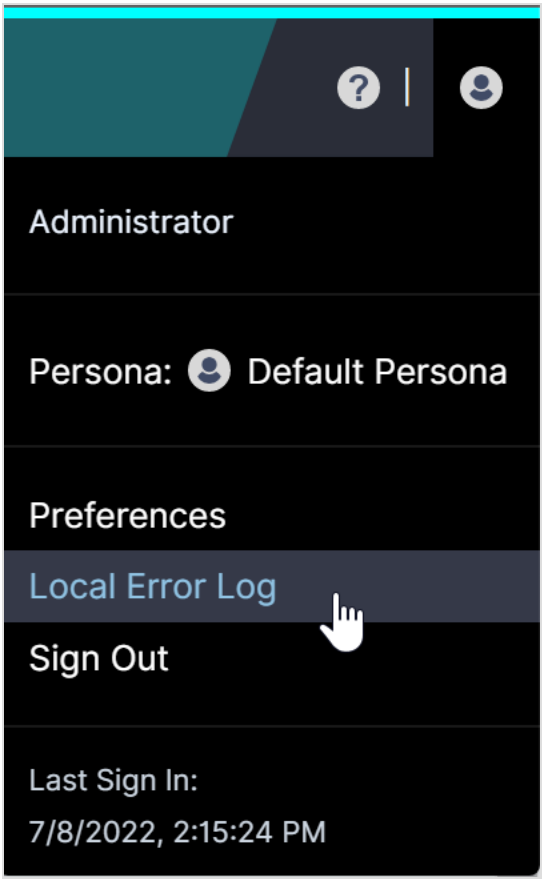
Troubleshooting Interact

If you encounter unexpected behavior, there are a few basic troubleshooting steps.

View and copy the Local Error Log

Tanium Interact maintains an error log on the local host computer for your web browser. It includes details on the last 100 errors that were returned to the Interact in response to actions that you performed through the browser. For example, the log records errors that are associated with attempting to save a configuration or import a content file. Interact maintains a separate log for each browser that you use.

1. In the Main menu, click and select **Local Error Log**.



2. (Optional) Expand a log entry and click Copy to copy the log details to the clipboard.
3. (Optional) Click **Clear Log** if you want to remove all the log entries. For example, you might want to remove the entries after you finish resolving the associated issues.

Collect Interact logs

To send information to Tanium Support for troubleshooting Tanium Interact, perform the following steps to collect logs and other relevant information. The information is saved as a ZIP file that you can download through your browser.

1. From the Interact **Overview** page, click Help .
2. In the **Troubleshooting** section, click **Download Support Package**.
   A `tanium-interact-support-<date-time>.zip` file downloads to the local download directory.
3. Attach the ZIP file to your Tanium Support case form or send it to Tanium Support.

Troubleshoot question runtimes

If Tanium Clients answer a question slower than expected, the question might use sensors that have long runtimes. Tanium Console displays runtime indicators to show the average runtimes of sensors that you select for questions. If necessary, you can customize the thresholds that determine which indicator appears for a specific runtime. See Tanium Console User Guide: Managing sensor runtime thresholds.

Troubleshoot question results issues

If Tanium Clients do not answer questions, review the following issues and remediation tasks:

Question results issues

Issue	Remediation
No results	The **Question Results** grid displays `[no results]` to indicate that a Tanium Client was instructed to answer but does not have a value that matches the sensor filter. This occurs if you apply a filter to the `get` clause and not the `from` clause. For example, if the question is `Get IP Address ending with 2 from all machines`, all endpoints return answers and all endpoints without an IP address ending in 2 return `[no results]`. BEST PRACTICE Add the filter in the `from` clause. For example, `Get IP Address from all machines where IP Address ends in 2` does not return unexpected `[no results]` rows. You might also see `[no results]` if the sensor does not return a value or cannot execute the script.
Current result unavailable	If an endpoint takes longer than usual to evaluate a sensor, it might initially supply the answer `[current result unavailable]` to the answer message that it passes along the linear chain and ultimately to the Tanium Server. However, the sensor process continues on the endpoint after supplying that initial answer and, upon completing the process, the endpoint sends its updated answer. The server then updates the **Question Results** grid.
Results currently unavailable	The **Question Results** grid displays the `[results currently unavailable]` message to indicate that the Tanium Server cannot correctly parse an answer. Contact Tanium Support if you observe this message.

Question results issues (continued)

Issue	Remediation
Too many results	The **Question Results** grid displays `[too many results]` to indicate that more results are available, but the Tanium Clients will not return the additional results. The Tanium Server has certain checks to limit the network and memory impact of questions. Because of how these messages are generated, you cannot drill down on this response. To avoid this message, uses sensors that are more focused, or target only a certain endpoint or computer group to limit the unique number of strings for each answer.
TSE-Error	Messages that begin with `[TSE-Error` indicate a Tanium Client is in a state that prevents it from answering the question. Common reasons include: • Unstable operating system (OS) • Configuration issues • Lack of memory • Antivirus software blocks: To ensure that all the required exclusions are configured in your antivirus software, see Tanium Core Platform Deployment Reference Guide: Host system security exclusions. • Corrupted Windows Management Instrumentation (WMI) repositories • Sensor quarantines: The **Question Results** page displays `TSE-Error: The sensor is quarantined` if the question uses quarantined sensors. You can remove those sensors from quarantine if appropriate. See Tanium Console User Guide: Manage sensor quarantines. • Issues related to the roles that are assigned to your user account. See Tanium Console User Guide: Troubleshoot role-based access control (RBAC) issues. • Issues related to the computer groups that are assigned to your user account. See Results missing from certain endpoints on page 89.

Question results issues (continued)

Issue	Remediation
Results missing from certain endpoints	You can see question results only from endpoints in computer groups that are assigned to the user account or persona that you use to issue questions. If certain endpoints to do return results, troubleshoot computer group assignments and configurations: • **Assignments**: Verify that the appropriate computer groups are assigned. If your user account inherits computer group assignments, you might have to assign a different user group: ◦ Tanium Console User Guide: Manage computer group assignments for a user ◦ Tanium Console User Guide: Manage computer group assignments for a persona ◦ Tanium Console User Guide: Manage computer group assignments for a user group ◦ Tanium Console User Guide: Manage user group assignments for a user • **Configurations**: View the computer group configurations to ensure that their membership **Expression** is correct. Note that you cannot edit the membership of a computer group. If the membership does not include the correct endpoints, you must create and assign a new computer group. ◦ Tanium Console User Guide: View computer group details ◦ Tanium Console User Guide: Create a computer group
Tanium Client communication	View the status of client connections and, if necessary, correct them. See Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

Troubleshoot action deployment issues

To ensure actions deploy as expected and to troubleshoot deployment issues, see Tanium Console User Guide: Monitor actions.

Troubleshoot Tanium Data Service issues

Tanium Data Service collects and stores the results of all sensors that are registered for collection so that users can see those results for offline endpoints when issuing questions. Sensor collection consumes resources such as network bandwidth, processing on endpoints, and disk space on the Tanium Server. To monitor and troubleshoot resource usage for sensor results collection, see Tanium Console User Guide: Troubleshoot Tanium Data Service issues.

Uninstall Interact

If you need to uninstall Interact, perform the following steps.

IMPORTANT If you uninstall Interact, and no users, personas, or user groups are assigned to the **Feed User** role before uninstalling Interact, you lose the ability to access Tanium™ Feed. To regain access to Feed, either reinstall Interact, or assign users, personas, or user groups to the **Feed User** role.

1. Sign in to Tanium Console as a user with the Administrator role.
2. From the Main menu, select **Administration > Configuration > Solutions**.
3. In the **Interact** tile, click **Uninstall**  .

To reinstall Interact, see Installing Interact on page 37.

Contact Tanium Support

To contact Tanium Support for help, sign in to https://support.tanium.com.

Reference: Example questions

Review the following examples to learn about the kinds of questions that Tanium Interact enables you to issue to endpoints.

Example starter questions

The following examples show common questions.

How can I get a list of running services on all endpoints or a specific endpoint?

```
Get Running Service from all machines
```

```
Get Service Details from all machines
```

```
Get Running Service from all machines with Computer Name containing "<hostname>"
```

How can I get a list of running processes on all endpoints or a specific endpoint?

```
Get Running Processes from all machines
```

```
Get Running Processes from machines where Computer Name contains "<hostname>"
```

```
Get Running Processes and Computer Name contains "<hostname>" from all machines
```

How can I display Windows Registry keys and values?

```
Get Registry Value Data[registry key path, value-name] from all machines
```

```
Get Registry Value Data[HKEY_LOCAL_
MACHINE\Software\Microsoft\Windows\CurrentVersion, CommonFilesDir] from all
machines
```

```
Get Registry Key Value Exists[registry key path, value-name] from all machines
```

```
Get Registry Key Exists[HKEY_LOCAL_
MACHINE\Software\Microsoft\Windows\CurrentVersion, CommonFilesDir] from all
machines
```

How can I get a list of open ports?

```
Get Computer Name and Open Port from all machines
```

```
Get Open Port from machines where Computer Name contains "<hostname>"
```

```
Get Open Port from all machines with Computer Name containing "<hostname>"
```

How can I get user authentication information?

```
Get Logged In Users contains "<user name>" from all machines
```

```
Get Logged In Users containing "BABOON08D9ANGUI\Administrator" from all machines
```

```
Get Logged In Users and Computer Name from all machines
```

```
Get Local User Login Dates from all machines
```

```
Get Logged In Users and Client Date from all machines
```

```
Get Last Logged In User and Client Date from all machines
```

```
Get Local Administrators from all machines
```

How can I see the current logged on user?

```
Get User Sessions from all machines
```

How can I see when users last logged in?

```
Get local User Login Dates from all machines
```

How can I get the Service Account logins?

```
Get Service Login Names from all machines
```

How can I get certificate information?

```
Get Machine Certificates[authroot] from all machines
```

```
Get Machine Certificates[disallowed] from all machines
```

```
Get Machine Certificates[root] from all machines
```

For Intermediate Certs:

```
Get Machine Certificates[CA] from all machines (Intermediate Certs)
```

How can I detect all running Oracle instances within a Linux environment?

```
Get computer name and running processes that contains "ora_pmon" from machines
with running processes contains "ora_pmon"
```

How can I get asset information?

```
Get Cpu and Cpu Details and Chassis and Architecture and Serial Number and
Computer Name and Bios and IP Address and Mac Address and serial number from all
machines
```

Example dashboard questions

Reviewing the list of predefined saved questions in dashboards and categories is a good way to learn how to use questions to get meaningful results. The following examples illustrate a few such predefined questions that are organized by ***<category> > <dashboard>***.

Security > Data Leakage

```
Get Computer Name and Non-Approved Established Connections from all machines with
Non-Approved Established Connections containing ":"
```

Security > Wireless Network Security

```
Get Wireless Networks Visible from all machines
```

```
Get Hosted Wireless Ad-Hoc Networks from all machines with Hosted Wireless Ad-Hoc Networks containing "started"
```

```
Get Unencrypted Wireless Networks from all machines with Unencrypted Wireless Networks containing "open"
```

```
Get Wireless Networks Using WEP from all machines with Wireless Networks Using WEP containing "wep"
```

Security > Proactive Security

```
Get Firewall Status containing "disabled" from all machines with Firewall Status containing "disabled"
```

```
Get Computer Name and Open Share Details from all machines with Open Share Details not containing "No shares"
```

Security > Workstation USB Write Protection

```
Get USB device details from all machines
```

```
Get Computer Name and Username from all machines with ( Operating System not containing "server" and USB Write Protected containing "False" )
```

```
Get Computer Name and Username from all machines with ( Operating System not containing "server" and USB Write Protected containing "True" )
```

Reference: Advanced question syntax

Use reserved words or characters

Reserved words or characters in question text

The Tanium™ parser uses certain words and characters to interpret the question text that you enter as valid query syntax. For example, the parser uses the bracket characters `[` and `]` to enclose the values of parameterized sensors and uses variations of the word `match` to support regular expressions. You must enclose these reserved words and characters in quotation marks when you use them as string literals in questions. For example, to see all endpoints that have computer names containing the letter combination `in`, issue the question `Get Computer Name from all machines with Computer Name contains "in"`.

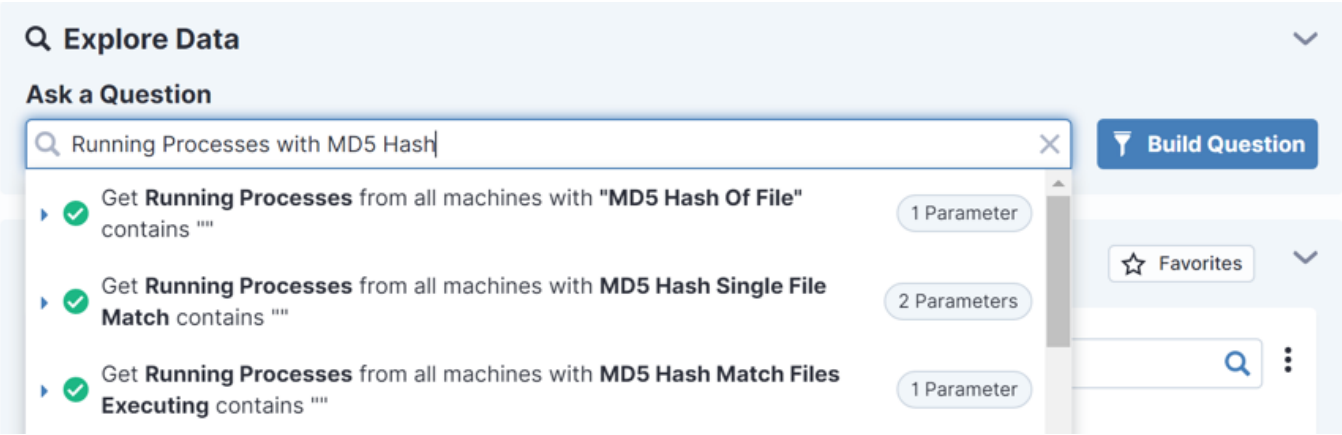
- "
  Use double quotation marks as an escape-character sequence for each instance of quotation marks in a text string. For example, to see which endpoints have a computer name that contains the string `"test"`, issue the question:
  `Get Computer Name from all machines with Computer Name contains """test"""`
- .
- ,
- :
- ?
- $
- White spaces
  For example, to see which endpoints have a computer name that has a blank space before and after the string `DBserver`, issue the question:
  `Get Computer Name from all machines with Computer Name contains " DBserver "`
- all
- and
- any
- contain
- containing
- contains
- does match
- does not match
- ending
- ends

- equals
- get
- having
- in
- matches
- matching
- not
- or
- with
- starting
- starts

Reserved words in sensor names

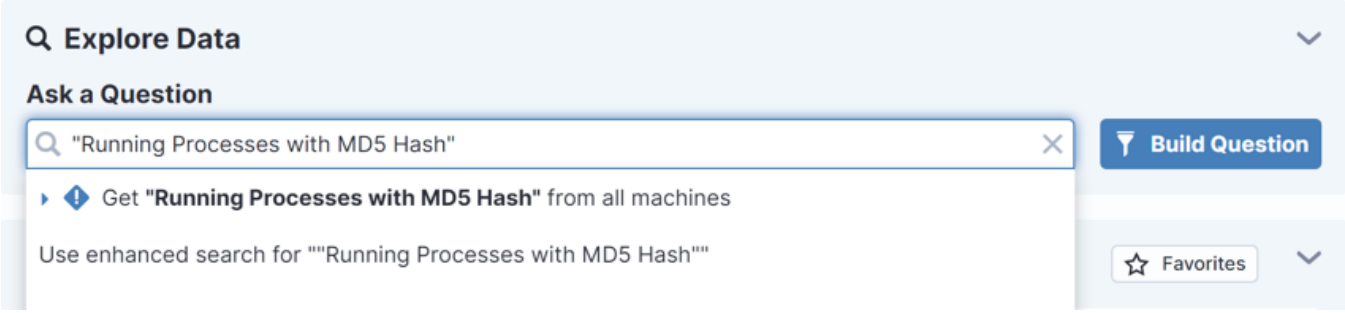
Sensors with names that use reserved words require quotation marks when you use them as string literals in the Interact **Ask a Question** field. Otherwise, the dropdown list that displays suggested questions cannot accurately match your entry. For example, if you enter the **Running Processes with MD5 Hash** sensor without quotation marks, the dropdown list displays suggestions that confuse your entry with other sensors that contain the words `MD5 Hash`:

Figure 18: Sensor name without quotations



If you use quotation marks around the sensor name, the dropdown list displays the correct question:

Figure 19: Sensor name with quotations



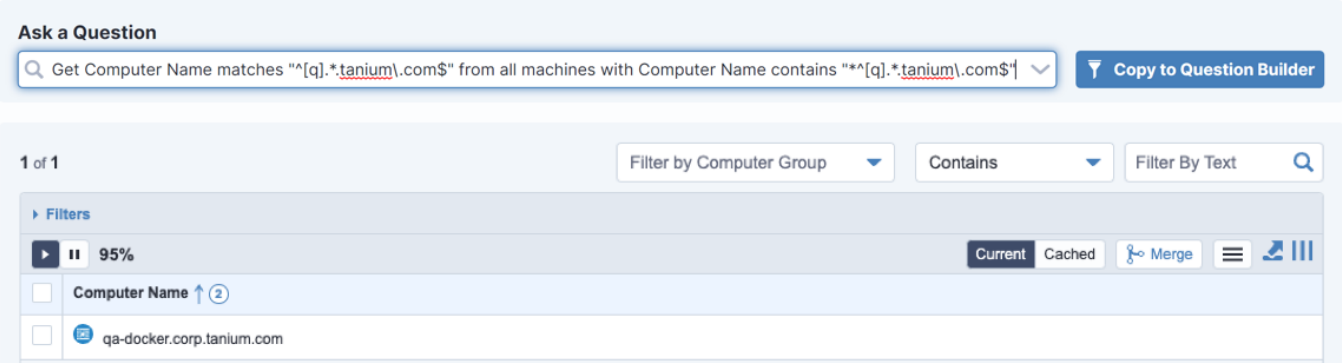
- $serverNames
- $serverIDs
- $substring
- $unescape
- all
- All
- ALL
- and
- any
- computers
- Computers
- COMPUTERS
- contains
- containing
- equals
- from
- From
- FROM
- get
- Get
- GET
- having
- Having

- HAVING
- in
- machines
- Machines
- MACHINES
- matches
- matching
- not
- number
- Number
- NUMBER
- of
- Of
- OF
- or
- where
- Where
- WHERE
- with
- With
- WITH

Use regular expression filters

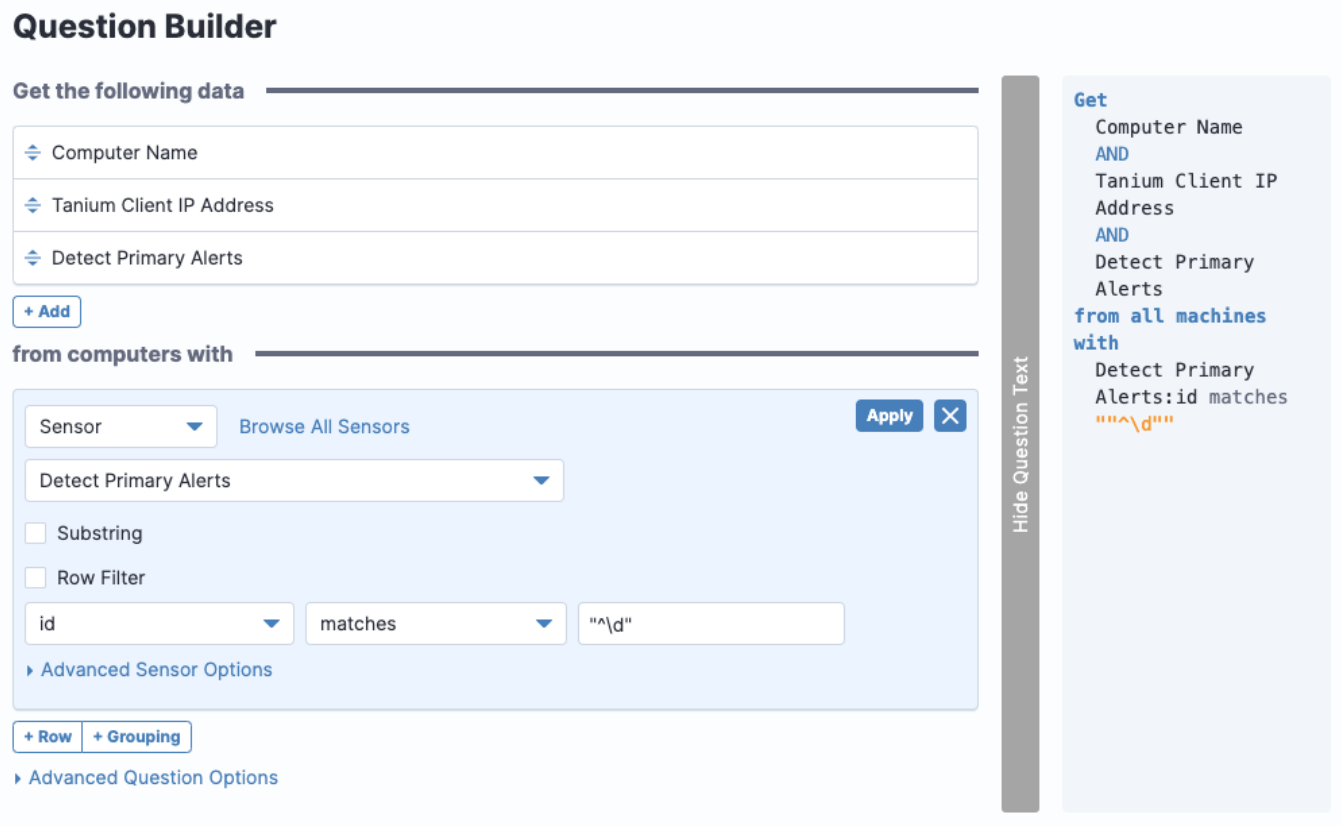
The question parser supports regular expression matching based on Boost syntax. The following example matches computer names that begin with the letter `q` in the `tanium.com` domain.

Figure 20: Matching a regular expression



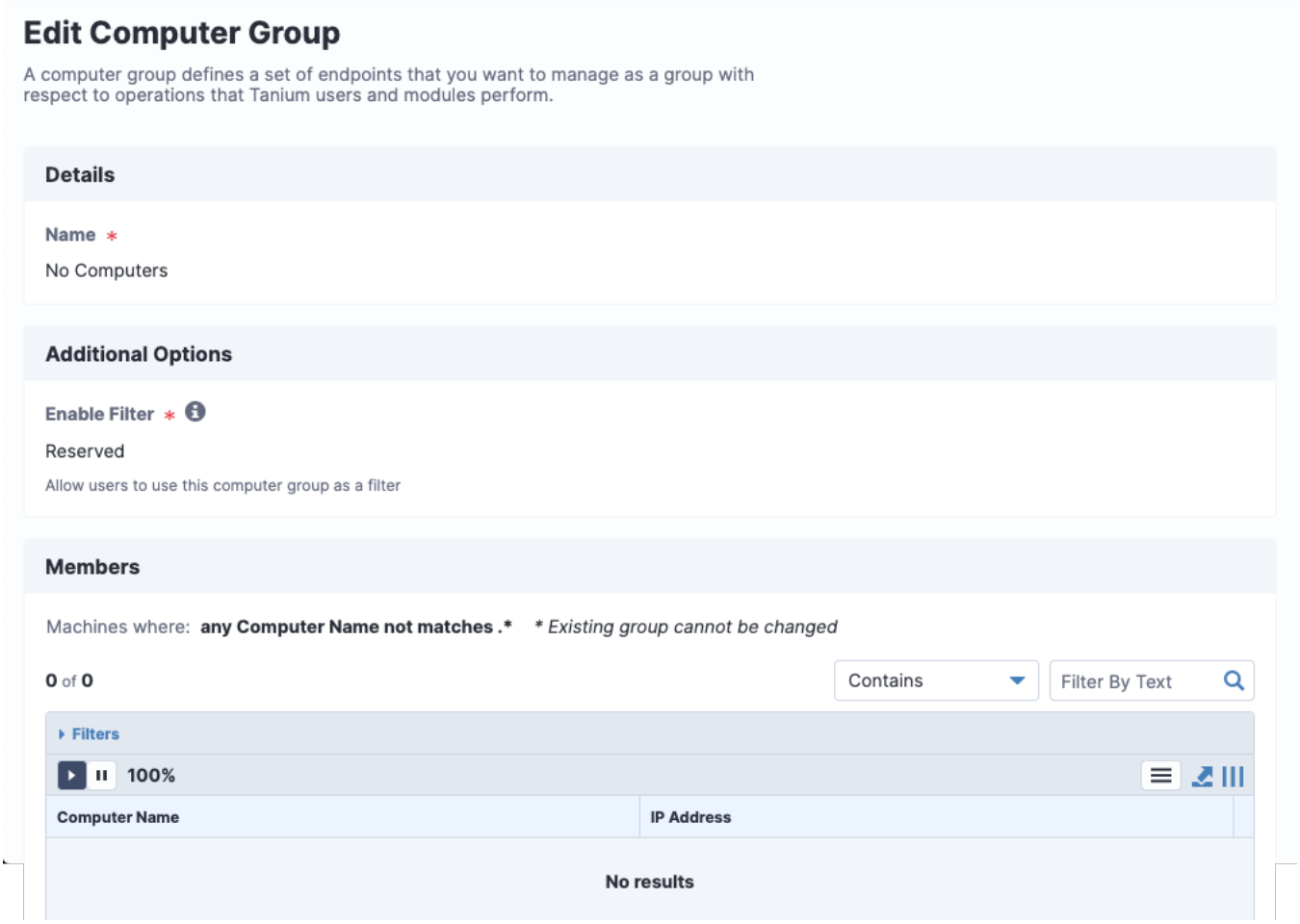
The **Detect Primary Alerts** sensor uses a regular expression to collect results that match any digit in the range 0 to 9. Because alerts have numeric IDs, this expression excludes empty results.

Figure 21: Regular expression to exclude empty results



You can also use a combination of negation and regular expressions to build filter expressions. For example, the predefined computer group **No Computers** uses a question with the `not matches` expression and a regular expression (`.*`) to match empty results. Because the **Computer Name** sensor always returns a string, this combination provides a way to prevent action deployment. To stop the Tanium Server from deploying certain actions to any endpoints, configure those actions to target the **Default** action group, which includes only the **No Computers** computer group.

Figure 22: Regular expression to not match anything

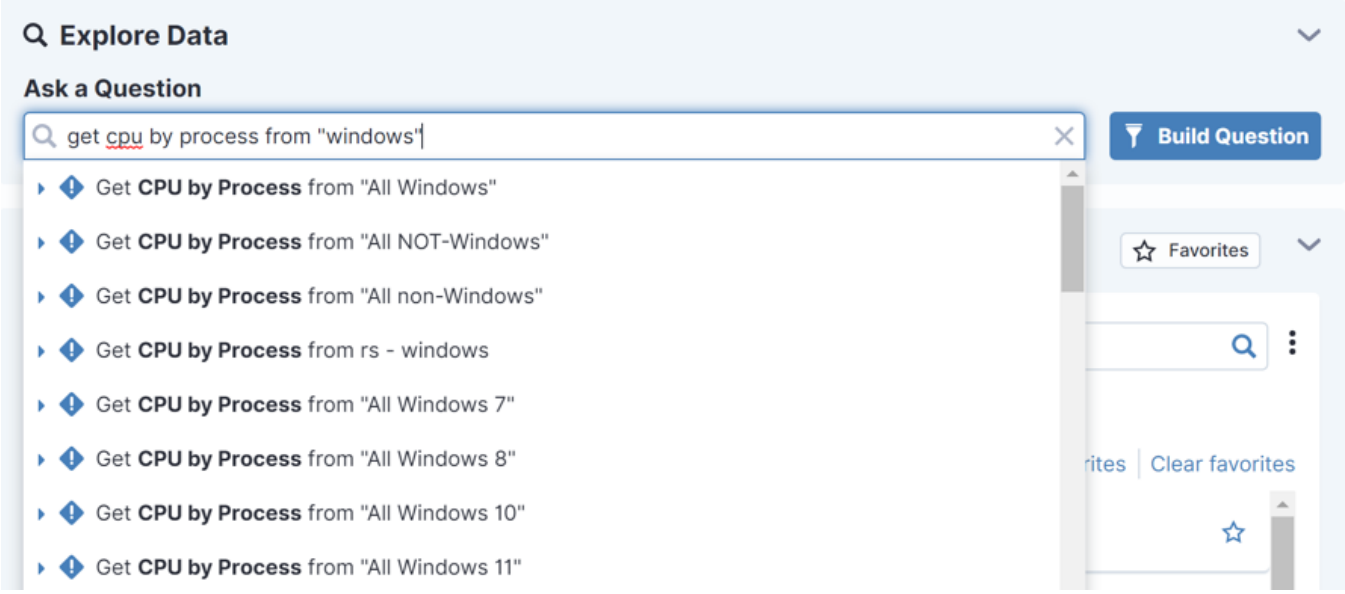


Use computer group filters

You can issue questions that specify a computer group in the `from` clause. Use quotation marks around the computer group name. The computer group can be a management group or filter group. For details about these types, see Managing computer groups.

For computer groups with filter-defined membership, the question parser converts the specified computer group name into the question that determines membership.

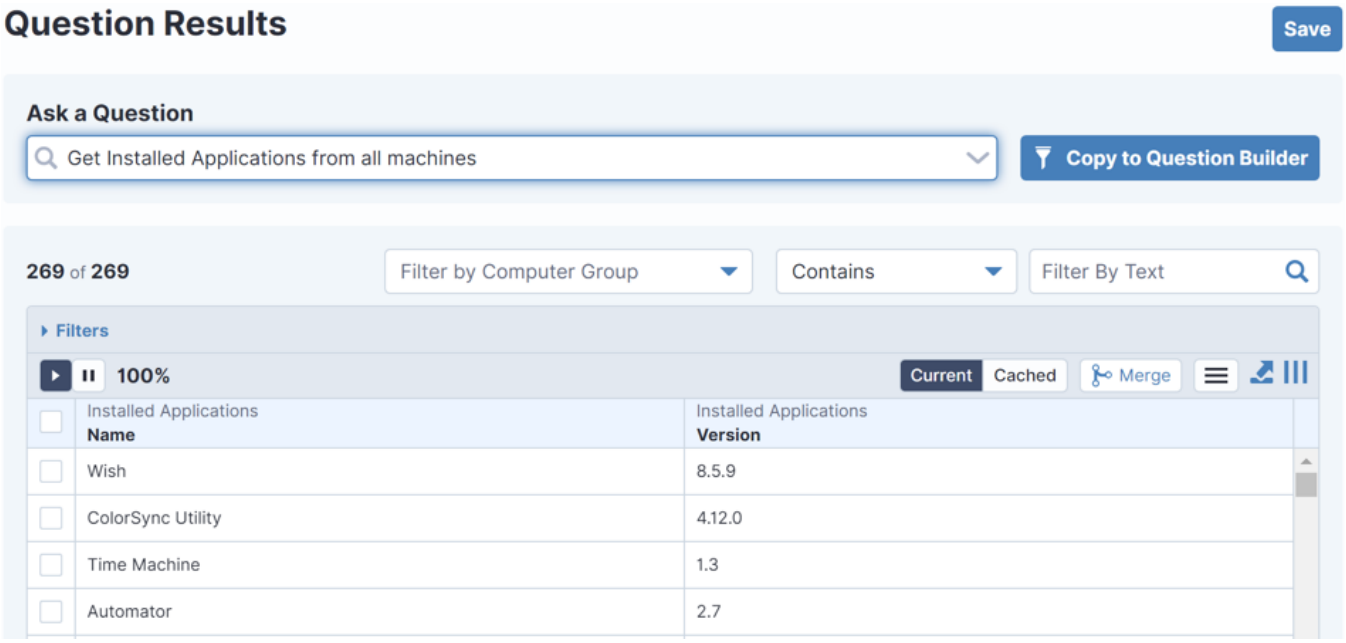
Figure 23: From clause with computer group



Use sensor column filters

Multi-column sensors are designed to collect multiple pieces of related information in a single answer.

Figure 24: Results from a multi-column sensor

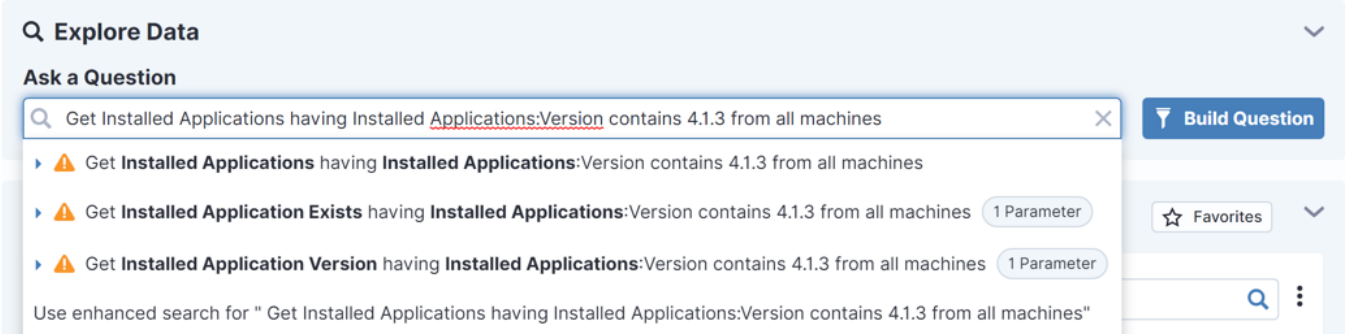


Using the regular expression `starts with`, `ends with`, or `contains` to filter results for a multi-column sensor, such as **Installed Applications**, can be tricky because the result string for a multi-column sensor is actually a single string with column delimiters. If you are not careful, you might match a string in an unexpected column or unknowingly match a string in a hidden column. For a multi-column sensor, you can specify a particular column for results matching. The syntax is `get <sensor> having`

`<sensor>:<column> contains <value>`. The column name is case sensitive. Note that single-column filtering works only if the sensor configuration specifies column delimiters (Split into multiple columns field) with a single character (such as `|`), not multiple characters (such as `|:`). To match results from all the columns, the syntax is `get <sensor> contains <value>`.

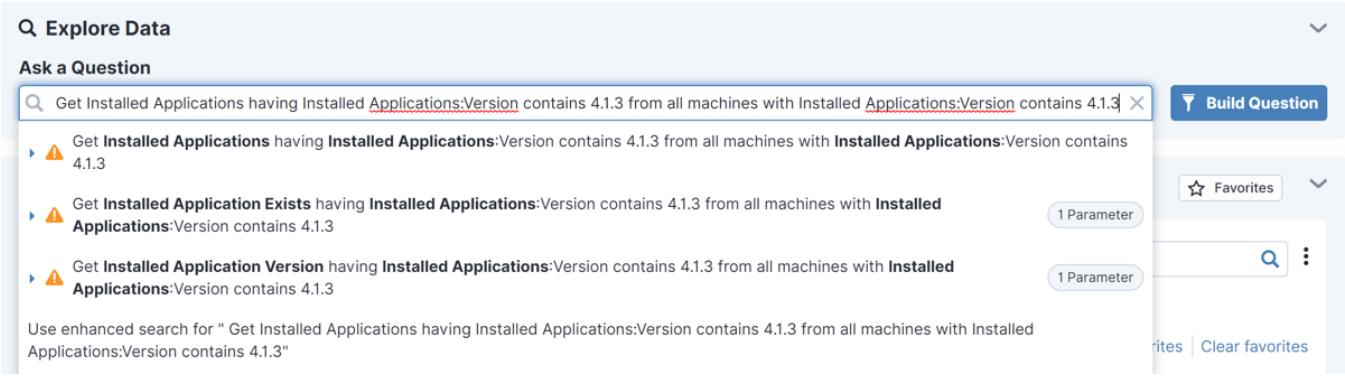
The following example uses a sensor column filter in the `get` clause.

Figure 25: Sensor column filter in the get clause



The following example uses a sensor column filter in both the `get` clause and the `from` clause.

Figure 26: Sensor column filter in the get clause and the from clause

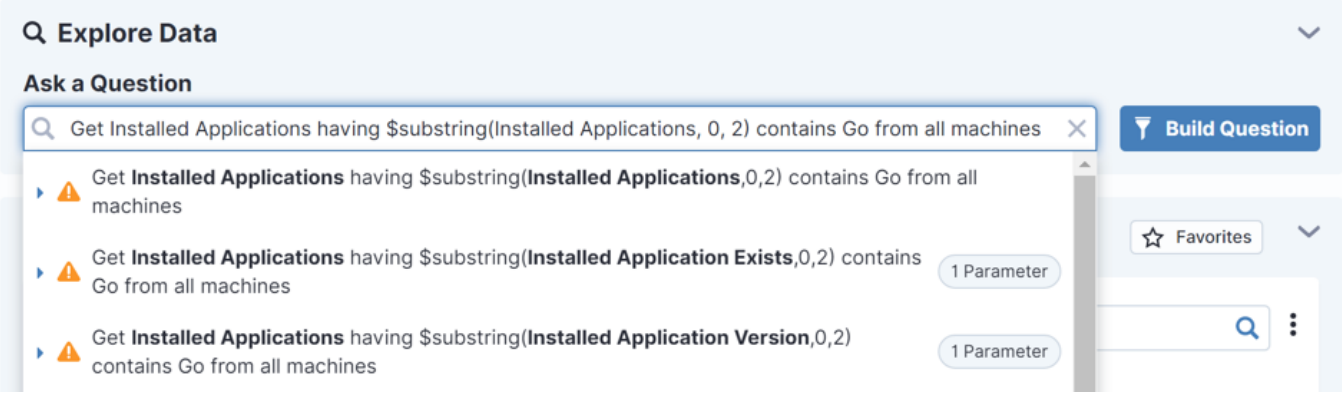


Use $substring() filters

You can use `$substring()` filters to match result string patterns. The `$substring()` function takes the following arguments: sensor name, starting position (where 0 is the first position), number of characters.

The following example matches results from the **Installed Applications** sensor where the first two characters match the string `Go`.

Figure 27: $substring() filter



NOTE

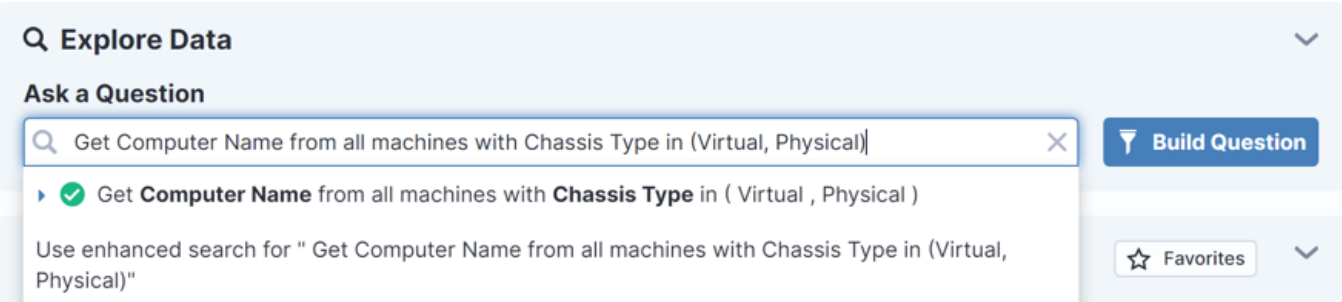
You cannot use the `$substring()` filter with multi-column sensors.

Use the in operator for filtering

You can use the `in` operator to specify a collection of matching sensor results. The operator takes a comma-separated list of arguments that is parsed into a Boolean OR.

The following example uses the `in` operator to match a sensor filter in the `from` clause with results containing `Virtual` or `Physical`.

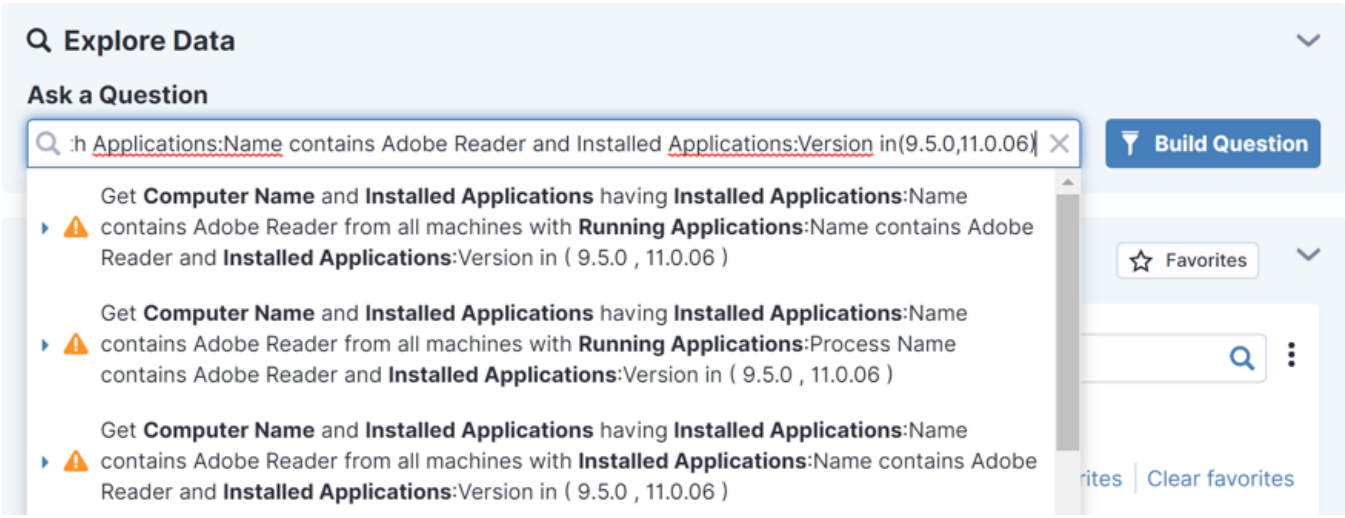
Figure 28: in operator in the from clause



The following example uses the `in` operator to match a sensor column filter in the `from` clause. The question syntax is:

```
Get Computer Name and Installed Applications having Installed Applications:Name contains Adobe Reader from all machines with Installed Applications:Name contains Adobe Reader and Installed Applications:Version in(9.5.0,11.0.06)
```

Figure 29: in operator with a sensor column filter



Use nested filters

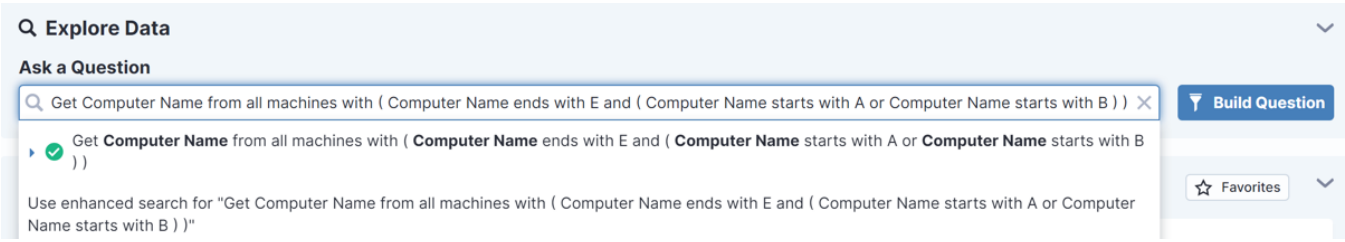
In the `from` clause of a question, you can configure multiple filters, including nested filters.

The following example shows nested filters in the **Question Builder**. The example combines one matching expression with either one of the nested expressions.

Figure 30: Nested filters in the Question Builder

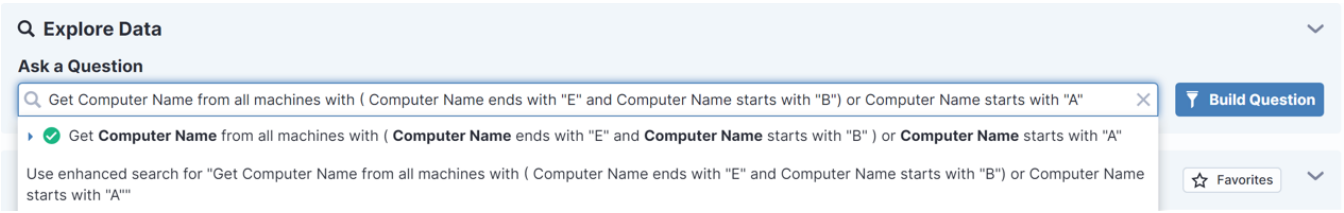
You can also specify nested filters in the **Ask a Question** field.

Figure 31: Nested filters in the Ask a Question field



The following example shows different Boolean logic: match both of these OR this one.

Figure 32: Nested filters in the Ask a Question field

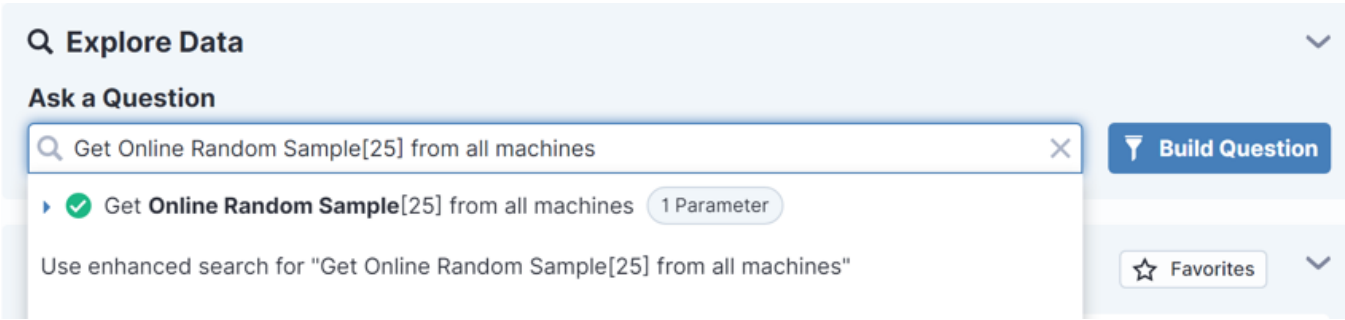


Target random endpoints

Use the **Online Random Sample** sensor to identify a random subset of online endpoints from all targeted endpoints. You might want to target random endpoints when you test a new package or configuration on a random subset of endpoints, or to check a random set of endpoints to ensure they have proper configurations prior to an audit. The **Online Random Sample** sensor is included in the content-only solution Default Content.

The **Online Random Sample** sensor retrieves `True` and `False` results from all targeted endpoints. The sensor accepts a **Sample %** parameter from 0-100 to determine the rough percentage of endpoints that answer with True. For example, if you pass 25 as a parameter and target `from all machines`, approximately 25% of endpoints in the environment will return a True response. Because each endpoint evaluates the sensor and generates a random True or False answer according to the percentage that you specify, the number of endpoints that return True can vary. The default value for **Sample %** is 5.

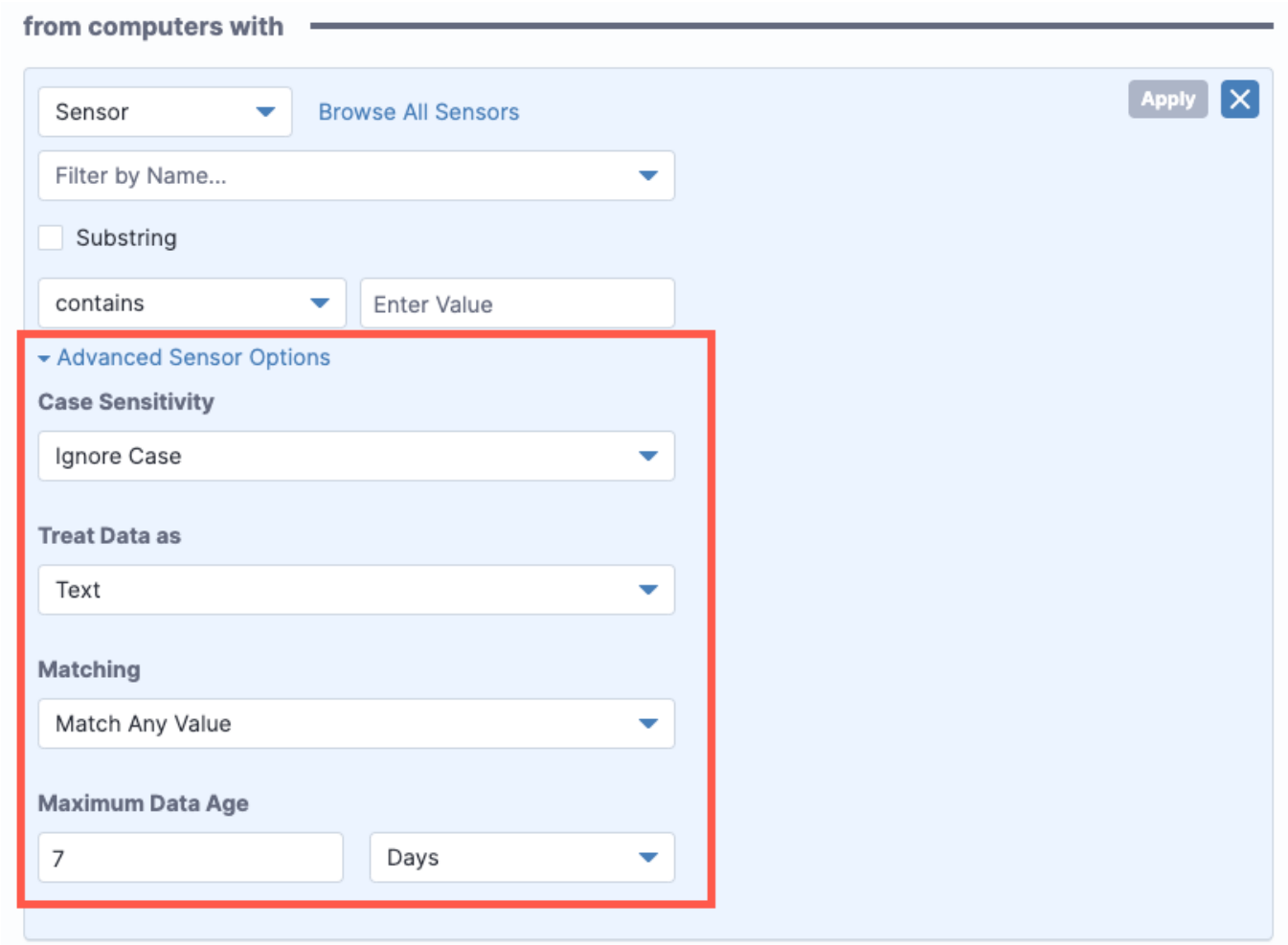
Figure 33: Online Random Sample sensor



Use advanced sensor options

Question results from Tanium Clients must conform with any advanced options that you specify for sensors in the question. You can configure advanced sensor options in the **Question Builder** (see Figure 34) or in the **Ask a Question** field (see the examples after Table 10).

Figure 34: Question Builder: Advanced sensor options



The following table describes the advanced sensor options:

Table 10: Advanced sensor options

Option	Guidelines
Case Sensitivity	Select whether Interact factors in upper-case and lower-case characters when grouping and counting question results: • **Ignore case** • **Match case** See Example: Case Sensitivity on page 109.

Table 10: Advanced sensor options (continued)

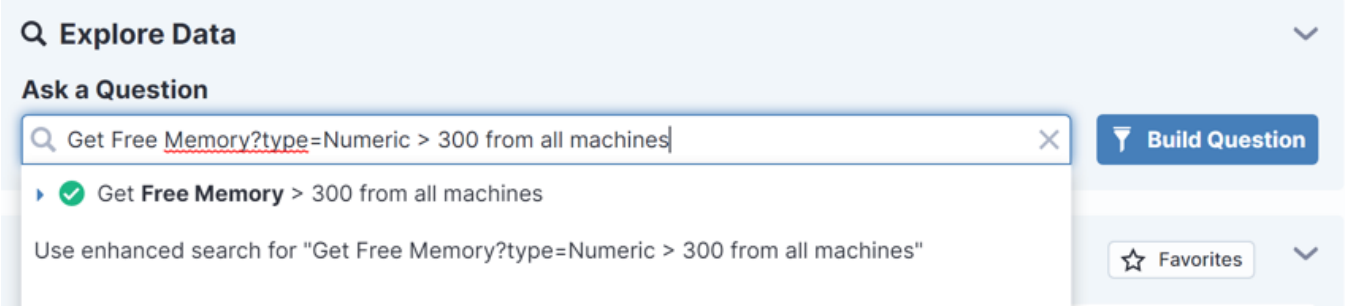
Option	Guidelines
Matching	This option is available only in the **from computers with** section of the **Question Builder**, which corresponds to the `from` clause of a question in the **Ask a Question** field. A Tanium Client might compute multiple results for certain sensors. For example, a client that has multiple interfaces returns multiple results for the **IP Address** sensor. You can use the **Matching** option as a filter such that a client answers the question only if its results conform to your selection: • **Match Any Value**: The client returns results if any of its results match the value that is specified in the question. • **Match All Values**: The client returns results only if all its results match the value that is specified in the question. See Example: Matching on page 109.
Treat Data As	Interact treats sensor values as the type of data that you specify. For a descriptions of the data types, see Tanium Console User Guide: Result Type. For an example, see Example: Treat data as type on page 107.
Maximum Data Age	Specify the maximum time for which the Tanium Client can use a cached result for the sensor, instead of reexecuting it for a fresh result, when answering questions. For example, you might specify 15 minutes for the **File Size** sensor. When a client receives a question that executes the **File Size** sensor, it caches the result. Over the next 15 minutes, if the client receives another question with the **File Size** sensor, it returns the cached result. After 15 minutes, if the client receives a question with the **File Size** sensor, it reexecutes the sensor script to return a fresh result. For an example, see Example: Maximum Data Age on page 108. To improve the accuracy of results, use shorter ages for sensors with values that change frequently, such as status and utilization sensors. To reduce unnecessary CPU usage on endpoints, use longer ages for sensors with values that typically do not change frequently, such as the chassis type or Active Directory domain membership. NOTE If you omit the **Maximum Data Age**, the **Max Sensor Age** setting in the sensor configuration determines the maximum time for cached results. See Tanium Console User Guide: Max Sensor Age. BEST PRACTICE Specify a **Maximum Data Age** only when issuing dynamic questions, not when creating saved questions or configuring endpoint membership in computer management groups and filter groups. Setting a **Maximum Data Age** that is lower than the **Max Sensor Age** increases CPU usage on endpoints.

The following examples describe how to enter advanced sensor options in the **Ask a Question** field using the syntax `<sensor>?<option>=<value>`.

Example: Treat data as type

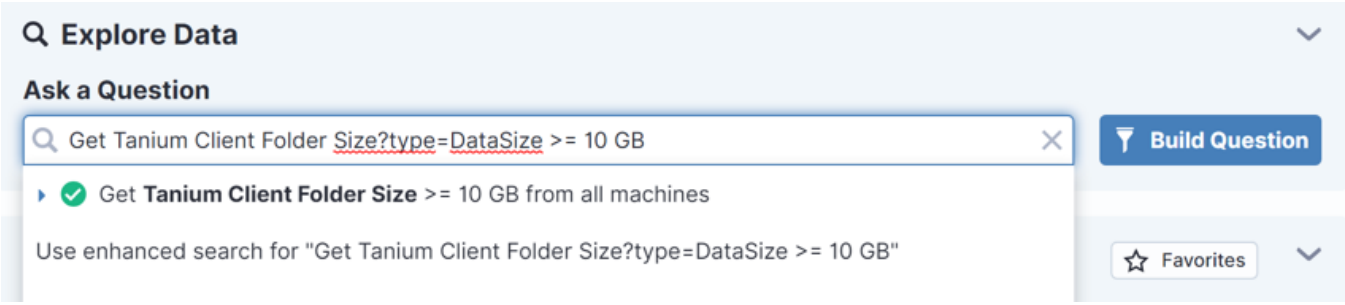
The syntax for filtering by data type is `<sensor>?type=<type>`. The following example specifies **Numeric** as the type.

Figure 35: Advanced Sensor Options: Treat Data as Numeric



The **File Size** data type in the **Question Builder** corresponds to the `DataSize` type in the **Ask a Question** field, where the syntax is `<sensor>?type=DataSize`. The following example returns results from endpoints where the installation folder of the Tanium Client is at least 10 GB.

Figure 36: Advanced Sensor Options: Treat Data as File Size



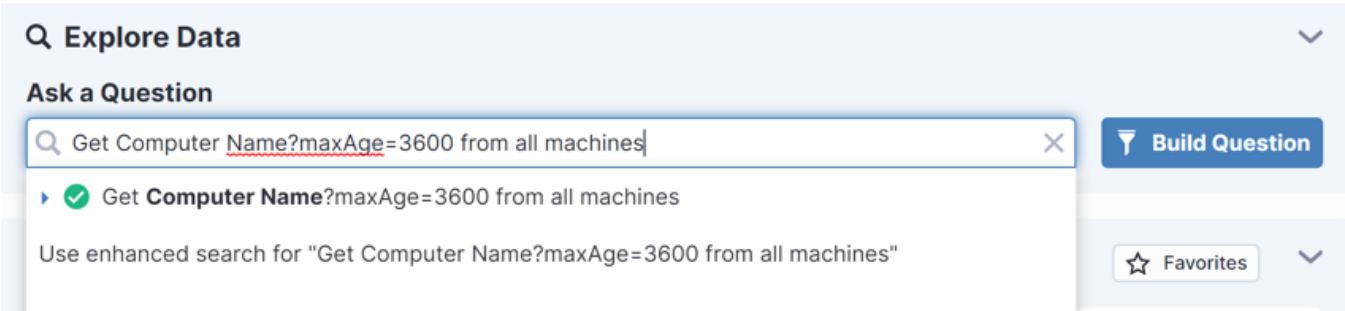
NOTE

Use the **Treat Data as *<type>*** option only with comparison operators, such as `Free Memory > 300`.

Example: Maximum Data Age

The syntax for setting the **Maximum Data Age** for cached results is `<sensor>?maxAge=<value>`. In the **Question Builder**, you can specify the age units (**minutes**, **hours**, **days**). In the **Ask a Question** field, the age is always in seconds. The following example specifies a maximum age of `3600` seconds.

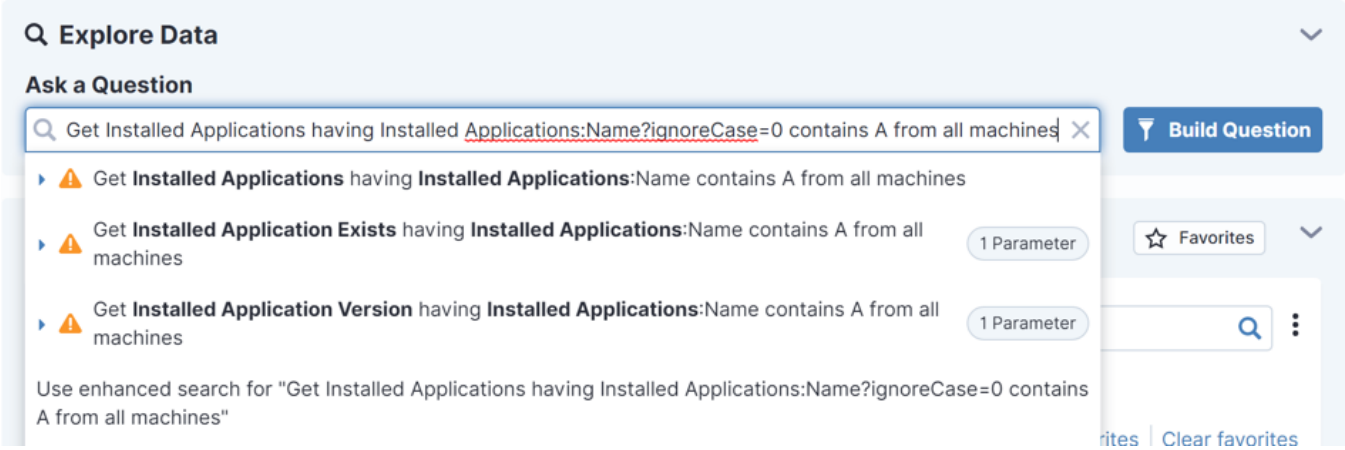
Figure 37: Advanced Sensor Options: Maximum Data Age



Example: Case Sensitivity

The **Case Sensitivity** option in the **Question Builder** corresponds to the `ignoreCase` option in the **Ask a Question** field, where the syntax is `<sensor>?ignoreCase=[0|1]`. The value `0` means match the case and the value `1` means ignore the case for sensor results with letters. The following example specifies the **Case Sensitivity** option with a value set to **Ignore Case**.

Figure 38: Advanced Sensor Options: ignore case



Example: Matching

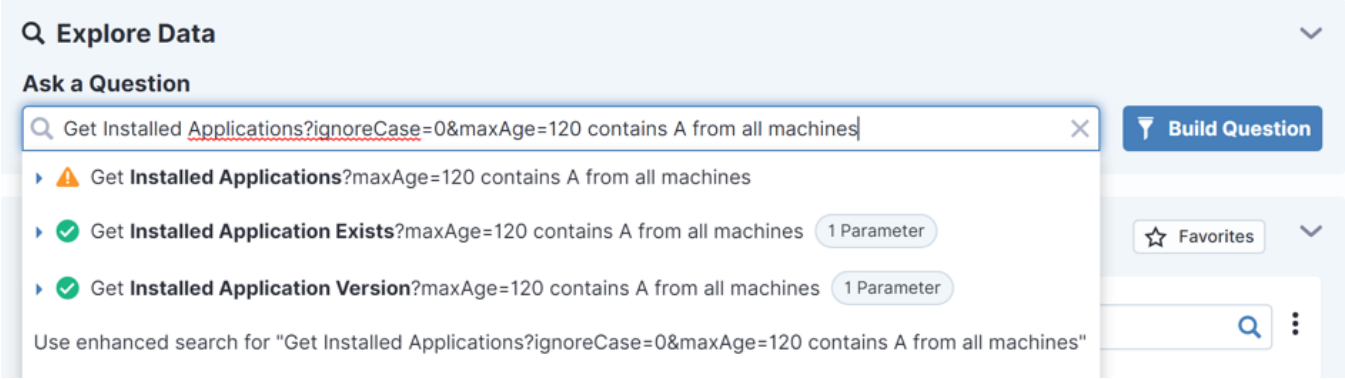
This **Matching** option applies only in the `from` clause of a question. The syntax for matching all or any results for a sensor is `with [all] <sensor> contains <value>`, where omitting the `all` option specifies **Match Any Value**. In the following example, the **Matching** option is set to **Match All Values** (`with all`) for the **IP Address** sensor. This example addresses a case where each endpoint might have multiple interfaces and you want to return results only from endpoints on which all the interfaces have an IP address that contains the string `192`.

Figure 39: Advanced Sensor Options: match all

Example: Multiple options

To specify multiple advanced options for a sensor, separate each option with an ampersand `&`. The syntax is `<sensor>?<option 1>=<value>&<option 2>=<value>...&<option N>=<value>`. The following example shows a question with two options for the **Installed Applications** sensor:

Figure 40: Advanced sensor options - multiple options



Use advanced question options

Enable the **Force Computer ID** option to convert a single-sensor, counting question into a non-counting question by forcing Tanium Clients to include the computer ID in their answers. Note that the **Question Results** page does not include the computer ID results when you select this option. Converting to a non-counting question is a workaround that resolves cases where a counting question returns the `too many results` answer. For details, see Enable or disable live updates on page 51. You can enable the option in the **Ask a Question** field by using the `Get?forceComputerIdFlag=1` statement. You can also enable the option in the **Question Builder**, under **Advanced Question Options**.

Change log

Date	Revision Summary
July 10, 2023	Removed "the" from instances of "Tanium Data Service".
July 6, 2023	Updated the version requirements for accessing Endpoint Details in Reporting.
June 20, 2023	Republished for 2.15.112
June 8, 2023	Republished for 2.15.111
June 5, 2023	Updated for PLATDOCS-1602
May 23, 2023	Republished for 2.15.102
May 2, 2023	Republished for 2.15.98
April 11, 2023	Republished for 2.14.137
April 4, 2023	Noted that Interact has a feature-specific dependency on Reporting.
March 14th, 2023	Republished for 2.14.129
February 28th, 2023	Republished for 2.14.125
February 15th, 2023	Republished for 2.14.118
February 7th, 2023	Republished for 2.14.114
January 10, 2023	Republished for 2.14.106
November 22, 2022	Republished for 2.13.126
November 15, 2022	Republished for 2.13.124
November 1, 2022	Updated for PLATDOCS-1368
October 18, 2022	Republished for 2.12.150
October 3, 2022	EOL for Tanium Core Platform 7.3
September 20, 2022	Republished for 2.12.145
August 30, 2022	Republished for 2.12.141
August 25, 2022	Updated for PLATDOCS-1399
August 9, 2022	Republished for Interact 2.12.131

Date	Revision Summary
June 28, 2022	Republished for Interact 2.12.119
June 14, 2022	Republished for Interact 2.12.114
June 6, 2022	Republished for Interact 2.12.113
May 24, 2022	Republished for Interact 2.11.64
May 10, 2022	Republished for Interact 2.11.62
April 19, 2022	Republished for Interact 2.11.58
March 29, 2022	Republished for Interact 2.11.52
March 15, 2022	Republished for Interact 2.11.49
February 8, 2022	Republished for Interact 2.9.91
January 27, 2022	Restructured Tanium dependencies in the Requirements chapter; no content changes
January 4, 2022	Republished for Interact 2.9.87
November 30, 2021	Republished for Interact 2.9.83
October 26, 2021	Republished for Interact 2.8.111
September 21, 2021	Republished for Interact 2.8.108
September 14, 2021	Republished for Interact 2.8.105
September 7, 2021	Added configuration section for predefined roles
July 27, 2021	Republished for Interact 2.7.217
July 13, 2021	Republished for Interact 2.7.215
June 29, 2021	Republished for Console 2.1 updates
May 18, 2021	Republished for Interact 2.6.114
April 27, 2021	Republished for Interact 2.6.108
April 1, 2021	Republished for Interact 2.6.107
March 16, 2021	Republished for Interact 2.6.102
February 9, 2021	Republished for Interact 2.5.167
November 24, 2020	Republished for Interact 2.5.161

Date	Revision Summary
November 2, 2020	Republished for Interact 2.5.137
September 15, 2020	Republished for Interact 2.4.50
August 18, 2020	Republished for Interact 2.4.48
July 2, 2020	Republished for Interact 2.3.4
June 16, 2020	Republished for Tanium Core Platform 7.4.3 release.
May 14, 2020	Republished for Interact 2.1.5 and 2.0.6.
April 7, 2020	Republished for Interact 2.0.5: addition of Core Content and Core MSSQL Content to Interact roles.
April 2, 2020	Updated content pack names: Initial Content packs become Default Content and Core Content.
February 25, 2020	Released 7.4.2 (common module import feature).
February 6, 2020	Released 7.4 GA for the Tanium Client.
January 28, 2020	Released 7.4 GA for Tanium Core Platform servers.
July 30, 2019	Updated for PLATDOCS-302 and PLATDOCS-306.
July 17, 2019	Changed the title of Table 3 in Interact role requirements.
July 2, 2019	Updated for 7.3-Next.
June 4, 2019	Updated for Interact 2.0.3 release.
February 22, 2019	Removed "Other Versions" section from all pages; only current version is available as HTML.
February 5, 2019	Updated for Interact 2.0.2 release.
December 17, 2018	Updated for DOC-885, DOC-884, DOC-873, DOC-872, DOC-868.
November 27, 2018	Republished for CUIC 1.3.1.0495.
November 6, 2018	Updated for 7.2 backport release.
September 18, 2018	Published for 7.3 release.
July 31, 2018	Update for 2.0.1 release.
June 29, 2018	Updated advanced questions topic.
May 15, 2018	Interact 2.0 initial release.