Tanium™ Performance User Guide

Version 1.1.0

November 21, 2019

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.

Tanium is a trademark of Tanium, Inc. in the U.S. and other countries. Third-party trademarks mentioned are the property of their respective owners.

Table of contents

Performance overview

With Performance, you can monitor, investigate, and remediate endpoint performance problems.

Configure profiles to define events for specified computer groups. You can define event rules to monitor critical metrics related to hardware resource consumption, application health, and system health.

You can visualize the problems that have occurred across your environment and the commonalities between them on the **Events** page. Proactively solving problems increases end user productivity.

If you are troubleshooting an issue or find an endpoint to investigate further, use Tanium™ Direct Connect. There, you can view historical process-level data from a single endpoint. This data can help you quickly troubleshoot or understand the impact of software and hardware changes on performance.

Profiles and Events

Profiles define events for specified computer groups. For each profile, you can select computer groups to monitor and rules that determine when an event occurs.

Events are generated when an endpoint experiences the conditions that you defined in an event rule in a profile.

When a profile targets an endpoint, tools are distributed to that endpoint to collect and monitor performance data. Data is collected every 15 seconds and stored for one week. This local data store is queried when you analyze events in Performance.

For example, you might want to know when available memory falls below a certain threshold on specific computers. You can create a profile with an **Available Memory is less than 250 MB** event rule and set the target for that profile to a computer group you want to monitor. When you analyze events in Performance, memory events are reported if any endpoints that you are targeting had less than 250 MB of available memory during the time frame (scope) that you selected for analysis.

The **Events** page displays charts that provide a high-level overview of events in the environment. You can also see a list of the specific endpoints that experienced a particular event (such as low memory) to identify and investigate issues in your environment. For more information, see Analyzing events.

Event rules

Event rules determine what conditions cause targeted endpoints to report events. Performance includes these event rules:

- **CPU Critical**
- **Available Memory**
- **Disk Capacity**
- **Disk Latency**
- **Application Crashes**

You can select heuristics for each event rule. For example, if you add the **Disk Latency** event rule, you can monitor **Read Latency** or **Write Latency**. If either heuristic is reached, the event rule is triggered.

For more information, see Reference: Event rules.

Direct Connect

Use Direct Connect to connect directly to a particular endpoint to troubleshoot an issue. For more information, see Connecting directly to endpoints.

Getting started

1. Install Performance. See Installing Performance on page 14.
2. Configure computer groups. See the Tanium Console User Guide: Managing computer groups.
3. Configure profiles. See Configuring profiles on page 18.
4. Analyze events that have occurred on monitored endpoints. See Analyzing events on page 20.
5. Use Direct Connect to troubleshoot performance problems on a specific endpoint. See Connecting directly to endpoints on page 28.

Performance requirements

Review the requirements before you install and use Performance.

Tanium dependencies

In addition to a license for the Performance product module, make sure that your environment meets the following requirements.

Component	Requirement
Tanium™ Core Platform Servers	Version 7.2 or later
Tanium™ Client	Version 7.2.314.3211 or later
Tanium Direct Connect	Version 1.1.0 or later (Optional; for connecting directly to an endpoint to view historical data)
Tanium™ solutions that use the Tanium™ Client Recorder Extension	If you are using any of the following Tanium solutions that use the endpoint recorder, you must use the specified versions: • Tanium™ Integrity Monitor 1.7.0.0035 or later • Tanium™ Map 1.1.1.0006 or later • Tanium™ Threat Response 1.2.0.0037 or later • Tanium™ Trace 2.9.0.0035 or later

Endpoints

Performance is supported on the following endpoint operating systems:

- Windows 7 and later
- macOS 10.11 and later
- Red Hat Enterprise Linux (RHEL) 6.x, 7.x
- CentOS 6.x, 7.x

Support for specific metrics varies by operating system. For more information, see Reference: Event Rules.

Host and network security requirements

Specific ports and processes are needed to run Performance.

Ports

The following ports are required for Performance communication.

Component	Port	Direction	Purpose
Module Server	17475	Inbound	Required only for Direct Connect. Used for connecting to the Module Server for direct connections to endpoints.

Security exclusions

A security administrator must create exclusions to allow Tanium processes to run without interference if security software is in use in the environment to monitor and block unknown host system processes.

Table 1: Performance security exclusions

Target device	Process
Tanium Module Server	`<Tanium Module Server>\services\performance\node.exe`
	`<Tanium Module Server>\services\event-service\twsm.exe`
Windows x86 and x64 endpoints	`<Tanium Client>\Tools\Performance\TaniumTSDB.exe`
macOS, and Linux x86 and x64 endpoints	`<Tanium Client>/Tools/Performance/TaniumTSDB`

User role requirements

Table 2: Performance user role privileges

Privilege	Performance Administrator	Performance Service Account	Performance User
Show Performance[1] View Performance workbench.	✓[2]	✗	✓[2]

Privilege	Performance Administrator	Performance Service Account	Performance User
Performance Administer View all pages in Performance. Update settings, profiles, and the service account credentials. Can generate and retrieve a support bundle.	✓	✗	✗
Performance Direct Connect Read[3] Connect to an endpoint using Direct Connect and read data from that endpoint.	✓[2]	✗	✓
Performance Event Read View performance events.	✓[2]	✗	✓

Privilege	Performance Administrator	Performance Service Account	Performance User
Performance Profile Read View performance profiles.	✓[2]	✗	✓
Performance Settings Read View performance settings.	✓[2]	✗	✓
Performance Components Manage Manage back-end components for Performance, such as actions.	✗	✓	✗

[1] To install Performance, you must have the reserved role of Administrator.

[2] Denotes an implicit permission that is provided by a privilege with a higher permission level. For example, a write permission provides an implicit read permission.

[3] Also requires the **Direct Connect Use API** privilege for the Direct Connect service.

Table 3: Provided Advanced user role permissions for Tanium 7.1.314.3071 or later

Permission	Content Set for Permission	Performance Administrator	Performance Service Account	Performance User
Ask Dynamic Questions		✓	✗	✓

Permission	Content Set for Permission	Performance Administrator	Performance Service Account	Performance User
Read Sensor	Reserved	✓	✗	✓
Read Sensor	Base	✓	✗	✓
Read Sensor	Performance	✓	✗	✓
Read Sensor	Hardware	✓	✗	✓
Read Plugin	Performance	✓	✓	✓
Execute Plugin	Performance	✓	✓	✓
Read Saved Question	Reserved	✓	✗	✓
Read Saved Question	Base	✓	✗	✓
Read Saved Question	Performance	✓	✗	✓
Read Saved Question	Hardware	✓	✗	✓

Installing Performance

Before you begin

- Read the release notes.
- Review the Performance requirements on page 9.
- You must be assigned the Administrator reserved role to import the Performance solution.

Import Performance

Import Performance from the **Tanium Solutions** page.

1. From the Main menu, click **Tanium Solutions**.
2. Under **Performance**, click **Import *Version***.
3. In the **Content Import Preview** window, you can expand the package to review the Tanium content that is being installed. Click **Import**.
4. Depending on your Tanium Server configuration, either enter your password or click **Yes** to proceed.
5. After the installation process completes, refresh your browser.
6. From the Main menu, click **Performance**. The Performance **Home** page displays.

Verify the installation

To verify that Performance is installed, go to the **Tanium Solutions** page and check the installed version. To check the installed version on the Performance **Home** page, click Info .

Configure Performance

> **Note:** If the **Configure Performance** section is not visible in the Performance **Home** page, click **Manage Home Page**, select **Configure Performance**, and click **Save**.

Configure the Performance action group

The action group defines the set of endpoints to which you are deploying the **Performance - Tools** package. By default, the **Computer Group Targets** setting for the Performance

action group is set to **No Computers**. Set the action group to **All Computers** or any computer group that you have defined.

As a best practice, include only endpoints with operating systems that are supported by Performance in this action group. If you include endpoints with unsupported operating systems, the **Endpoints without configuration** metric in the **Targeted Endpoint Status - Events Occurring Now** section might provide misleading information because those endpoints are included in the number.

> **IMPORTANT:** Only endpoints that are members of this action group can be targets of profiles because the **Performance - Distribute Tools [*<operating system>*]** action distributes the necessary tools exclusively to those endpoints. Metric collection begins when these tools and profiles are installed on an endpoint.

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Add Computer Groups** step and click **Add Computer Groups**.
2. Select the **Tanium Performance** action group.
3. Click **Edit**.
4. Select the computer groups that you want to include in the action group. If you select multiple computer groups, choose an operand (AND or OR) to combine the groups.
5. (Optional) In the **All machines currently included in this action group** section, review the included endpoints.

   > **Note:** These results might take a few moments to populate.
6. Click **Save**.
7. If prompted, enter your password and click **OK**.

Configure the Performance service account

You must create and configure a Performance service account to run several background processes, such as creating the actions to distribute the **Performance - Tools** package. This user must have the following roles and access configured:

- **Performance Components Manage** permission, which the **Performance Service Account** role provides.
- Access granted to the computer groups that provide input to Performance reports. For more information about assigning computer groups to a user, see Tanium Core Platform User Guide: Assign computer groups to a user.

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Configure Service Account** step and click **Configure Service Account**.
2. Enter the Tanium credentials and click **Set Credentials**.

> **Note:** You can also set or update the service account from the Performance settings. From the Performance **Home** page, click Settings ⚙, and update the service account settings in the **Service Account** section. Click **Set Credentials**.

For more information about Performance privileges, see User role requirements.

Import Missing Sensors

Performance utilizes several sensors that the **Initial Content - Hardware** content pack includes.

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Import Missing Sensors** step and click **Import Initial Content - Hardware**.
2. Click **Import**.
3. If prompted, enter your password and click **OK**.

Configure Profiles

Profiles define performance events for specified computer groups.

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Configure Profiles** step and click **Go to Profiles**.
   The **Profiles** page displays.
2. Create and prioritize profiles. For more information, see Configuring profiles.

(Optional) Install and configure Direct Connect

If you want to connect directly to endpoints to see live and historical performance data, install and configure Direct Connect.

> **Note:** You must have the **Performance Direct Connect Read** and **Direct Connect Use API** privileges to use Direct Connect in Performance.

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Install Direct Connect** step and click **Install Direct Connect**.
2. Click **Import**.

3. If prompted, enter your password and click **OK**.
4. Configure Direct Connect. You must configure Direct Connect before you can connect to endpoints from Performance. For more information, see Direct Connect User Guide: Configure Direct Connect.

For more information about using Direct Connect with Performance, see Connecting directly to endpoints.

Upgrade Performance

Upgrade Performance to the latest version from the **Tanium Solutions** page.

1. From the Main menu, click **Tanium Solutions**.
2. Locate Performance and click **Upgrade to *X.X.X.XX***.
3. Click **OK**.
   The **Import Solution** window opens with a list of all the changes and import options.
4. Click **Proceed with Import**.
5. Depending on your Tanium Server configuration, either enter your password or click **Yes** to proceed.
   The Tanium Performance installation and configuration process begins.
6. To confirm the upgrade, return to the **Tanium Solutions** page and check the **Installed: *X.X.X.XX*** version for Performance.

What to do next

See Getting started on page 8 for more information about using Performance.

Configuring profiles

Profiles define events for targeted computer groups. For each profile, configure event rules and select the target computer groups to which the event rules apply.

> **Note:** Profiles and the event rules that they contain do not determine what data is collected on endpoints. The same data is monitored on all endpoints that a profile targets. Profiles determine which conditions on the endpoint generate a negative performance event.

For the best results, try to minimize the total number of profiles in your environment. For example, you might want to have two profiles: one for standard workstations and one for high-profile workstations because you want to set stricter thresholds for the heuristics on high-profile workstations. As a best practice, do not create multiple profiles with the same event rules and thresholds as a way to organize the endpoints that you are monitoring because you can analyze events using computer groups as a filter instead.

Create a profile

1. From the Performance menu, click **Profiles > Create Profile**.
2. In the **Details** section, specify the **Profile Name** and **Description**.
3. In the **Target** section, select the computer groups to which the event rules in this profile apply.
4. In the **Event Rules** section, configure rules that determine when the targeted endpoints report events. The available event rules are **CPU Critical**, **Application Crashes**, **Disk Latency**, **Available Memory**, and **Disk Capacity**.

   > **Note:** You must select at least one event rule for the profile. For more information about event rules, see Reference: Event Rules.

5. Click **Save**.

When you save a profile, packages and scheduled actions are created to distribute the profile to endpoints. The profiles should be distributed within an hour, and metric monitoring and collection begins after the profile is placed on an endpoint. Any events that occur on the targeted endpoints based on the configured profile display on the **Events** page. For more information, see Analyzing events.

Set the priority of profiles

All profiles are exclusive, meaning that only one profile can be in effect on an endpoint at a given time. If you target multiple profiles with the same event rules to a particular endpoint, Performance must resolve the conflict to decide which profile to apply.

If two or more profiles target and endpoint with the same event rules, only the highest priority profile is applied.

Set the prioritization of profiles to determine which profile is applied if a conflict exists. The **Profiles** page shows the current priority for each profile.

1. From the Performance menu, click **Profiles > Prioritize Profiles**.

   > **Note:** The **Prioritize Profiles** button displays only when you have two or more profiles configured.

2. Drag and drop the profiles into the order that you want. The profile with the highest priority is at the top of the list.
3. Click **Save**.

Modify a profile

1. From the Performance menu, click **Profiles**.
2. Click Edit in the row for the profile that you want to edit.
3. Modify the profile.
4. Click **Save**.

Delete a profile

1. From the Performance menu, click **Profiles**.
2. Click Delete in the profile.

Analyzing events

A targeted endpoint reports an event after experiencing the conditions that you defined in an event rule in a profile. The **Events** page displays charts that provide more information about events in your environment.

View the Events page

1. From the Performance menu, click **Events**.
2. Specify the computer group for which you want to see events in the **Define Computer Groups** parameter.
3. Select a time period for the displayed events from the **Scope** menu:
    - **1 hour**
    - **4 hours**
    - **8 hours**
    - **1 day**
    - **2 days**
    - **1 week**
4. If you changed the default values, click **Get Results**.

The **Events** page refreshes and displays the events that match the specified parameters.

The **Events** page displays only events that occurred on endpoints a profile targeted during the specified **Scope**. If no events occurred during the specified scope, or no profile is configured to monitor for events of that type, the chart for that event type displays **No data to display**.

Targeted Endpoint Status

The **Targeted Endpoint Status - Events Occurring Now** section displays a high-level overview of the current status of targeted endpoints.

> **Note:** Unlike the rest of the **Events** page, the **Targeted Endpoint Status - Events Occurring Now** section displays the current state of endpoints in your environment that are targeted by a profile, not in the time frame that you selected in the **Scope** parameter.

Total Targeted Endpoints

Displays the total number of endpoints that you are targeting in the computer group that you specified in the **Define Computer Groups** parameter.

Endpoints with events

Displays the total number of endpoints in the specified computer group that reported an event.

Endpoints without configuration

Displays the total number of endpoints in the specified computer group that do not have the necessary configuration in place for metric collection. They might not be targeted by a profile, or they might be missing the Performance tools.

Endpoints without events

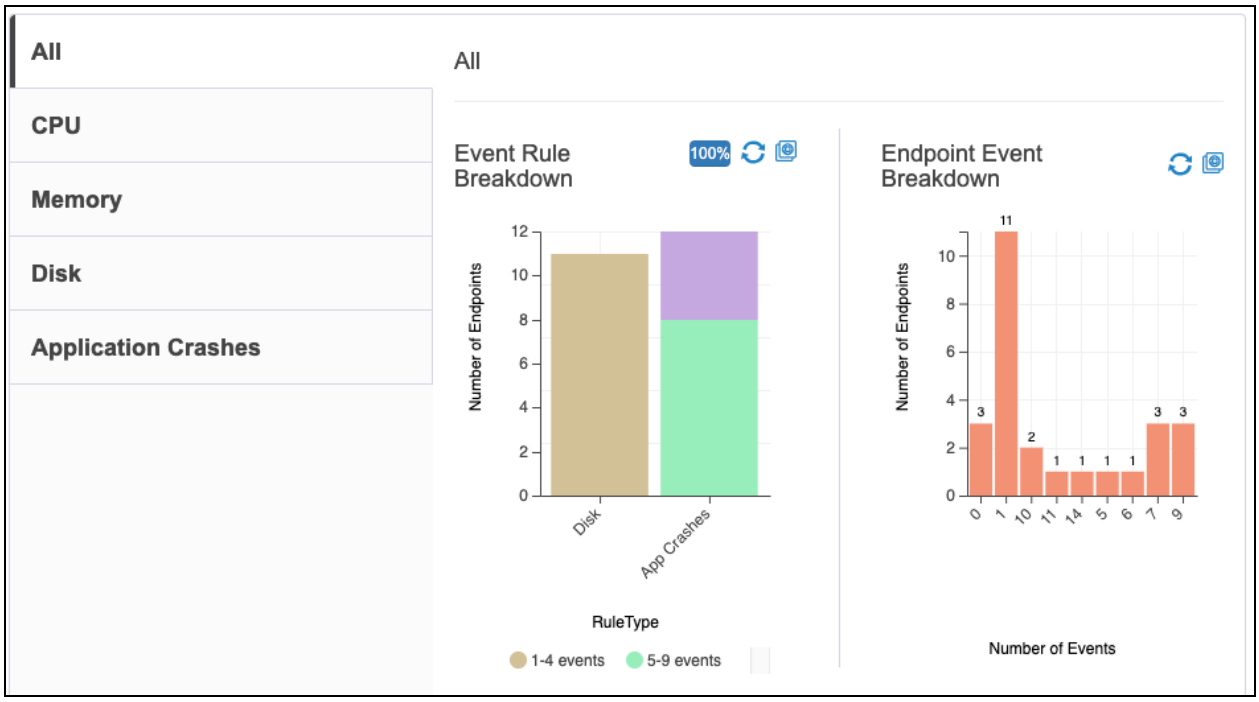
Displays the total number of endpoints in the specified computer group that have not reported any events.

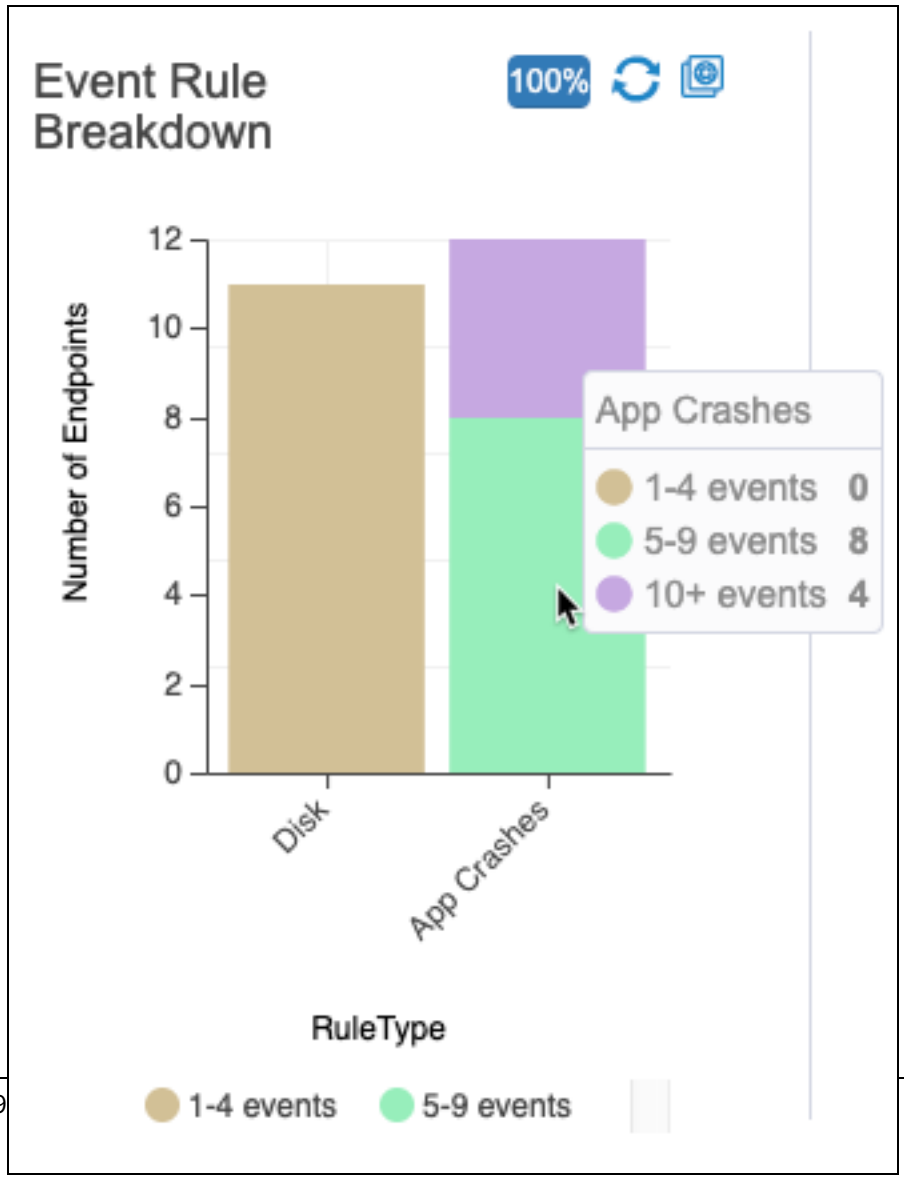
View all events

Click the **All** tab in the charts section to display charts with all reported events for the defined computer groups during the time frame that you selected in the **Scope** parameter. Two charts display that show a summary of the reported events:

Event Rule Breakdown

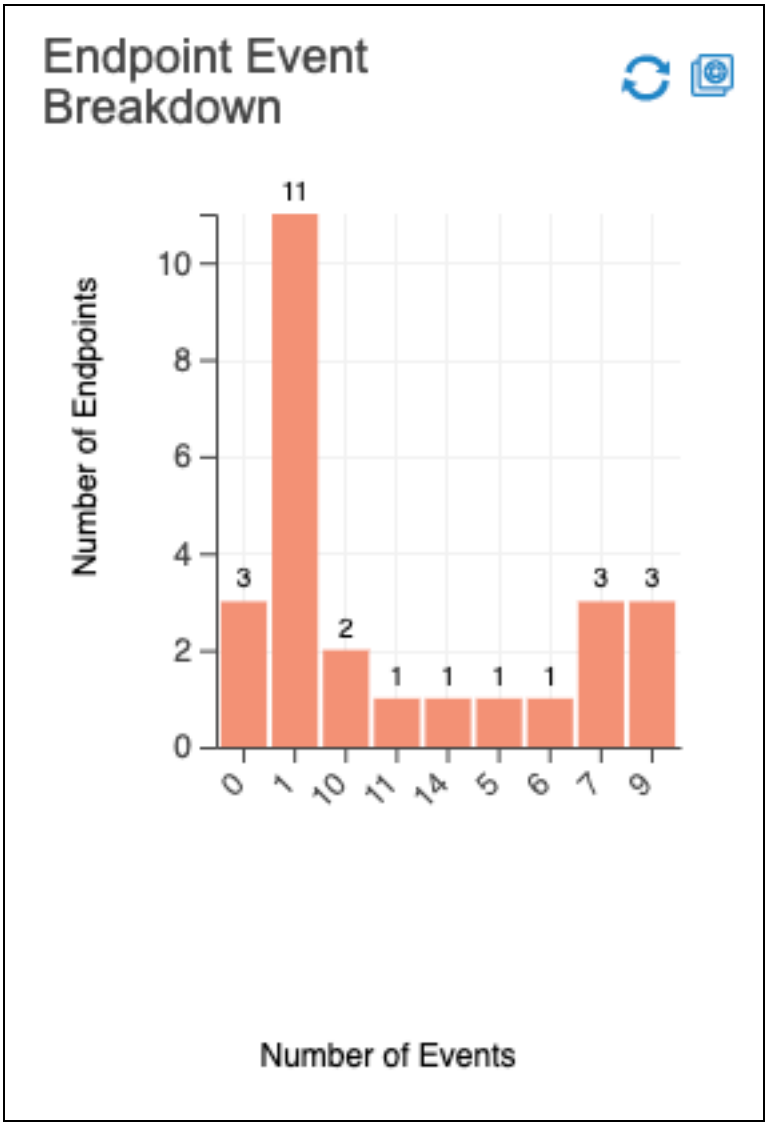
This chart displays the number of endpoints that reported each type of event: **Disk**, **App Crashes**, **Network**, **Memory**, and **CPU**. Each bar in the bar chart is color coded to indicate how many events of that type were reported by each endpoint. For example, the beige portion of the bar indicates the number of endpoints that reported 1-4 events. Hover your mouse over the bar to see a breakdown of the number of events per endpoint.


All
CPU
Memory
Disk
Application Crashes
All
Event Rule Breakdown
100%
Number of Endpoints
12
10
8
6
4
2
0
Disk
App Crashes
RuleType
1-4 events
5-9 events
Endpoint Event Breakdown
Number of Endpoints
11
3
2
1
1
1
1
3
3
0
1
10
11
14
5
6
7
9
Number of Events


Event Rule Breakdown
100%
Number of Endpoints
12
10
8
6
4
2
0
Disk
App Crashes
App Crashes
1-4 events 0
5-9 events 8
10+ events 4
RuleType
1-4 events
5-9 events

Endpoint Event Breakdown

This chart displays the total number of events by the number of endpoints. Use this chart to quickly identify the endpoints that are having the most problems in the defined computer group.



View CPU events

Click the **CPU** tab in the charts section to display charts that provide more information about endpoints in the defined computer groups that reported CPU events during the selected time frame. These charts are designed to help you find patterns and commonalities among the endpoints that are having issues in your environment. Two charts display that show a summary of the reported events:

Process associated

This chart shows specific processes and the number of CPU events that are associated with each of those processes.

The process that consumes the highest amount of CPU for the duration of the event is reported as the process associated with the event. Consider an example where you create an event rule in a profile to trigger an event if the CPU use is above 90% for longer than 10 minutes. The CPU on an endpoint that is targeted by that profile has CPU usage at 95% for an hour, which generates a performance event. The highest process consumer during that hour was `badprocess.exe`. Because `badprocess.exe` was the highest CPU consumer during that event, it is reported as the process that is associated with the event in the chart. If several endpoints are reporting events that are associated with `badprocess.exe`, you can investigate this process further. For example, perhaps a recent upgrade touched this process and the associated program needs to be tuned, or perhaps anti-virus software settings are not configured correctly.

Models with Events

This chart displays the model of the endpoint that reported an event. Hover over a slice in the pie chart to see the exact number of endpoints with that model that reported an event.

View memory events

Click the **Memory** tab in the charts section to display charts that provide more information about endpoints in the defined computer groups that reported memory events during the selected time frame. Two charts display that show a summary of the reported events:

Process associated

This chart shows specific processes and the number of memory events that are associated with each of those processes.

The process that consumes the highest amount of memory for the duration of the event is reported as the process associated with the event. Consider an example where you create an event rule in a profile to trigger an event if the available memory is less than 50 MB for longer than 10 minutes. The memory on an endpoint that is targeted by that profile has only 40 MB of free memory for an hour, which generates a performance event. The highest memory consumer during that hour was `badprocess2.exe`. Because `badprocess2.exe` was the highest consumer of memory during that event, it is reported as the process that is associated with the event in the chart.

Models with Events

This chart displays the model of the endpoint that reported an event. Hover over a slice in the pie chart to see the exact number of endpoints with that model that reported an event.

View disk events

Click the **Disk** tab in the charts section to display a chart that provides more information about endpoints in the defined computer groups that reported disk events during the selected time frame. One chart displays that shows a summary of the reported events:

Models with Events

This chart displays the model of the endpoint that reported an event. Hover over a slice in the pie chart to see the exact number of endpoints with that model that reported an event.

View application crashes

Click the **Application Crashes** tab in the charts section to display charts that provide more information about endpoints in the defined computer groups that reported application crashes during the selected time frame. Two charts display that show a summary of the reported events:

Models with Events

This chart displays the model of the endpoint that reported an event. Hover over a slice in the pie chart to see the exact number of endpoints with that model that reported an event.

Application Crashes

This chart shows specific processes and the number of crashes that are associated with each of those processes.

Load endpoints

Below any chart, click **Load Endpoints with *[event type]*** to display a list of the endpoints that reported that event. Use the **Filter Events** section to filter the results based on **Model** or **Operating System**.

Customize the results display

Click **Customize Columns** to add or remove columns from the results table. Possible columns are:

- **Events** (The number of events for the selected chart, **All**, **CPU**, **Memory**, **Disk**, or **Application Crashes**, that occurred during the selected **Scope**)
- **Computer Name**
- **IP Address**
- **Total Memory**
- **Operating System**
- **Model**
- **Top Processes** (The processes that consume the highest amount of memory or CPU, depending on the chart that is selected, for the duration of the event are reported as

the top processes associated with the event)

- **Action** (If you installed Direct Connect, provides a link to connect to the endpoint)

Drag and drop the items in the **Displayed Columns** list to change the order of the columns in the results table. Click a column header to sort the results by that column.

Connect directly to an endpoint

Click Connect to *hostname* in the **Action** column to connect directly to the endpoint for further troubleshooting.

> **Note:** You must have the Direct Connect solution installed and configured to use this action. For more information, see Connecting directly to endpoints.

View in Tanium Interact

Click View question results in Interact to open a question in the Tanium™ Interact **Question Builder** that returns the results that were displayed in the chart or list where you clicked the button.

You might want to use this feature to refine the data that is returned or to schedule an action on the endpoints. For more information about working with the **Question Builder**, see Tanium Console User Guide: Using the Question Builder. This button is available in the event charts and lists of endpoints on the **Events** page.

Connecting directly to endpoints

Use Direct Connect to connect directly to an endpoint to troubleshoot an issue with historical data. You can use this data to:

- Understand performance events that occured on that endpoint.
- Visualize process-level resource consumption data from the time of an incident.
- See what processes are currently running and the resources they are consuming.
- Access important attributes about the endpoint (such as CPU model, memory capacity, and disk drive type).

Create a direct connection

Connect directly to an endpoint from the **Direct Connect** page.

1. From the Performance menu, click **Direct Connect**.
2. Enter the Computer Name (as it displays in the Computer Name sensor) or IP address for the endpoint in the **Create a Direct Connection** field.
3. Click **Connect**.

The page displays detailed information about the endpoint:

The ribbon at the top of page displays the **Hostname**, **IP Address**, **Computer ID**, **Serial Number**, **Operating System**, **Model**, **Cores**, **CPU Speed**, **Total Memory**, and **Disk Total Space** for the endpoint.

Charts display that show Events, Live Process Monitor, CPU, CPU Usage By Process, Memory, Memory Usage By Process, Network, Disk, IO Usage By Process, and Application Crashes (only Windows endpoints).

You can also connect to an endpoint from Performance by clicking Connect to *hostname* in the **Action** column of a chart. For more information, see Connect directly to an endpoint.

Troubleshooting Performance

To collect and send information to Tanium for troubleshooting, collect log and other relevant information.

Collect logs

The information is saved as a compressed ZIP file that you can download with your browser.

1. From the Performance home page, click Help ❓, then the **Troubleshooting** tab.
2. Collect the troubleshooting package. Click **Generate Support Package**. When the ZIP file is ready, click **Download Support Package**.
3. Attach the ZIP file to your Tanium Support case form or send it to your TAM.

Check the action group

Performance requires two actions to report metrics from an endpoint:

> First, an action must run to install the performance tools on the endpoint. This action should run about an hour after an endpoint is added to a computer group that is included in the Performance action group. The scheduled action is named `Performance - Distribute Tools [Operating System]`.
>
> Second, when a profile is saved, an action must run to drop the profile (if it is new) or update the profile (if it is modified) on the targeted endpoints. This action should run about an hour after the profile is created or modified. The name of this scheduled action is `Performance - Profile Profile Name - [Operating System]`.

Complete these steps to verify the computer groups that are included in the Performance action group:

1. From the Performance **Home** page, in the **Configure Performance** section, click the **Add Computer Groups** step and click **Add Computer Groups**.
2. Select the **Tanium Performance** action group.
3. Review the computer groups that are listed in the **Computer Group Targets** field.
4. If needed, click **Edit** to make changes.
5. If you made changes, click **Save**.

Uninstall Performance

If you need to uninstall Performance, first clean up the Performance artifacts on endpoints and then uninstall Performance from the server.

Remove Performance content and tools from endpoints

Each operating system has its own remove action. Therefore, you must select a group of endpoints for cleanup that has the same operating system.

1. From the Main menu, click **Interact**.
2. Ask a question to target the endpoints from which you want to remove Performance content and tools. For example, `Get Performance - Tools Version from all machines`.
3. Select the row for the endpoints from which you want to remove the Performance profile (**Windows Package Installed**, **Mac Package Installed**, or **Linux Package Installed**).
4. Click **Deploy Action**.
5. On the **Deploy Action** page, enter `Performance - Remove` in the **Enter package name here** field.
6. Select the **Performance - Remove Profile *operating system*** action, where *operating system* matches the operating system of the endpoints that you selected.
7. Click **Show preview to continue**.
8. A results grid displays at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.
9. Return to Interact. If your question results are still available, select the row for the endpoints from which you want to remove the Performance tools. If they are not, reissue the `Get Performance - Tools Version from all machines` question and then select the appropriate row.
10. On the **Deploy Action** page, enter `Performance - Remove` in the **Enter package name here** field.
11. Select the **Performance - Remove Tools *operating system*** action, where *operating system* matches the operating system of the endpoints that you selected.
12. Click **Show preview to continue**.
13. A results grid displays at the bottom of the page showing you the targeted endpoints for your action. If you are satisfied with the results, click **Deploy Action**.

Remove the Performance solution from the Tanium Module Server

1. From the Main menu, click **Tanium Solutions**.
2. In the Performance section, click **Uninstall**.
3. Review the content that will be removed and click **Uninstall**.
4. Depending on your configuration, enter your password or click **Yes** to start the uninstall process.
5. Return to the **Tanium Solutions** page and verify that the **Import** button is available for Performance.

Note: By design, the uninstall process does not remove Performance content (actions, packages, saved questions, and sensors) so that other solutions are not impacted if they use this content. If you are sure that this content is not being used by any other solutions, you can manually remove it.

Reference: Event Rules

Use event rules to specify the heuristic parameters for which the targeted endpoints report performance events.

You can configure these event rules:

- CPU Critical
- Application Crashes
- Disk Latency
- Available Memory
- Disk Capacity

Some event rules have multiple parameters, such as **CPU Critical**. This event rule has two rule blocks for Windows endpoints:

1. **CPU Kernel Time**, which contains **CPU Utilization** and **Kernel Time**
2. **DPC Time**

Within the **CPU Kernel Time** event rule block, the two heuristics (**CPU Utilization** and **Kernel Time**) are joined by a Boolean `AND`, meaning both conditions must meet the specified thresholds to generate an event. Within the **CPU Critical** event rule, if you choose to monitor both **CPU Kernel Time** and **DPC Time** (two separate event rule blocks), they are joined by a Boolean `OR`, meaning that an event is generated if either condition meets the specified thresholds.

If you add multiple event rules to a profile, such as **CPU Critical** and **Application Crashes**, the event rules are joined by a Boolean `OR`, meaning that an event occurs if the conditions for any of the event rules are met.

> **Note:** Profiles and the event rules that they contain do not determine what data is collected on endpoints. The same data is monitored on all endpoints that a profile targets. Profiles determine which conditions on the endpoint generate a negative performance event.

After you add an event rule to a profile, select and configure the heuristics that you want to monitor.

CPU Critical

The **CPU Critical** event rule contains three heuristics:

1. **CPU Kernel Time** monitoring is supported Windows, macOS, and Linux endpoints. With this heuristic, you can monitor:
   - **CPU Utilization**: Monitor CPU utilization to detect CPU contention.
   - **Kernel Time**: Monitor kernel time to detect when the CPU is spending too much time on kernel mode operations.

     CPUs operate in two modes: kernel mode and user mode. Kernel mode is typically used for core operating system functions, I/O, and filter driver operations. If the CPU on an endpoint spends the majority of time on kernel mode operations, little CPU time is available for user mode operations, which might cause a negative performance condition.

     > **Note:** If you configure an event rule for **CPU Kernel Time**, the **CPU Utilization** and **Kernel Time** for targeted endpoints are monitored for the specified thresholds. A performance event occurs if the CPU utilization and kernel time are greater than the percentages that you configure in the event rule (both conditions must be met for an event to occur).

2. **DPC time** monitoring is supported only for Windows endpoints.

   If you configure an event rule for **DPC time**, processor DPC for targeted endpoints is monitored. Specify the highest DPC time that is allowed on an endpoint before a performance event occurs. An unusually high amount of time spent on deferred procedure calls on an endpoint could indicate a processor bottleneck or driver problem.
3. **Load Average** monitoring is supported only for macOS and Linux endpoints.

   If you configure an event rule for **Load Average**, the load average for targeted endpoints is monitored. Specify the load average that is allowed on an endpoint before a performance event occurs.

   The load average is an exponential average of the number of processes in a running or waiting state. This metric is a standard UNIX method for detecting CPU contention. This rule monitors the 15 minute load average for the CPU. If the load average is equal to the number of cores on an endpoint, the CPU usage is at its maximum capacity.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

Note: If you choose to monitor both **CPU Kernel Time** and **DPC time** (Windows endpoints) or both **CPU Kernel Time** and **Load Average** (macOS and Linux endpoints), a performance event occurs if either of the metrics meet the specified conditions for the specified duration.

Application Crashes

You can monitor this event rule only on Windows endpoints.

This event rule monitors the Windows Event Log for targeted endpoints. An event occurs if an application crashes.

Disk Latency

You can monitor this event rule on Windows, macOS, and Linux endpoints.

You can create event rules for **Read Latency**, **Write Latency**, or both.

Disk latency is a measurement of the average amount of time that a disk operation (read or write) takes to complete. Acceptable values vary based on the type of drive.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

Note: If you choose to monitor both **Read Latency** and **Write Latency**, a performance event occurs if either metric meets the specified condition for the specified duration.

Available Memory

You can monitor this event rule on Windows, macOS, and Linux endpoints.

You can create event rules for available memory by MB, percentage of total memory, or both.

Available Memory is a measurement of the amount of memory available to be immediately allocated to programs. Paging occurs when an endpoint runs low on available memory, which puts a load on disks and might result in workstation slowdowns or hangs. Monitor available memory to detect when programs might not have enough available memory to run without paging.

In the **Duration** field, specify the amount of time that the specified conditions must be present to trigger a performance event.

> **Note:** If you choose to monitor available memory by both MB and percentage of total memory, an event occurs if either metric meets the specified condition for the specified duration.

Disk Capacity

You can monitor this event rule on Windows, macOS, and Linux endpoints.

You can create an event rule for free disk space by MB, percentage of total disk capacity, or both.

Disk capacity is a measurement of the free space on the disk. When disks run low on space, fragmentation increases. Fragmented disks contribute to slow response times.

> **Note:** If you choose to monitor free disk space by both MB and percentage of total disk capacity, an event occurs if either metric meets the specified conditions.