Tanium Maintenance User Guide

Version: All

May 23, 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

Getting started with Tanium maintenance

After you set up a Tanium deployment, perform regular maintenance tasks to ensure that the deployment uses resources efficiently and provides the best user experience. This guide is intended to provide a baseline of recommended maintenance tasks for all Tanium deployments at various intervals. For example, the recommended tasks alert you to changes in your network, tools deployment, and role-based access control (RBAC) assignments. The specifics of your environment might require different tasks and different intervals, and both might change over time. Contact Tanium Support on page 10 if you need help determining the appropriate maintenance tasks or help troubleshooting issues that you discover during maintenance.

Perform the one-time tasks described in the following sections to facilitate regular maintenance.

Back up your deployment

Create a disaster recovery plan and back up the Tanium™ Core Platform servers and databases so that you can restore your deployment to a known functional state in case of issues. For example, if a system failure makes the host system of the Tanium™ Server unrecoverable, you can use a backup to quickly restore functionality on a new host.

The backup procedure depends on your Tanium infrastructure:

- Tanium Appliance Deployment Guide: Reference: TanOS backup and recovery
- Tanium Core Platform Deployment Guide for Windows: Back up Tanium Core Platform servers and databases

NOTE

Review and update backups and the disaster recovery plan on page 35 during quarterly maintenance.

Test disaster recovery on page 43 during annual maintenance.

Configure RBAC for maintenance tasks

Decide which users are responsible for performing Tanium maintenance tasks and assign the required roles, user groups, personas, and computer groups. For example, users can apply custom tags only to endpoints in computer groups that are assigned to their user accounts. Users who then configure computer groups with tag-based membership require **Computer Group** write permission, **Interact Module** write permission, and **Sensor** read permission.

To assign Tanium-defined roles or to create and assign custom roles, see Tanium Console User Guide: Managing roles. For the Tanium™ solution-specific role permissions that are required to perform maintenance tasks, see the corresponding user guides:

- API Gateway
- Asset
- Benchmark
- Certificate Manager
- Client Management
- Comply

- Connect
- Criticality
- Deploy
- Direct Connect
- Directory Query
- Discover
- Endpoint Configuration
- End-User Notifications
- Enforce
- Engage
- Feed
- Health Check
- Impact
- Integrity Monitor
- Interact
- Map
- Patch
- Performance
- Provision
- Reporting
- Reputation
- Reveal
- Threat Response
- Trends

Verify TPAN report generation

The Tanium™ Platform Analyzer (TPAN) report can facilitate future troubleshooting regardless of whether your deployment currently has issues. If your Tanium license includes Tanium™ Health Check, verify that it is configured to generate TPAN reports:

1. From the Main menu, go to **Administration > Shared Services > Health Check**.
2. Scroll to the **Reports** section and verify that TPAN reports are generated at the expected cadence.
3. If TPAN reports are not generated as expected, see:
   - Tanium Health Check User Guide: Configuring Health Check
   - Tanium Health Check User Guide: Generating reports

Configure Tanium™ Appliance monitoring

Perform any of the following tasks to facilitate monitoring the health of your Tanium deployment if it uses Appliance infrastructure. For example, if your organization has a syslog server or SNMP manager, you can integrate it with the Appliance for monitoring. If these monitoring solutions reveal issues that require resolution, see Tanium Appliance Deployment Guide: Troubleshooting.

Configure TanOS alerts

TanOS can send alerts to a syslog server or to an email recipient. For optimal results, configure an SMTP email recipient. If the syslog server fails, the SMTP recipient receives a failure notification every 15 minutes until either the failure is resolved or syslog forwarding is disabled. See Tanium Appliance Deployment Guide: Configure alerts.

Configure syslog forwarding

You can forward Appliance logs to a remote syslog server. The syslog forwarding configuration is separate from the syslog alert configuration. For the differences, and the steps to configure syslog forwarding, see Tanium Appliance Deployment Guide: Configuring syslog.

Configure SNMP

You can configure integration with an SNMP manager to collect and analyze Appliance information. After you configure credentials, the user `tansnmp` can make a remote SNMP connection to the Appliance or to the Integrated Dell Remote Access Controller (iDRAC) interface of a physical Appliance to conduct SNMP polling from a remote host or SNMP manager. See Tanium Appliance Deployment Guide: Configuring SNMP.

Configure alerts for disconnected Tanium™ Clients

Users with local administrative rights might be able to uninstall the Tanium Client, stop the Tanium Client service, or tamper with Tanium Client files. In such cases, previously managed endpoints might become unmanaged. Configure Tanium™ Discover to regularly audit endpoints to which you have deployed the Tanium Client and configure Tanium™ Connect to automatically generate alerts when endpoints become unmanaged. You can also configure Tanium Discover to automatically redeploy the Tanium Client to endpoints that become unmanaged. For the steps, see Tanium Client Management User Guide: Configure automated maintenance.

Configure a failed connections report

If you use Tanium Connect, you can configure an HTTP destination to schedule the automatic delivery of reports about failed connections. You can set the report format to CSV, delimiter separated values, HTML, or JSON.

If you have the authority to disable or delete failed connections, configuring the report is optional. You can use the report for reviewing and troubleshooting connections before you decide which to disable or delete. Alternatively, you can manually Review and remediate Tanium Connect issues on page 23 without a report.

If another team in your organization has the authority to disable or delete failed connections, configure the report with the settings that the team requires.

Configure the report as described in Tanium Connect User Guide: Configuring HTTP destinations. A failed connections report requires the following settings:

Table 1: HTTP destination for failed connections report

Section	Settings
Configuration	• **Source**: **Event** • **Event Group**: **Connect** • **Failed Connection Run**: select • **Unexpected Process Exit**: select • **Destination**: **HTTP**
Enablement	**Listen for this Event**: select

Contact Tanium Support

Tanium Support is your first contact for assistance with troubleshooting your deployment. If you require further assistance from Tanium Support, include version information for Tanium Core Platform components and specific details on dependencies, such as the host system hardware and OS details and database server version. You can also send Tanium Support a collection of support bundles for all the solutions in your Tanium license. See Review and update backups and the disaster recovery plan on page 35.

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

Performing weekly maintenance

Review and resolve critical and high TPAN findings

Check the TPAN report for critical or high findings:

1. Copy the latest Tanium Platform Analyzer (TPAN) report to wherever you store Tanium files for diagnostics. See Tanium Health Check User Guide: Download a TPAN report.
2. Open the report and select the **Findings** page to see if **Critical** or **High** findings exist.
3. Troubleshoot any **Critical** or **High** findings. See Tanium Core Platform Deployment Reference Guide: Troubleshoot issues during server deployment or solution operations.
4. Contact Tanium Support on page 10 for help troubleshooting the findings if necessary.

> NOTE
>
> Review all TPAN findings on page 15, including **Medium** and **Low** findings, during monthly maintenance.

Review the Tanium Client deployment

Check how many endpoints are running the Tanium Client (managed endpoints), how many clients function as endpoint leaders in Tanium™ linear chains, and the state of custom or enhanced tags on the clients.

> NOTE
>
> Review and remediate Tanium Client issues on page 19 during monthly maintenance.

Check the endpoint leader percentage

In linear chains of Tanium Clients, minimizing the percentage of endpoints that function as leaders helps to reduce bandwidth usage in communications with Tanium Servers and Tanium™ Zone Servers. The leader percentage varies among networks and no specific percentage is ideal for all networks. However, unexpected changes in the percentage might indicate network issues that your networking team must address. For example, a sharp increase in the percentage might cause excessive wide area network (WAN) traffic. Therefore, monitor changes in the leader percentage over time by recording the percentage at weekly intervals.

> NOTE
>
> For details about leaders, linear chains, and how the servers evaluate subnet boundaries, see Tanium Client Management User Guide: Client peering.

1. Open the latest TPAN report and select the **Tuning** page.
2. Check the value of **What's the actual or anticipated leader count percentage?**

   Typically, this value does not change significantly unless your network changes in ways that affect the number and size of client subnets.

3. If the leader percentage changes more than expected, investigate the possible causes. The percentage might change if:

    - Subnets join or leave your network. Check the endpoint count on page 12 to see if the number of managed endpoints has changed. If the change is due to new subnets, verify that they are authorized to join your network. If the change is due to subnets no longer registering with Tanium Servers or Tanium Zone Servers, verify whether network disruptions or misconfigurations are responsible.
    - A shift occurs between the number of users who are connecting within your internal network and the number who are connecting through virtual private network (VPN) connections. Typically, VPN endpoints do not peer with each other and therefore each one is effectively a leader. See Tanium Client Management User Guide: Configure isolated subnets.

4. Contact Tanium Support on page 10 for help optimizing the leader count, if necessary.

Check the endpoint count

The number of managed endpoints might fluctuate as endpoints join or leave your network. View the number of managed endpoints to check for potential anomalies and to ensure compliance with your Tanium license:

- Go to the Tanium **Home** page to check the **Total Endpoints**. This field displays the most accurate tally of online and offline managed endpoints that have registered with the Tanium Server or Zone Server within the retention period (default is 30 days). For details, see Tanium Console User Guide: View environment status.

  If the endpoint count is lower than expected, investigate whether network disruptions or misconfigurations prevent endpoints from registering. If the count is higher than expected, verify that the new endpoints are authorized to join your network.

  > TIP
  >
  > You can configure an automatic Discover label and a Connect destination to alert you when endpoints become unmanaged. See Tanium Client Management User Guide: Audit and remediate disconnected Tanium Clients.

- Go to **Administration > Configuration > Client Status** to check the endpoint count as it relates to your Tanium license, regardless of whether it matches the **Total Endpoints** value on the Tanium **Home** page. For details, see Tanium Console User Guide: View managed endpoints count for license compliance.

  Track changes in the weekly endpoint count to project future growth. Contact Tanium Support on page 10 to update your license for a higher number of maximum managed endpoints if necessary.

Review and update tags

If you use computer groups for which membership is based on custom tags or enhanced tags, review which endpoints have which tags. Deploy changes to the tags and configure new computer groups if necessary.

REVIEW AND UPDATE ENHANCED TAGS

For the steps to review and update enhanced tags, sign in to the Tanium™ Knowledge Base and see the Enhanced Tags Documentation.

REVIEW AND UPDATE CUSTOM TAGS

1. Determine which endpoints have which tags. See Tanium Console User Guide: Review custom tags.
2. Add or remove custom tags if necessary. See Tanium Console User Guide: Manage custom tags for computer groups.
3. Create or delete computer groups with tag-based membership if necessary. See Tanium Console User Guide: Managing computer groups.

   > NOTE
   >
   > You cannot change the membership definition of existing computer groups. You must delete existing groups and recreate them with the correct definition.

4. Add or edit action groups to target tag-based computer groups if necessary. See Tanium Console User Guide: Managing action groups.

Review and update actions that target No Computers

Actions that target the **Default** action group do not deploy to endpoints because **Default** includes only the **No Computers** computer group. In some cases, **Default** might be targeted to prevent unexpected changes on endpoints. Perform the following steps to review the actions that target **Default**, assess whether your environment is ready for deploying the actions, and assign a different action group if necessary.

> BEST PRACTICE
>
> If you want actions that target **Default** to deploy to endpoints, assign a different action group instead of reconfiguring **Default** to include other computer groups.

> NOTE
>
> For information about actions that target **Default**, see Tanium Console User Guide: Reconfigure actions that target the Default action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.
2. In the **Name** column, click **Default** to view the configuration of that action group.
3. Verify that the assigned **Computer Groups** include only **No Computers**.

   If other computer groups are assigned, deselect them and click **Save**.
4. From the Main menu, go to **Administration > Actions > Scheduled Actions**.
5. In the **Action Group** drop-down, select **Default** to list only the actions that target that action group.
6. If you want to deploy any of the listed actions to endpoints, assign the actions to a different action group. See Tanium Console User Guide: Edit action group assignments for scheduled actions.

> NOTE
>
> Review and update scheduled actions on page 39 during quarterly maintenance.

Review Tanium™ Deploy metrics

Monitor Deploy metrics and update the configurations, if necessary.

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click **IT Operations Metrics** to view the **Maintenance Coverage**, **Endpoints Missing Software Updates Released Over 30 Days**, **Mean Time to Maintenance Software**, and **Software Installed by Self Service User Request** panels in the **Deploy** section.
3. Tanium Deploy User Guide: Monitor and troubleshoot Deploy coverage.
4. Tanium Deploy User Guide: Monitor and troubleshoot endpoints missing software updates released over 30 days.
5. Tanium Deploy User Guide: Monitor and troubleshoot mean time to deploy software.
6. Tanium Deploy User Guide: Monitor and troubleshoot software installed by self service user request.

Performing monthly maintenance

Monthly maintenance includes reviewing health and performance information for the Tanium Core Platform, Tanium Clients, and Tanium solutions.

TIP

For all tasks that provide the option to issue a question in Tanium™ Interact, you can perform additional investigation or remediation on the **Question Results** page by issuing drill-down questions, opening single endpoint views, or deploying actions. See Tanium Console User Guide: Managing question results.

For tasks that involve viewing reports, you can perform additional investigation or remediation in the Tanium™ Reporting workbench. See Tanium Reporting User Guide: Working with reports.

For tasks that involve viewing Tanium™ Trends boards, you can perform additional investigation in the Trends workbench. See Tanium Trends User Guide: Viewing chart results.

Review Tanium security advisories

Review the security advisories that Tanium publishes to identify and remediate vulnerabilities in Tanium solutions. A Tanium™ Community account is required to perform this task.

1. In your browser, go to the Tanium Technical Support home page and click **Tanium Vulnerabilities**.
   For each advisory, the page provides a brief description that indicates the affected solution and provides a link to a page with full details about the associated vulnerability, such as its severity level.

2. Click each link for vulnerabilities that apply to your licensed solutions and review the vulnerability details.

3. Perform one of the following tasks:

   - (Best practice) Import any **Available Updates** that resolve the vulnerabilities. See Tanium Console User Guide: Import or update specific solutions.

   - Apply any **Workarounds and Mitigations** for the vulnerabilities if solution updates are not available or you plan to delay the updates.

Review all TPAN findings

1. Copy the latest Tanium Platform Analyzer (TPAN) report to wherever you store Tanium files for diagnostics. See Tanium Health Check User Guide: Download a TPAN report.

2. Open the report and select the **Findings** page.

3. Review any **Critical**, **High**, **Medium**, or **Low** findings to decide whether they require:

- **Resolution**: Resolve all **Critical** and **High** findings. For example, if the report indicates that the Tanium™ Module Server is not connected, you must resolve the issue immediately because numerous Tanium operations depend on that server. Resolve the **Medium** and **Low** findings only if appropriate. For example, if the **Medium** findings indicate that some actions target the **Default** action group, which includes only the **No Computers** computer group, those actions do not deploy to endpoints. Reconfiguring the actions to target another action group is required only if deploying them to endpoints is appropriate.
- **Investigation**: You might have to see more information about findings before deciding if they require resolution or no action. For example, if the **Low** findings indicate that the Tanium Server is using a self-signed certificate for securing user access to the Tanium™ Console, you might have to consult your network security team before deciding whether to replace that certificate with one that a certificate authority (CA) has signed.
- **No action**: Some findings might be known conditions that you regard as acceptable. For example, if the **Low** findings indicate that isolated subnets are not defined but you already know that your network does not require isolated subnets, no action is required.

4. Troubleshoot the findings. See Tanium Core Platform Deployment Reference Guide: Troubleshoot issues during server deployment or solution operations.
5. Contact Tanium Support on page 10 for help troubleshooting the findings if necessary.

Review Appliance health

Perform the following tasks if your Tanium deployment uses Appliance infrastructure. If these tasks reveal issues that require resolution, see Tanium Appliance Deployment Guide: Troubleshooting.

Review the Health Check report

The Health Check report provides information on the health of the Appliance operating system, hardware, users, network, services, applications, database replication, RAID security, Postgres SSL, and virtual machine (if applicable).

1. Run the report. See Tanium Appliance Deployment Guide: Run the Health Check.
2. Review the output for actionable items, which are summarized at the end of the output.

   For example, the output might indicate that the End User License Agreement (EULA) is not accepted.

Monitor Appliance performance (optional)

See the following tasks in the Tanium Appliance Deployment Guide for the steps to run commands for viewing Appliance performance information:

- Run a sar command to view statistical information such as CPU load, memory paging, memory utilization, swap usage, and network input/output (I/O).
- Run the iotop command to view I/O utilization by process.
- Run the perf-top command to view CPU usage by function.
- Run the htop command to view detailed information about each running process, such as memory and CPU consumption. The output provides an interface whereby you can navigate among values and tabs by keyboard and mouse.

Review and update global bandwidth throttles

Global throttles limit the bandwidth and the number of concurrent connections that the Tanium Server or Zone Server uses to send data to all Tanium Client subnets. Disruptions to server functions might occur if they consume too much bandwidth or do not have enough bandwidth to perform operations at a reasonable speed. Review the global throttles and, if necessary, update them.

> NOTE For details about global throttles, see Tanium Console User Guide: Bandwidth throttling overview.

1. Check the delays for global throttles to evaluate the current risk of disruptions to Tanium functions. See Tanium Console User Guide: Verify throttle delays.
2. Update the global throttles if necessary. See Tanium Console User Guide: Configure global throttles.

> NOTE Review and update site bandwidth throttles on page 38 during quarterly maintenance.

Review and import solution updates

Determine whether updates are available for Tanium solutions (modules, shared services, and content-only solutions), and import the updates if appropriate. The best practice is to import solution updates as soon as they become available. However, in certain cases, you might need to delay updates for some solutions while importing others immediately. For example, your organization might have a policy that mandates testing each update in a lab environment before importing it into a production environment.

To review and import solution updates, see Tanium Console User Guide: Import or update specific solutions.

Review and remediate Tanium™ API Gateway issues

1. Verify that API tokens have not expired. See Tanium Console User Guide: View API token details.
2. Verify whether any API tokens are due for rotation based on the policy of your organization. See Tanium Console User Guide: Rotate an API token.
3. Revoke any API tokens that are no longer needed. See Tanium Console User Guide: Revoke API tokens.
4. Check for deprecated fields and, if necessary, update the integration scripts that use them. See Tanium API Gateway User Guide: Reference: Deprecated fields.
5. To investigate and remediate API Gateway issues, see Tanium API Gateway User Guide: Troubleshooting API Gateway.

Review and remediate Tanium™ Asset issues

Review Tanium source imports

1. From the Main menu, go to **Modules > Asset > Overview**.
2. Scroll to the **Health** dashboard to see load time metrics for source data that Asset imports.
3. To investigate load time issues, click **Load Time** to view the import schedules.
4. For any jobs with failed runs ❗, click Edit ✎, set the **Log Level** to **Trace**, and click **Update**.
5. To troubleshoot source imports, see Tanium Asset User Guide: Troubleshoot asset data exports and imports.

Review the status of import and export jobs

1. From the Main menu, go to **Modules > Asset > Overview** and scroll to the **Activity** dashboard.

   The dashboard shows the status of import and export jobs.
2. Select each of the **Recent & Upcoming Jobs** and check the status of finished jobs for both **Yesterday** and **Today**. If all the jobs have success status ✓, no troubleshooting is necessary.
3. From the Asset menu, go to **Inventory Management > Schedules** to see more information about the last completed run for each job in the **Import Schedules** and **Export Schedules** tabs.
4. For any jobs with failed runs ❗, click Edit ✎, set the **Log Level** to **Trace**, and click **Update**.
5. To troubleshoot failed jobs, see Tanium Asset User Guide: Troubleshoot asset data exports and imports.

Review reports

1. From the Asset menu, go to **Reports** and check the **Status** of the reports.

   If all the reports are enabled ✓, no troubleshooting is necessary.
2. For any custom reports that have disabled or missing attributes (columns) ⚠, click Edit ✎, correct the report configuration as necessary, and click **Submit**.

> TIP
>
> If you see a report timeout error message when viewing a report, see Tanium Asset User Guide: Troubleshoot reports.

Review views

1. From the Asset menu, go to **Views** and check the **Status** of the views.

   If all the views are enabled ✓, no troubleshooting is necessary.
2. For any custom views that have disabled or missing attributes (columns) ⚠, click Edit ✎, correct the view configuration as necessary, and click **Submit**.

Review and remediate Tanium™ Benchmark issues

1. From the Main menu, go to **Modules > Benchmark > Risk > Risk Health**.
2. Review the **Risk Coverage** and **Risk Vector Calculation Issues** panels.
3. If the panels indicate endpoints need attention, see Tanium Benchmark User Guide: Monitor and troubleshoot Risk health.

Review and remediate Tanium™ Certificate Manager issues

1. From the Main menu, go to **Modules > Certificate Manager > Overview**.
2. In the Overview section, review the **Certificate Manager Coverage** panel for endpoints with the **Needs Attention** status.
3. To investigate issues, see Tanium Certificate Manager User Guide: Monitor and troubleshoot Certificate Manager Coverage.
4. To troubleshoot other Certificate Manager issues, see Tanium Certificate Manager User Guide: Troubleshooting Certificate Manager.

Review and remediate Tanium Client issues

Perform the following tasks to review the state of the Tanium Clients running on endpoints, as well as client communication and registration with Tanium Servers and Zone Servers. If you observe client issues that require resolution, see Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

Review and remediate Tanium Client health and client extension issues

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Deployment** tab to review the **Health Failures** panel. This panel shows failures associated with Tanium™ Client Extensions. Perform the remaining steps if you need to troubleshoot client extension issues.
3. Click Interact in the **Health Failures** panel to display the question results that provide the panel data.
4. Retrieve any additional details from endpoints that you need to diagnose client extension issues. See Tanium Console User Guide: Managing question results.
5. To resolve client extension failures, see the following sections:
    - To resolve Client Index Extension failures, see Tanium Client Index Extension User Guide: Reference: Common health check issues.
    - To resolve Client Recorder Extension failures, see Tanium Client Recorder Extension User Guide: Troubleshooting the Client Recorder Extension.
    - To resolve failures associated with client extensions for other Tanium solutions, see Tanium Console User Guide: Troubleshoot solution-specific issues and Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Review and adjust the distribution of Tanium Client registration traffic

Tanium Clients must register with a Tanium Server or Zone Server for the client hosts to function as managed endpoints. As clients and client subnets are added to or removed from your network, you might have to update client-server connections to optimize registration traffic.

Each Tanium Client connects to only one Tanium Server or Zone Server at a time. However, to avoid a single point of failure, you can configure the **ServerNameList** setting with a list of servers to which the client can attempt a connection.

> NOTE
>
> For details about client-server connections, see Tanium Client Management User Guide: Configuring connections to the Tanium Core Platform.

To determine which servers are processing client registrations and, if necessary, to rebalance registration traffic among them:

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Settings** tab.
3. Scroll to the **ServerNameList** setting to determine whether clients are connecting to the correct servers.
4. Review the **ServerName** setting to verify that client connections are balanced among Zone Servers.
5. Deploy actions with packages that reset the **ServerNameList** settings if necessary to connect clients to different servers. See Tanium Client Management User Guide: Content for configuring connections to Tanium Cloud.
6. Add Zone Servers if necessary to rebalance client registration traffic and then repeat step 5 to connect clients to those servers. See the procedure for your Tanium infrastructure:
   - Tanium Appliance Deployment Guide: Installing an Appliance Array: See the tasks for adding array members and assigning roles.
   - Tanium Core Platform Deployment Guide for Windows: Installing the Tanium Zone Server

Review and update Tanium Client logging levels

Tanium Clients generate logs that can help you troubleshoot issues. Higher logging levels record more details about events on clients but also consume more client resources. The default logging level is `1`. Review client logging levels and adjust them if necessary to ensure new endpoints that join your network have optimal logging levels.

> BEST PRACTICE
>
> Set the logging level to `0` (logging disabled) for clients that run on sensitive endpoints, endpoints with limited resources, or virtual desktop infrastructure (VDI) endpoints.

> NOTE
>
> For details about logging levels, see Tanium Core Platform Deployment Reference Guide: Logging levels.
>
> For Tanium™ Client Containers, the default logging level is `10` and you cannot change it through actions. Contact Tanium Support on page 10 to change the logging level on Client Containers.
>
> For details about logs on Tanium Clients, see Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

1. From the **Client Management** menu, go to **Client Health** and click the **Settings** tab.

   If the logging level is set to a value other than the default `1` on any clients, the **LogVerbosityLevel** setting displays the **Count** of clients for each value. If all clients have the default value, the page does not display the setting.

   > TIP
   >
   > To verify that the logging level is set to the best practice value `0` for clients on VDI endpoints, select **All Virtual Machines** in the **Computer Group** drop-down.

2. To update the logging level on clients, see Tanium Client Management User Guide: Managing client settings and configurations in Client Management.

Review and update Tanium Client settings

1. From the **Client Management** menu, go to **Client Health** and click the **Settings** tab.
2. Verify that the setting values are correct and that the **Count** column indicates they apply to the expected number of clients.
3. To update settings, see Tanium Client Management User Guide: Managing client settings and configurations in Client Management.

Review and upgrade Tanium Client versions

The best practice is to run the latest Tanium Client version on all endpoints. However, in certain cases, temporarily running earlier client versions might be acceptable for some endpoints. For example, if you are rolling out client upgrades in phases, one group of endpoints at a time, you might want to finish testing the upgrade for the first phase before upgrading more endpoints in the next phase. Endpoints might also run an earlier client version if the upgrade process failed.

> NOTE
>
> For details about client versions, see Tanium Client Management User Guide: Client version and host system requirements.

Determine which endpoints are running a client that is not at the latest version and decide whether to accept the earlier versions or upgrade the clients:

1. From the Main menu, go to **Administration > Client Management**.
2. Scroll to the **Health** dashboard to see the **Client Version** panel.
3. If any endpoints are running an earlier client version, click the **Client Version** title and then click Interact in the **Client Version** panel to display the question results that provide the panel data.
4. Retrieve any details from endpoints that you need to determine whether the versions are appropriate, or upgrades are required, or upgrades failed.

   For example, select a **Filter by Computer Group** option (such as **All Windows**) or issue a drill-down question. For the steps to retrieve additional details, see Tanium Console User Guide: Managing question results.

5. Upgrade the client on any endpoints that require the latest version. See Tanium Client Management User Guide: Upgrading

Tanium Clients.

6. Troubleshoot client upgrade issues if necessary. See Tanium Client Management User Guide: Troubleshooting Tanium Clients and Client Management.

Review and update Tanium Client subnets

Separated subnets, intentional subnets, and isolated subnets provide methods for modifying the default peering behavior of Tanium Clients. Default peering settings define the boundaries of client subnets in the Tanium linear chain architecture. As subnets are added to or removed from your network, you might have to update the client subnet configurations. For example, add isolated subnets for any new virtual private networks (VPNs).

NOTE

For details about client peering and subnets, see Tanium Client Management User Guide: Configuring Tanium Client peering.

REVIEW AND UPDATE ISOLATED SUBNETS

Configure isolated subnets for Tanium Clients that are in VPNs. VPN clients have local IP addresses in a special VPN address block, but their host endpoints are actually not close to each other. If VPN clients are not isolated, they use WAN links for peering and latency is significantly greater than for client-to-server connections.

1. Go to **Administration > Configuration > Subnets** and review the **Isolated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update isolated subnet configurations if necessary. See Tanium Client Management User Guide: Configure isolated subnets.

REVIEW AND UPDATE SEPARATED SUBNETS

Configure separated subnet configurations to apply more granular subnet boundaries for Tanium linear chains than the default boundaries.

1. Go to **Administration > Configuration > Subnets** and review the **Separated Subnets**. If necessary, consult your networking team to determine if the configurations require updates.
2. Update separated subnet configurations if necessary. See Tanium Client Management User Guide: Configure separated subnets.

REVIEW AND UPDATE INTENTIONAL SUBNETS

In a network configuration that uses network address translation (NAT), you might have to configure intentional subnets to ensure that clients in the same subnet can peer with each other.

1. From the Main menu, go to **Administration > Configuration > Client Status**.

   The **Network Location (from client)** values indicate which clients are in the same subnet based on the **AddressMask** setting. See Tanium Client Management User Guide: AddressMask.

   The **Network Location (from server)** column indicates the NAT IP addresses of clients.
2. Select the endpoints that are in the same subnet but are not peering because their NAT IP addresses differ.
3. Click Export, set the **Format** to **List of Clients - CSV**, and click **Export**.

4. Go to **Administration > Configuration > Subnets** and compare the **Intentional Subnets** configurations to the exported list of clients.

5. Update the intentional subnet configurations if necessary to enable peering among clients in the same subnets. See Tanium Client Management User Guide: Configure intentional subnets.

Review and remediate Tanium™ Comply issues

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

2. Scroll to the **Health** dashboard to review any Comply health check errors on endpoints.

   The **Comply Health Checks** panel shows a bar for each type of error, such as outdated tools, scan failures, or insufficient disk space. The number above each bar indicates how many endpoints are affected.

3. To investigate a health check error, click the number above the error bar. The Tanium Server issues a question that returns the computer name, operating system, IP address, coverage status, and client extensions status for the affected endpoints.

4. To troubleshoot health check errors, see Tanium Comply User Guide: Reference: Common errors.

> NOTE
>
> Review and update Comply assessments and configurations during quarterly maintenance.

Review and remediate Tanium Connect issues

Review and remediate connection issues

1. Check for connection failures:

   - If you configured a failed connections report with automatic delivery, access the report at the specified destination. See Configure a failed connections report.

     > NOTE
     >
     > If you do not have the authority to delete or disable connections that are no longer required, also configure delivery of the report to a team in your organization that has the authority.

   - To manually review connection failures, see Tanium Connect User Guide: View connection status.

     > TIP
     >
     > If the list of connections is long, click the **Failed** toggle to show only failed connections.

2. Review connection throughput metrics to check for issues. See Tanium Connect User Guide: View connection metrics.

3. Troubleshoot connection issues if necessary. See Tanium Connect User Guide: Troubleshooting.

4. Edit connections if necessary to resolve failures. See Tanium Connect User Guide: Edit connections.

5. Delete or disable connections that are no longer required if you have the authority to perform those actions:

   a. From the Main menu, go to **Modules > Connect > Connections**.

   b. Select the connections that require an action and select **Actions > Disable** or **Actions > Delete**.

Review and remediate connection schedules

1. From the Connect menu, go to **Connections**.

   Perform the remaining steps for each connection.

2. Click the connection **Name** to show all its details.

3. Verify that the **Schedule** and **Next Run** show the expected values.

4. If you must change the schedule, click **Edit**, update the **Schedule** settings, and click **Save** or **Save and Run**.

Review and update connection owners

1. From the Connect menu, go to **Connections**.

   Perform the remaining steps for each connection.

2. Click the connection **Name** to show all its details.

3. Verify that the connection **Owner** (user account) and persona (**Run as Persona**) are still valid.

   > NOTE
   >
   > When you delete a user or persona, connections that the user or persona owns stops running. If this occurs, perform one of the following tasks:
   >
   > - Transfer ownership of the connection to an existing user. See Tanium Console User Guide: Delete or transfer content for a non-active user.
   > - Export and import the scheduled connection to create a new scheduled connection. See the following tasks in the Tanium Connect User Guide: Export connections and Import connections.

   a. Verify that the user account is active. See Tanium Console User Guide: View user settings.

   b. If an alternative persona runs the connection, verify that the persona still exists. See Tanium Console User Guide: View persona details.

   c. Verify that the owner has the role permissions that are required to run the connection:

      - If the default persona runs the connection, verify the user permissions. See Tanium Console User Guide: View effective role permissions for a user.
      - If an alternative persona runs the connection, verify the persona permissions. See Tanium Console User Guide: View effective role permissions for a persona.

4. Verify that the user password is compliant with the password rotation policy of your organization.

Review and remediate destination issues

1. From the Connect menu, go to **Connections**.

   Perform the remaining steps for each connection.
2. Click the connection **Name** to show all its details.
3. Verify that the **Destination** settings are correct.
4. If you must change the settings, click **Edit**, update the settings, and click **Save** or **Save and Run**.
5. Verify that the destination (such as a server) is available and running without issues.
6. Verify that the destination certificates are still valid.

Review and remediate Tanium™ Criticality issues

To monitor and troubleshoot Criticality health issues, see Tanium Criticality User Guide: Troubleshooting Criticality.

Review and remediate Tanium Deploy issues

Review and remediate Deploy coverage

1. From the Main menu, go to **Modules > Deploy > Overview**.
2. Scroll to the **Health** dashboard to verify that the Deploy process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **False** in the **Running Deploy** panel. The Tanium Server opens the **Deploy - Endpoint Deployment Process Running** report for the affected endpoints.
4. To investigate Deploy coverage issues, scroll up to the **Summary** dashboard and click the number above **Needs Attention** in the **Deploy Coverage** panel. The Tanium Server opens the **Deploy - Coverage Status Details** report for the affected endpoints.
5. To troubleshoot issues related to the Deploy process or coverage, see .Tanium Deploy User Guide: Troubleshoot Deploy Process Not Running.

Remove unused Deploy software packages

1. Go to **Modules > Deploy > Software**.
2. Review the **Software Packages** and delete unused packages.

   For example, delete software packages that are not the latest version or software that you are no longer using. For more information, see .Tanium Deploy User Guide: Managing software.

Stop unneeded ongoing deployments

1. Go to **Modules > Deploy > Deployments > Active**.
2. Review the deployments and stop any deployments that are no longer needed.

Review and remediate Tanium™ Direct Connect issues

To troubleshoot connection or screen sharing issues for Direct Connect, see Tanium Direct Connect User Guide: Troubleshooting Direct Connect.

Review and remediate Tanium™ Directory Query issues

1. From the Main menu, go to **Administration > Shared Services > Directory Query**.
2. Review the **Domains** grid for errors. Hover over an Error icon ❗ to display a popup with the error message.
3. To troubleshoot errors, see Tanium Directory Query User Guide: Troubleshooting satellite configuration.

Review and remediate Tanium Discover issues

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Discover - Module Health** board and review the panels for resource usage issues.
3. To troubleshoot resource usage issues, see Tanium Discover User Guide: Troubleshooting Discover.

Review and remediate Tanium™ Endpoint Configuration issues

Review and remediate tools deployment

1. From the Main menu, go to **Administration > Shared Services > Endpoint Configuration**.
2. Review the deployment status of tools:
   - From the Endpoint Configuration menu, select **Tools**. See Tanium Endpoint Configuration User Guide: View deployed endpoint tools.
   - From the Endpoint Configuration menu, select **Content-Only Solutions**. See Tanium Endpoint Configuration User Guide: View the status of content-only solutions.
3. To troubleshoot deployment issues for tools, see Tanium Endpoint Configuration User Guide: Identify and resolve issues with endpoint tools or client extensions.

Verify whether endpoints have the latest manifest

Verify that endpoints have the latest Endpoint Configuration *manifest*, which is a file that determines the versions of solution tools to install on endpoints. If endpoints do not have the latest manifest because of action locks or some other issue, the endpoints do not install the latest tools versions.

1. From the Endpoint Configuration menu, go to the **Overview** page, and note the **Manifest Revision** (version) in the **Summary** section..
2. Go to the Tanium **Home** page and ask the following question: `Get Endpoint Configuration - Manifest Metadata?maxAge=60 and Action Lock Status from all machines`

   BEST PRACTICE The manifest changes whenever a configuration or tool change occurs. Therefore, use the `maxage=60` option for the **Manifest Metadata** sensor to ensure that you retrieve the latest data from endpoints.

   TIP Sort the **Question Results** grid by **Revision** to list the versions in descending numerical order, which makes it easier to identify endpoints with an earlier manifest version.

3. If the **Question Results** indicate **Action Lock Status** is on for some endpoints that do not have the latest manifest:
   a. Consult whoever turned on the action locks to verify that it is now safe to run actions on those endpoints.
   b. Perform one of the following tasks:
      - Disable action locks on the endpoints that require an updated manifest. See Tanium Console User Guide: Turn off action locks.
      - Configure Endpoint Configuration to ignore action locks for all endpoints. See Tanium Endpoint Configuration User Guide: Global Endpoint Configuration settings.
4. Update the manifest on page 27 on any endpoints that require an updated version.

Update the manifest

Windows and non-Windows endpoints require separate packages to update the manifest. Therefore, perform the following steps for each type of endpoint:

1. Go to the Tanium **Home** page and ask the following question: `Get Endpoint Configuration - Manifest Metadata?maxAge=60 from all machines`
2. Select the endpoints that have an outdated manifest and click **Deploy Action**.
3. Select the **Deployment Package** that matches the target endpoints:
   - Windows endpoints: **Endpoint Configuration - Manifest [Windows] (v. <*latest_manifest_version*>)**
   - Non-windows endpoints: **Endpoint Configuration - Manifest [Non-Windows] (v. <*latest_manifest_version*>)**
4. Configure the remaining action settings and deploy the action. See Tanium Console User Guide: Deploying actions.

If the manifest update fails, investigate environmental factors, such as security exclusions, file locks, CPU usage, RAM usage, and disk failures. Contact Tanium Support on page 10 for additional help.

Review and remediate Tanium™ End-User Notifications coverage

1. From the Main menu, go to **Administration > Shared Services > End-User Notifications**.
2. Scroll to the **Health** dashboard to verify whether the latest End-User Notifications tools are installed and active on all endpoints.
3. To investigate endpoints that do not have the latest tools installed, click the number above **No** or **Unsupported**. The Tanium Server issues a question that returns the computer name, operating system, IP address, tools installation status, and installed tools version.
4. To troubleshoot installation issues for End-User Notifications tools, see Tanium End-User Notifications User Guide: Problem: End user notifications are not displayed..

Review and remediate Tanium™ Enforce coverage

1. From the Main menu, go to **Modules > Enforce > Overview**.
2. Scroll to the **Health** dashboard to verify whether Enforce tools are installed and active on all endpoints.
3. To investigate endpoints that do not have Enforce tools installed, click the number above **Not Installed**. The Tanium Server issues the following question: `Get?forceComputerIdFlag=1 Endpoint Configuration - Tools Status?ignoreCase=0&maxAge=600 contains Enforce from all machines`
4. To troubleshoot installation issues for Enforce tools, see Tanium Enforce User Guide: Monitor and troubleshoot Enforce coverage status (% of total).

Review and remediate Tanium™ Engage issues

To monitor and troubleshoot Engage issues, see Tanium Engage User Guide: Troubleshooting Engage.

Review and remediate Tanium™ Feed issues

To monitor and troubleshoot Feed health issues, see Tanium Feed User Guide: Troubleshooting Feed.

Review and remediate Tanium Health Check issues

To monitor and troubleshoot Health Check issues, see Tanium Health Check User Guide: Troubleshooting Health Check.

Review and remediate Tanium™ Impact coverage

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Impact** board and review the **Impact Coverage Status** panel for endpoints with the following status:
   - **Needs Attention**: Python tools that are required for Impact sensors are not installed.
   - **Unsupported**: Impact does not support the operating system.
3. To investigate endpoints that need attention, click the **Needs Attention** bar in the chart and select **View Current Endpoint Details filtered by Needs Attention**. The Tanium Server issues the following question: `Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Needs Attention from all machines with Impact - Coverage Status equals Needs Attention`
4. To investigate endpoints that do not support Impact, click the **Unsupported** bar in the chart and select **View Current Endpoint Details filtered by Unsupported**. The Tanium Server issues the following question: `Get Computer Name and Operating System and IP Address and Impact - Coverage Status equals Unsupported from all machines with Impact - Coverage Status equals Unsupported`
5. To troubleshoot Impact coverage, see Tanium Impact User Guide: Monitor and troubleshoot Impact Coverage.

Review and remediate Tanium™ Integrity Monitor issues

1. From the Main menu, go to **Modules > Integrity Monitor > Overview**.
2. Scroll to the **Health** dashboard to review any health check errors.
3. To investigate issues with client extensions that appear in the panel, click **Health Check**. For specific troubleshooting steps, see Integrity Monitor User Guide: Identify and resolve issues with client extensions.
4. To see detailed health information about endpoints that are included in an error category, click the bar for that category in the chart. For specific troubleshooting steps, see Integrity Monitor User Guide: Reference: Endpoint monitoring health check errors.

Review and remediate Tanium Interact issues

To troubleshoot Interact issues, see Tanium Interact User Guide: Troubleshooting Interact.

Review and remediate Tanium™ Patch issues

Review Patch coverage, scan configurations, deployments, and maintenance windows. Update the configurations if necessary.

> NOTE
>
> Review and update custom action groups for Patch during quarterly maintenance.
>
> Review and update Patch block lists on an as-needed basis.

Review and remediate Patch coverage

1. From the Main menu, go to **Modules > Patch > Overview**.
2. Scroll to the **Health** dashboard to verify that the Patch process is running on all endpoints.
3. To investigate endpoints that are not running the process, click the number above **No** or **Error** in the **Running Patch** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch process status for the affected endpoints.
4. To investigate Patch coverage issues, click the number above **Needs Attention** in the **Patch Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Patch coverage status details for the affected endpoints.

   TIP You can also see this information in the predefined **Patch Coverage Status** report, which is available in the Tanium Reporting workbench.

5. To troubleshoot issues related to the Patch process or coverage, see Tanium Patch User Guide: Monitor and troubleshoot Patch coverage.

Review and update scan configurations

1. From the Patch menu, go to **Scan Management**.
2. Review the **Scan Configurations** for each operating system (OS) to verify that they conform to the practices of your organization.
3. Select the **Tanium Scan for Windows** tab and click **Edit**.
4. Review the **Products to Include in Scan**, add any products that you want to include, and click **Submit**.
5. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.
6. Review the **Days Since Last Patch Scan** and **Scan Errors - Last 7 Days** panels for any errors. Click a panel name to see more details.
7. Troubleshoot scan errors if necessary. See Tanium Patch User Guide: Troubleshooting Patch.
8. Edit scan configurations if necessary to resolve errors. See Tanium Patch User Guide: Edit a scan configuration.
9. Delete scan configurations if any are no longer useful. See Tanium Patch User Guide: Delete a scan configuration.

Review and update deployments

1. From the Patch menu, go to **Deployments**.
2. Review the deployments to determine if any are misconfigured, no longer useful, or do not comply with the practices of your organization.

   For example, if the number of targeted endpoints is low relative to the number of deployments, you might be able to make the patching process more efficient by configuring fewer deployments to target more endpoints.

3. Check the deployment summaries for error messages. See Tanium Patch User Guide: Review deployment summary.

4. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.

5. Review the panels in the **Summary**, **Missing Patches**, and **SLA Based Compliance Reporting** sections for any errors. Click a panel name to see more details.

6. Troubleshoot deployments if necessary. See Tanium Patch User Guide: Troubleshooting.

7. Add targets to the deployments if necessary to resolve errors. See Tanium Patch User Guide: Add targets to an existing deployment.

   NOTE

   For an existing deployment, you cannot perform edits other than adding targets.

8. Stop any deployments that are no longer useful. See Tanium Patch User Guide: Stop a deployment.

Review and update maintenance windows

1. From the Patch menu, go to **Deployments**.

2. Review the maintenance windows to determine if any are misconfigured or no longer useful.

   For example, maintenance windows that have end dates in the past are useful only as blocking maintenance windows. See Tanium Patch User Guide: Setting maintenance windows.

   IMPORTANT

   Deployments can run anytime if no maintenance windows are configured. If you imported Patch with default settings, it provides predefined maintenance windows that are not enforced on any computer groups. See Tanium Patch User Guide: Configuring Patch.

3. From the Main menu, go to **Modules > Trends > Boards** and click the **Patch** board.

4. If the **Endpoints Missing Critical or Important Patches Released Over 30 Days Ago** panel shows a higher than expected number, check whether maintenance windows are a contributing factor. See Tanium Patch User Guide: Monitor and troubleshoot mean time to patch.

5. Edit maintenance windows if necessary to resolve issues. See Tanium Patch User Guide: Edit a maintenance window.

6. Remove any maintenance windows that are no longer useful. See Tanium Patch User Guide: Delete a maintenance window.

Review and remediate Tanium™ Performance coverage

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

2. Scroll to the **Health** dashboard to verify that Performance tools are installed on all endpoints and to review which profiles are applied to endpoints.

3. To investigate endpoints that do not have Performance tools installed, click the number above **Needs Attention** or **Unsupported** in the **Performance Coverage** panel. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Performance coverage status for the affected endpoints.

> TIP
>
> You can also issue the question `Get Performance - Configured from all machines` through the **Ask a Question** field in Interact and then drill down on results to investigate endpoints that have issues with Performance tools or configuration. See Managing question results.

4. To review the status, priority, and endpoint targeting of all profiles, click **Active Profiles**: see Tanium Performance User Guide: Managing profiles.
5. To review the entire configuration of a specific profile, click its name in the **Active Profiles** panel.
6. To troubleshoot installation issues related to Performance tools or profiles, see Tanium Performance User Guide: Monitor and troubleshoot Performance coverage.

Review and remediate Tanium™ Provision coverage

1. From the Main menu, go to **Modules > Provision > Overview**.
2. Scroll to the **Health** dashboard to verify that the Provision service is running as expected ✓ on Provision endpoints.
3. If the **Health** dashboard indicates that the Provision service is not running on Provision endpoints:
   a. Click **Provision Endpoints** to see details about the service status and versions for all Provision endpoints.
   b. To see additional details about a particular endpoint, click Additional Data ◂ beside that endpoint.
4. To investigate deployment issues, see Tanium Provision User Guide: Monitor a deployment.
5. To troubleshoot other Provision issues, see Tanium Provision User Guide: Troubleshooting Provision.

Review and remediate Tanium™ Reporting issues

To monitor and troubleshoot Reporting health issues, see Tanium Reporting User Guide: Troubleshooting Reporting.

Review and remediate Tanium™ Reputation issues

1. From the Main menu, go to **Modules > Trends > Boards**.
2. Click the **Reputation** board and review the panels for issues that need attention.
3. If the **Failed Outbound API Requests** panel displays failures, verify that the reputation sources are configured correctly. See Tanium Reputation User Guide: Configuring reputation sources.
4. If data shows up faster in the **Inbound Items** panel than in the **Outbound Items** panel and the **Outbound Processing Queue** panel is consistently high, configure the reputation sources to send fewer hashes by lowering the **Maximum Hashes Processed Per Day** value.
5. To troubleshoot other Reputation issues or collect logs for a support package, see Tanium Reputation User Guide: Troubleshooting Reputation.

Review and remediate Tanium™ Reveal issues

1. From the Main menu, go to **Modules > Reveal > Overview**.
2. Scroll to the **Health** dashboard to review:
   - **Reveal Coverage**: To investigate endpoints that do not have Reveal tools installed, click the number above **Needs Attention**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal coverage (installation) status for the affected endpoints. See Tanium Reveal User Guide: Monitor and troubleshoot Reveal coverage.
   - **Endpoint Status**: To investigate endpoints that have issues related to Reveal operations, click **Attention Needed**. The Tanium Server issues a question that returns the computer name, operating system, IP address, and Reveal tools status for the affected endpoints. See Tanium Reveal User Guide: Remediating "Needs Attention" messages from Reveal Status.

Review and remediate Tanium™ Threat Response issues

1. From the Main menu, go to **Administration > Shared Services > Client Management**.
2. From the Client Management menu, select **Client Health** and click the **Deployment** tab.
3. Review the **Health Failures** panel for issues that relate to Threat Response domains:
   - `dec` (Direct Connect)
   - `index` (Tanium Index)
   - `recorder` (Tanium Recorder)
   - `stream` (Tanium™ Stream)
   - `threatresponse` (Tanium™ Threat Response Client Extension)
4. Investigate health failures and review the status and configurations of endpoint tools for Threat Response, including:
   - Non-default configuration settings on clients
   - Tools versions
   - Client extension versions
   - (Windows only) Tanium™ Driver status and version
   - Berkeley Packet Filter (BPF) support

   For the specific steps, see Tanium Threat Response User Guide: Get Threat Response endpoint tools status and configurations.
5. From the Main menu, go to **Modules > Threat Response > Overview**.
6. Scroll to the **Metrics** panel and check the Threat Response **Coverage**.

7. If the **Coverage** is lower than expected, investigate and remediate coverage as described under Tanium Threat Response User Guide: Monitor and troubleshoot Threat Response coverage. If coverage issues might result from missing or misconfigured Threat Response profiles, click the **Coverage** value to open the **Profiles** page and review profile configurations. For details about profile issues, see Tanium Threat Response User Guide: My device has no profile or the wrong profile.

8. To investigate and remediate other Threat Response issues, see the following sections in the Tanium Threat Response User Guide:

   - Troubleshooting
   - Reference: Common health check issues

Review and remediate Tanium™ Trends issues

To troubleshoot Trends issues, see Tanium Trends User Guide: Troubleshooting Trends.

Performing quarterly maintenance

Review and update backups and the disaster recovery plan

1. Verify that a backup of your Tanium deployment is stored in a safe location. Create the backup if it does not exist:
   - Tanium Appliance Deployment Guide: Reference: TanOS backup and recovery
   - Tanium Core Platform Deployment Guide for Windows: Back up the servers and database
2. Review the disaster recovery plan for all your Tanium Core Platform servers. Update the plan if necessary to accommodate changes to the deployment:
   - Tanium Appliance Deployment Guide: Reference: Define a disaster recovery plan
   - Tanium Core Platform Deployment Guide for Windows: Back up Tanium Core Platform servers and databases
3. Generate support bundles for all the Tanium solutions in your Tanium license every 90 days and store each set of bundles for 180 days. For the steps to generate a support bundle for a solution, see the corresponding user guide:
   - API Gateway
   - Asset
   - Client Management
   - Comply
   - Connect
   - Criticality
   - Deploy
   - Direct Connect
   - Discover
   - Endpoint Configuration
   - End-User Notifications
   - Enforce
   - Health Check
   - Impact
   - Integrity Monitor
   - Interact
   - Map

- Network Quarantine
- Patch
- Performance
- Provision
- Reporting
- Reputation
- Reveal
- Risk
- Threat Response
- Trends

> NOTE
> Test disaster recovery on page 43 during annual maintenance.

Verify the grub key backup (physical or virtual Appliance only)

You can use the grub key during the boot sequence to diagnose and recover from failure conditions. During recovery, you must provide the key to Tanium Support for a technician to extract the grub password.

1. Verify that a backup of the latest key resides in a safe location off the Appliance.

   > NOTE
   > A new backup is required whenever the key password is regenerated. See Tanium Appliance Deployment Guide: Change the grub key password.

2. Export the key and save it in a safe location if no backup exists or if the current backup is not the latest. See Tanium Appliance Deployment Guide: Export the grub key.

Review and update Console user accounts

Review user settings, and update them if necessary, to ensure that account configurations reflect personnel changes as users leave, join, or change roles in your organization:

1. From the Main menu, go to **Administration > Permissions > Users**.
2. Review the following settings:
   - **Name**: If the **Users** grid is missing accounts, the steps to add them depend on the type of identity store:
     - **Remote**: Work with your identity store administrator to verify that the accounts exist on the Lightweight Directory Access Protocol (LDAP) or Active Directory (AD) server and add the accounts if necessary. If the accounts already exist, verify that the LDAP/AD server connection and synchronization settings are correct. See

    Tanium Console User Guide: Configure an LDAP server.

    - **Local** (Tanium Server): See Tanium Console User Guide: Create a user.

  If the **Users** grid lists accounts for users who are no longer active, see Tanium Console User Guide: Delete, un-delete, or lock out a user.

- **Locked Out**: If the **Users** grid indicates that certain accounts are locked out, see Tanium Console User Guide: Locked-out users.
- **Last Sign In**: If the **Users** grid indicates that certain users have not signed in for a long time, verify that their accounts are still required. For example, a user administrator might have created accounts only for temporary testing, or users might have left your organization. If any accounts are no longer required, see Tanium Console User Guide: Delete, un-delete, or lock out a user.
- **RBAC assignments and authentication**: Verify that the appropriate computer groups, user groups, personas, and roles are assigned to user accounts and that they use the appropriate authentication services. See Review and update RBAC permissions and authentication settings on page 37.

NOTE For details about user accounts, see Tanium Console User Guide: Managing users.

Review and update RBAC permissions and authentication settings

RBAC permissions control what individual Tanium Console and Tanium™ API users can see and do with the Tanium Core Platform, and which endpoints they can monitor and manage. The permissions derive from personas, roles, user groups, and computer groups that are assigned to user accounts. To ensure that users can access all the Tanium features they need but without access to sensitive information they do not need, review and, if necessary, update their permissions. Also review how users are configured to authenticate for Tanium Console and API access.

NOTE If it is not feasible to review the RBAC permissions of every user on a quarterly basis, review a sample that is representative of the different types of users in your environment.

1. For each user, open the **Preview User** page and review the assigned permissions. See Tanium Console User Guide: View effective role permissions for a user.

   The page lists all the permissions that are directly assigned to the user account through roles or that are inherited from user groups. The page also lists the personas and computer groups that are assigned to the account.

2. Create, edit, reassign, or delete RBAC configurations if necessary to update user permissions. For the steps, see the following sections in the Tanium Console User Guide:

   - Managing roles
   - Managing user groups
   - Managing personas
   - Managing computer groups

3. Verify whether any users can access the Tanium Console through local authentication if your organization allows that. For details and related tasks, see the following sections in the Tanium Console User Guide:

    - User authentication
    - Disable or enable local user access

    BEST PRACTICE If you use an external service for authentication, maintain at least one user account that relies on local authentication and assign the **Administrator** reserved role to that account.

Review and update TanOS user accounts (Appliance only)

1. On each appliance, review the TanOS system users to ensure that they can access the Appliance operating system and that they have the appropriate authentication settings. For example, users who authenticate through passwords must comply with the password policy of your organization. See Tanium Appliance Deployment Guide: Modify the local authentication service security policy.

    The predefined roles for TanOS system users include:

    - `tanadmin`: Users with this role can access all TanOS console menus. It is useful to have more than one `tanadmin` user in case you forget the password for the initial `tanadmin` user that is created during Appliance setup.
    - `tancopy`: Users with this role can copy files to and from the `/incoming` and `/outgoing` directories on the Appliance.
    - `tanuser`: Users with this role can access only status menus in the TanOS console.

    For details and procedures, see Tanium Appliance Deployment Guide: Reference: User Administration menu.

2. Verify that the predefined `tanremote` user account is present if you configured an Integrated Dell Remote Access Controller (iDRAC) interface on the physical Appliance. The account provides remote access to the iDRAC virtual console. This is useful for diagnosing hardware and network interface issues if the TanOS system becomes unavailable. For details and procedures, see Tanium Appliance Deployment Guide: Manage the iDRAC interface.

Review and update site bandwidth throttles

Site bandwidth throttles are subnet-specific throttles that are more restrictive than the global throttles that apply to the rest of your network. Review the site throttles and, if necessary, update them. Disruptions to Tanium Core Platform functions might occur if they consume too much bandwidth or do not have enough bandwidth to perform operations at a reasonable speed.

NOTE For details about site throttles, see Tanium Console User Guide: Site throttles.

1. Check the delays for site throttles to evaluate the current risk of disruptions to Tanium functions. See Tanium Console User Guide: Verify throttle delays.
2. Update the site throttles if necessary. See Tanium Console User Guide: Configure site throttles.

Delete unnecessary computer groups

Users might create computer management groups and filter groups for time-limited activities that are no longer relevant. For example, a user might create a group for initial testing of a new feature after a Tanium solution update and then never use the group after testing finishes. In a Tanium deployment with numerous obsolete computer groups, users might struggle to identify the groups that are still relevant for ongoing activities, such as filtering questions and deploying actions.

> NOTE
>
> For details about computer groups, see Tanium Console User Guide: Computer groups overview.

Review the existing computer groups and delete any that are no longer useful or that have memberships that duplicate other groups:

1. Review computer groups. See Tanium Console User Guide: View computer group details.
2. Delete computer groups. See Tanium Console User Guide: Delete computer groups.

Review and update scheduled actions

You can reduce resource use on the Tanium Server and Tanium Clients by deleting actions that are no longer useful or that duplicate other actions.

> CAUTION
>
> Do not delete actions unless you understand the full impact.

> NOTE
>
> For details about scheduled actions, see Tanium Console User Guide: Managing scheduled actions and action history.

1. From the Main menu, go to **Administration > Actions > Scheduled Actions**.
2. Expand the ▶ **Filters** section and configure a filter based on an attribute that helps you determine whether actions are still useful. The following filters are examples:

Attribute	Operator	Value	Explanation
Status	is equal to	Disabled	Assess whether actions that are currently disabled might be enabled for future use. If a user disabled an action because it will never be useful, delete it.

Attribute	Operator	Value	Explanation
Issuer	is equal to	*<user name>*	Knowing the action issuer (owner) can help you assess whether an action is still needed. The issuer can be: • **Administrator (Windows) or tanium (Appliance)**: This is the account that Tanium solution services use to issue actions. For example, when you save a scan profile in Discover, the module automatically creates a corresponding scheduled action with Administrator as the issuer. Scheduled actions that the Tanium Server automatically imports through content-only solutions (such as **Core Content**) also have **Administrator** or **tanium** as the issuer. • **Tanium solution**: Tanium modules and shared services have solution-specific content that might include scheduled actions that the solution runs. For example, Tanium Endpoint Configuration is the issuer for the **Endpoint Configuration - Manifest** actions. To understand the purpose of these actions and the consequences of deleting them, see the user guides for the associated solutions. • **Tanium user**: Users might create scheduled actions for activities that are no longer relevant. For example, a user might create an action for initial testing of a new feature after a Tanium solution update and then never use the action again after testing finishes.

3. To disable actions that you want to stop deploying now but that you might deploy again in the future, select the actions and select **More > Disable Action(s)**.

4. To delete actions that are no longer useful, select the actions and select **More > Delete**.

5. To troubleshoot actions, see Tanium Console User Guide: Monitor actions.

Review and update Comply assessments

1. Go to **Modules > Comply > Assessments** and review the **Status** of assessments for errors or warnings. See Tanium Comply User Guide: Status definitions.

2. Investigate the error for each assessment.

   > To issue a question that returns details about all the endpoints associated with scan errors, click the **Scan Errors** value above the grid.

   a. In the assessment row, click Additional Data, scroll to **Endpoint Statistics**, and click the **Scan Errors** value.

   b. Click the **Endpoints** value to issue a question that returns details about the affected endpoints. You can then review the results and, optionally, issue a drill-down question to investigate the errors. See Tanium Console User Guide: Managing question results.

3. Troubleshoot assessments if necessary to resolve issues related to endpoint compliance distribution. See Tanium Comply User Guide: Troubleshooting.

4. Edit assessments if necessary to resolve issues. See Tanium Comply User Guide: Edit an assessment.

5. Delete outdated assessments and create new assessments if updated versions of configuration compliance standards are released. See Tanium Comply User Guide: Creating compliance assessments.

> NOTE
>
> Assessments that you delete on the **Assessments** page are removed from the Tanium Server but not from endpoints. Delete stale assessments from endpoints whenever you delete them from the server if retaining the associated data is no longer necessary. Otherwise, delete assessments from endpoints at intervals that preserve the data for a useful period without allowing the assessments to use too much disk space on endpoints. Base the intervals on how often users delete assessments from the server. See Tanium Comply User Guide: Delete stale assessments from endpoints.

Review and update custom action groups for Deploy

If you install Deploy with default settings, it includes the **Tanium Deploy** action group, to which the **All Computers** computer group is assigned. If you changed computer group assignments for the **Tanium Deploy** action group, or if you created custom action groups for Deploy, review those action groups and, if necessary, update them. For example, if you discover that the Deploy tools are not installed on all the necessary endpoints, you might have to change the computer group assignments in the **Tanium Deploy** action group.

1. From the Main menu, go to **Administration > Actions > Action Groups**.

2. Use the filters to list only the groups that are for Deploy operations. See Tanium Console User Guide: View action groups. For example, if the custom action groups all have the string "Deploy" in their names, enter `Deploy` in the **Filter items** field.

3. Edit, create, or delete action groups if necessary to ensure Deploy targets the correct computer groups. See Tanium Console User Guide: Managing action groups.

Review and update custom action groups for Patch

If you install Patch with default settings, it includes the **Patch** action group, to which the **Patch Supported Systems** computer group is assigned. If you changed computer group assignments for the **Patch** action group, or if you created custom action groups for Patch, review those action groups and, if necessary, update them. For example, if you discover that the Patch process is not starting on all the necessary endpoints, you might have to change the computer group assignments in the action group that is specified for **Patch - Start Patch Process** actions.

1. From the Main menu, go to **Administration > Actions > Action Groups**.

2. Use the filters to list only the groups that are for Patch operations. See Tanium Console User Guide: View action groups. For example, if the custom action groups all have the string "Patch" in their names, enter `Patch` in the **Filter items** field.

3. Edit, create, or delete action groups if necessary to ensure Patch targets the correct computer groups. See Tanium Console User Guide: Managing action groups.

Performing semi-annual maintenance

Review and update Deploy self-service profiles

Review Deploy self-service profiles and, if necessary, update them to ensure that users have access to all the self-service capabilities:

1. From the Main menu, go to **Administration > Modules > Deploy > Self Service Profiles** and review the profiles. Expand ▶ each profile and verify that all the operations are successful ✓.
2. From the Deploy menu, go to **Deployments > Self Service** and review the **Failures** column.
3. Troubleshoot self-service installations if necessary to resolve issues. See Tanium Deploy User Guide: Monitor and troubleshoot software installed by self service user request.
4. Edit, create, or delete self-service profiles if necessary to resolve issues. See Tanium Deploy User Guide: Managing end-user self service.

Performing annual maintenance

Test a planned failover

If you have an active-active Tanium Server deployment, fail over to your secondary server and then fail back to verify that the process works as expected. The failover steps depend on your Tanium infrastructure:

- **Appliance**: See Tanium Appliance Deployment Guide: Testing a planned failover.
- **Windows**: Contact Tanium Support on page 10 for the steps.

Test disaster recovery

Test restoring your Tanium deployment from a backup to verify that your disaster recovery plan works as expected. The restoration steps depend on your Tanium infrastructure:

- **Appliance**: See Tanium Appliance Deployment Guide: TanOS restore options.
- **Windows**: Contact Tanium Support on page 10 for the steps.

Performing as-needed maintenance

The following sections describe tasks you must perform at intervals that vary based on conditions in your Tanium environment or based on the policies of your organization.

Rotate certificates for Tanium Console, Module Server, and API access

Transport Layer Security (TLS) certificates secure connections to the Tanium Server, Module Server, and Tanium solution services for Tanium user and solution operations. For example, the `SOAPServer.crt` certificate secures user access to the Tanium Server for Tanium Console or API activities. If your organization has a certificate rotation policy, replace the TLS certificates at the intervals that the policy specifies. See Tanium Core Platform Deployment Reference Guide: Securing Tanium Console, API, and Module Server access.

Review and update Patch block lists

Review Patch block lists and, if necessary, update them:

1. Go to **Modules > Patch > Block Lists** and review the block lists.
2. Expand ▶ each block list that has one or more **Targets** (computer groups) and verify that the list is **Enforced**. If a list is **Unenforced** on endpoints or some endpoints have an **Old Version**, click the percentage (number) of affected endpoints to analyze the data in Interact.
3. Edit, create, or delete block lists if necessary to resolve issues. See Tanium Patch User Guide: Managing patches.