Red Hat Hardware Certification 2024

Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenStack Platform 17

Last Updated: 2024-05-30

Red Hat Hardware Certification 2024 Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide

For Use with Red Hat OpenStack Platform 17

Legal Notice

Abstract

The Red Hat OpenStack Platform Hardware Bare Metal Certification Policy Guide covers the procedural, technical and policy requirements for achieving a Red Hat Hardware Certification. Version 9.0 and 8.80 updated May 28, 2024.

Table of Contents

MAKING OPEN SOURCE MORE INCLUSIVE

Red Hat is committed to replacing problematic language in our code and documentation. We are beginning with these four terms: master, slave, blacklist, and whitelist. Due to the enormity of this endeavor, these changes will be gradually implemented over upcoming releases. For more details on making our language more inclusive, see our CTO Chris Wright's message.

CHAPTER 1. INTRODUCTION TO RED HAT OPENSTACK BARE-METAL HARDWARE CERTIFICATION POLICIES

The Red Hat OpenStack Platform (RHOSP) bare-metal hardware certification policy guide is intended for hardware vendors who want to certify their bare-metal servers with Red Hat. The RHOSP bare-metal certification tests ensures that you can orchestrate your servers automatically without manual intervention.

Through this program, if the servers meet the requirements you can certify your servers for the IPI component by deploying it on the Red Hat OpenStack Platform.

1.1. AUDIENCE

This guide is intended for Partners who offer their own infrastructure hardware like system servers, or management controllers for use with Red Hat OpenStack Platform in a supported customer environment.

1.2. OVERVIEW OF THE PROGRAM

The Red Hat OpenStack Platform (RHOSP) bare-metal hardware certification creates value for customers, because the systems can be managed and automatically deployed and redeployed with Red Hat OpenStack bare-metal hardware without manual intervention.

The certification process, through a series of tests, validates that a certified solution meets the requirements of an enterprise cloud, and is jointly supported by Red Hat and your organization.

The RHOSP bare-metal hardware certification program policies include multiple tests each with a series of subtests and checks, which are explained in the document.

CHAPTER 2. CERTIFICATION PREREQUISITES

NOTE

A strong working knowledge of Red Hat Enterprise Linux and Red Hat OpenStack is required. A Red Hat Certified Engineer and a Red Hat OpenStack Platform Certified Engineer accreditation is preferred and suggested before participating.

2.1. PARTNER ELIGIBILITY CRITERIA

Ensure to meet the following requirements before applying for a Red Hat bare-metal hardware certification:

- You are part of the Red Hat Hardware Certification program .
- You are in a support relationship with Red Hat by means of the TSANet network or a custom support agreement.

2.2. CERTIFICATION TARGETS

The certification targets provide details and requirements about the components and products relevant to the certification.

Specific information for each of the certification components is provided when applicable.

2.2.1. Server

- Ensure that the server must have the following certifications:
  - Red Hat Enterprise Linux System
  - Red Hat OpenStack Platform Compute Node
    Each certification is keyed to the specific Cloud Platform product version and its associated ironic revision. You can certify your server for RHOSP, if your hardware is compatible with the ironic drivers for that platform.
- The server must have a baseboard management controller (BMC) installed.

2.2.2. Red Hat Cloud Platform Products

Bare-metal certification

Through this program you can certify BMC and bare-metal servers on Red Hat OpenStack Platform 17.1.

2.2.3. Baseboard management controllers (BMC)

A BMC is a specialized microcontroller on a server's motherboard that manages the interface between systems management software and physical hardware. The bare metal service in Red Hat Platforms provisions systems in a cluster by using the BMC to control power, network booting, and automate node deployment and termination.

BMC can be certified as a component for use in leveraging components, across multiple server systems. Similar to Red Hat Hardware Certification programs, Red Hat leverages partners' internal quality testing to streamline the certification process without adding risk to customer environments.

Red Hat recommends partners using component leveraging features in bare-metal hardware certifications conduct their testing with the specific server system, BMC, and Red Hat cloud platform product to validate each combination. However, you do not need to submit individual certification results to Red Hat for every combination.

2.2.4. Bare Metal Drivers

IPI component certification

BMCs must use supported Red Hat OpenStack Platform Bare Metal Drivers provided in the corresponding Red Hat Cloud platform product. You cannot certify a BMC that requires an ironic driver that is not included in the Red Hat product.

CHAPTER 3. OVERVIEW OF BARE METAL CERTIFICATION

The bare-metal certification overview provides details about product publication in the catalog, product release, certification duration, and recertification.

3.1. PUBLICATION IN THE CATALOG

When you certify your server for bare-metal hardware on Red Hat OpenStack Platform, it is published in the Red Hat Ecosystem Catalog as **Bare Metal**. The Bare Metal Management feature also appears as a certified component of your server.

3.2. RED HAT PRODUCT RELEASES

You have access to and are encouraged to test with pre-released Red Hat software. You can begin your engagement with the Red Hat Certification team before Red Hat software is generally available (GA) to customers to expedite the certification process for your product. However, conduct official certification testing only on the GA releases of Red Hat OpenShift Container Platform bare-metal hardware.

3.3. CERTIFICATION DURATION

Certifications are valid starting with the specific major and minor releases of Red Hat OpenStack Platform software as tested and listed on the Red Hat Ecosystem Catalog. They continue to be valid through the last minor release of the major release. This allows customers to count on certifications from the moment they are listed until the end of the product's lifecycle.

3.4. RECERTIFICATION WORKFLOW

You do not need to recertify after a new major or minor release of RHOSP if you have not made changes to your product. However, it is your responsibility to certify your product again any time you make significant changes to it.

Red Hat recommends that you run the certification tests on your product periodically to ensure its quality, functionality, and performance with the supported versions of RHOSP.

To recertify your product, open a supplemental certification.

CHAPTER 4. CERTIFICATION TESTING

The certification testing briefs about the prerequisites for testing, understanding the certification process, and its requirements.

4.1. PREREQUISTES FOR CERTIFICATION TESTING

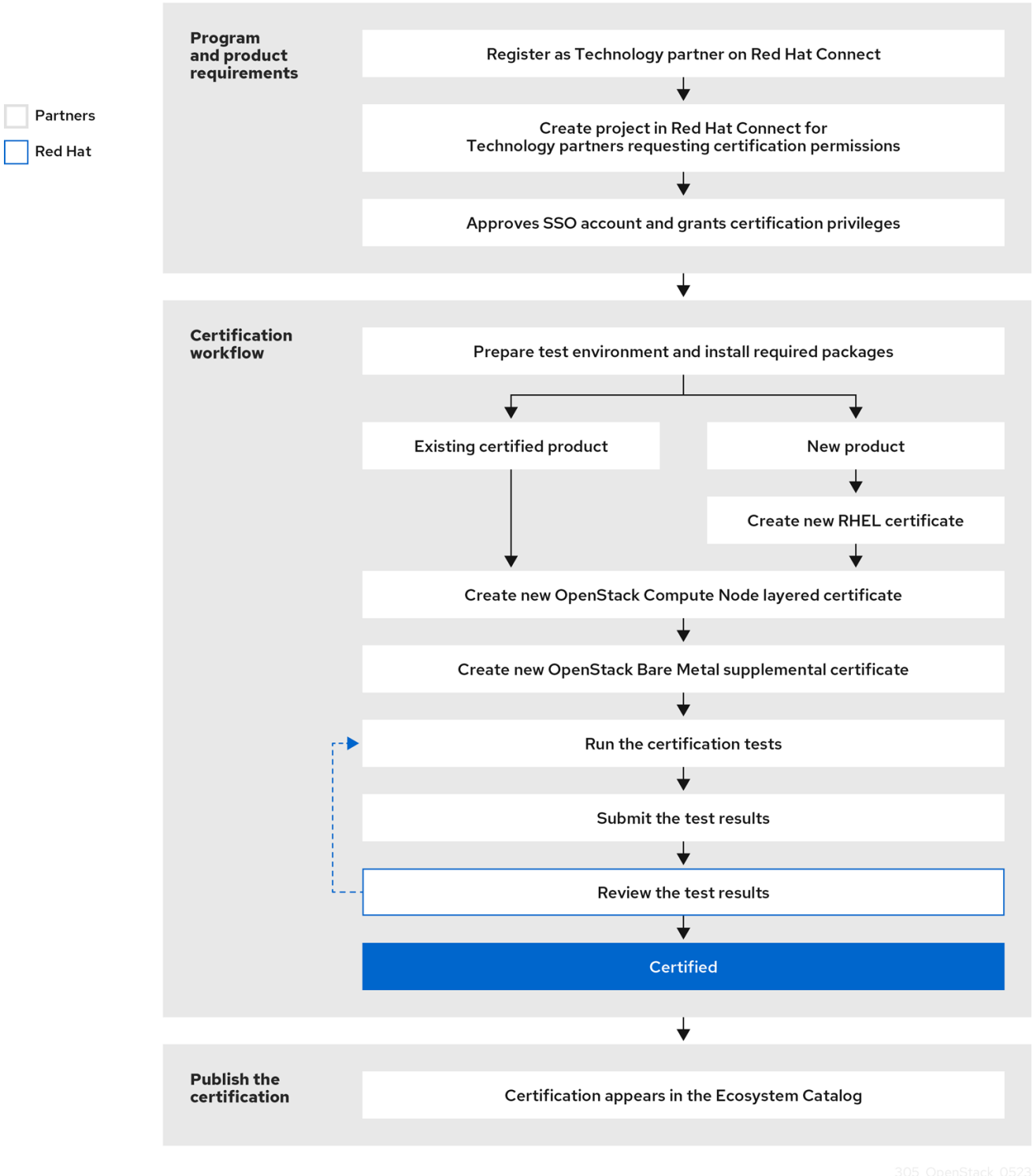
Bare-metal certification

- The corresponding RHEL server certification is successfully completed and posted.
- The corresponding Red Hat OpenStack Platform Compute Node certification is successfully completed and posted.
- The corresponding bare-metal driver is on the supported Drivers List for the corresponding Red Hat OpenStack Platform release.

4.2. CERTIFICATION WORKFLOW

The Red Hat Bare Metal Hardware certification process includes the following requirements and steps:

Figure 4.1. Red Hat OpenStack Platform Bare Metal Hardware Certification Process



4.3. CERTIFICATION REQUIREMENTS

Ensure you follow the Red Hat OpenStack bare metal hardware guide . Additional details for the certification requirements include:

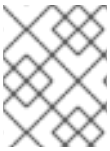
- The Host Under Test (HUT) must already be RHEL certified. Additionally, the tests must run on a previously certified server, and all the tests prescribed in the test plan must be executed in a single run.

- If you have a failed test, take the corrective action and execute **all the tests in a single run** Open a support case if necessary for guidance.

CHAPTER 5. LEVERAGING CERTIFICATION

Leveraging allows you to request credit for previous successful certification tests when similar or substantially similar BMCs are used across a family of server systems. It is based on your internal qualification testing of the specific BMC on each system, confirming that any variations are not material and the solution matches a previously certified one.

Leveraging can reduce the amount of official testing needed for certification. You can request leveraging when the solution includes a previously certified BMC with the same firmware branch and equal or fewer features.



NOTE

It is your responsibility to verify that any differences in BMC-to-server interaction do not affect the certification.

CHAPTER 6. PASS-THROUGH CERTIFICATION

A Pass-Through Certification refers to the ability of a third-party system or component to be granted certification for hardware previously certified by the original hardware manufacturer. Pass-Through can reduce the overall amount of testing that is required to be performed and submitted to Red Hat to achieve certification for the third-party hardware.

System manufacturers can extend a certification granted to their own systems to another vendor's system where the original vendor:

- Has permission from the third-party,
- Has the mechanics to ensure the third party does not alter the hardware in such a way that it would no longer be considered a subset of the original model certified by Red Hat, and
- Extends their responsibilities of support and representative hardware to include situations involving third-party hardware.

The third-party cannot then extend their Pass-Through Certification to another vendor.

While both vendors are required to be members of the Red Hat Hardware Certification Program, only the original vendor may request Pass-Through Certifications. Vendors may also utilize the Pass-Through process, where the same vendor has multiple names for the same hardware.

CHAPTER 7. SUPPLEMENTAL CERTIFICATION

Open supplemental certifications in the following scenarios:

First time certification

The bare-metal supplemental certification can be automatically created during a different certification process, for example, when you applied for the Red Hat Enterprise Linux System certification.
If it was not automatically created, or if you need to apply for the certification at a later date, open a new supplemental certification above the Red Hat OpenStack Compute Node certification.

Recertification

Open a supplemental certification to update an existing RHOSP bare-metal certification.
You may want to recertify your product, for example, to certify the same system on different versions of a Red Hat platform or because your product has received a significant update.

You are responsible for initiating these certifications and notifying Red Hat of any material changes to your product.

CHAPTER 8. IPI CERTIFICATION TESTS

The certification includes *self-check*, *supportable*, *director_undercloud* and *bare metal* tests.

8.1. SELF CHECK TEST

The **self-check** test confirms that all required software packages for certification are installed and unaltered, ensuring the test environment is ready for certification. Certification packages must not be modified for testing or any other purpose.

Success Criteria

The test environment includes all necessary certification packages and the packages have not been modified.

8.2. SUPPORTABLE TEST

The supportable test, also known as **baremetal/supportable**, ensures that the test environment is compliant with Red Hat's support policy. The test confirms that the test node (an OpenStack deployment under test) consists only of components supported by Red Hat (Red Hat OpenStack Platform, Red Hat Enterprise Linux).

An OpenStack deployment under test refers to the node where the plugin or application under test is installed.

Supportability tests must be run on both the control node and the compute node.

This test is required for all OpenStack software certifications.

Compute Node Considerations:

- If your kernel is not updated, ensure that you update the kernel test section to verify that the compute uses the GA kernel to prevent review exit. Review will need to account for the status of RHEL certification.
- Driver Update Programs (DUPs) are acceptable on the compute node but will cause the test to exit review. Review needs to confirm the DUP that aligns with the one used in the corresponding RHEL certification.

The **baremetal/supportable** tests include the following subtests:

8.2.1. Kernel subtest

The **kernel** subtest checks the kernel module running on the test environment. The version of the kernel can be either the original General Availability (GA) version or any subsequent kernel update released for the RHEL major and minor releases.

The kernel subtest also ensures that the kernel is not tainted when running in the environment.

Success criteria

- The running kernel is a Red Hat kernel.
- The running kernel is released by Red Hat for use with the RHEL version.

- The running kernel is not tainted.
- The running kernel has not been modified.

Additional resources

- Red Hat Enterprise Linux Life Cycle
- Red Hat Enterprise Linux Release Dates
- Why is the kernel "tainted" and how are the taint values deciphered?

8.2.2. Kernel modules subtest

The **kernel modules** subtest verifies that loaded kernel modules are released by Red Hat, either as part of the kernel's package or added through a Red Hat Driver Update. The kernel module subtest also ensures that kernel modules do not identify as Technology Preview.

Success criteria

- The kernel modules are released by Red Hat and supported.

Additional resources

- What does a "Technology Preview" feature mean?

8.2.3. Hardware Health subtest

The Hardware Health subtest checks the system's health by testing if the hardware is supported, meets the requirements, and has any known hardware vulnerabilities. The subtest does the following:

- Checks that the Red Hat Enterprise Linux (RHEL) kernel does not identify hardware as unsupported. When the kernel identifies unsupported hardware, it will display an unsupported hardware message in the system logs and/or trigger an unsupported kernel taint. This subtest prevents customers from possible production risks which may arise from running Red Hat products on unsupported configurations and environments.
  In hypervisor, partitioning, cloud instances, and other virtual machine situations, the kernel may trigger an unsupported hardware message or taint based on the hardware data presented to RHEL by the virtual machine (VM).
- Checks that the Host Under Test (HUT) meets the minimum hardware requirements.
  - RHEL 8 and 9: Minimum system RAM should be 1.5GB, per CPU logical core count.
  - RHEL 7: Minimum system RAM should be 1GB, per CPU logical core count.
- Checks if the kernel has reported any known hardware vulnerabilities, if those vulnerabilities have mitigations and if those mitigations have resolved the vulnerability. Many mitigations are automatic to ensure that customers do not need to take active steps to resolve vulnerabilities. In some cases this is not possible; where most of these remaining cases require changes to the configuration of the system BIOS/firmware which may not be modifiable by customers in all situations.
- Confirms the system does not have any offline CPUs.
- Confirms if Simultaneous Multithreading (SMT) is available, enabled, and active in the system.

Failing any of these tests will result in a WARN from the test suite and should be verified by the partner to have correct and intended behavior.

Success criteria

- The kernel does not have the UNSUPPORTEDHARDWARE taint bit set.
- The kernel does not report an unsupported hardware system message.
- The kernel should not report any vulnerabilities with mitigations as vulnerable.
- The kernel does not report the logic core to installed memory ratio as out of range.
- The kernel does not report CPUs in an offline state.

Additional resources

- Minimum required memory
- Hardware support available in RHEL 8 but removed from RHEL 9 .
- Hardware support available in RHEL 7 but removed from RHEL 8 .
- Hardware support available in RHEL 6 but removed from RHEL 7 .

8.2.4. Installed RPMs subtest

The **installed RPMs** subtest verifies that RPM packages installed on the system are released by Red Hat and not modified. Modified packages may introduce risks and impact the supportability of the customer's environment. You might install non-Red Hat packages if necessary, but you must add them to your product's documentation, and they must not modify or conflict with any Red Hat packages.

Red Hat will review the output of this test if you install non-Red Hat packages.

Success criteria

- The installed Red Hat RPMs are not modified.
- The installed non-Red Hat RPMs are necessary and documented.
- The installed non-Red Hat RPMs do not conflict with Red Hat RPMs or software.

Additional resources

- Production Support Scope of Coverage

8.2.5. System report subtest

Red Hat uses a tool called **sos** to collect configuration and diagnostics information from a RHEL system. The **sos** tool assists customers in troubleshooting a RHEL system and following the recommended practices.

The System Report subtest ensures that the sos tool functions as expected on the image or system and captures a basic sosreport.

Success Criteria

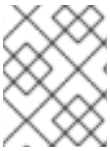
The RHCERT tool captures a basic sosreport on the OpenStack deployment under test.

Additional resources

- For more information about sosreport, see What is an sosreport and how to create one in Red Hat Enterprise Linux?

8.2.6. SELinux subtest

Confirms that SELinux is running in **enforcing mode** on the OpenStack deployment-under test.



NOTE

Security-Enhanced Linux (SELinux) adds Mandatory Access Control (MAC) to the Linux kernel, and is enabled by default in Red Hat Enterprise Linux.

SELinux policy is administratively-defined, enforced system-wide, and is not set at user discretion, reducing vulnerability to privilege escalation attacks helping limit the damage made by configuration mistakes. If a process becomes compromised, the attacker only has access to the normal functions of that process, and the files that the process has been configured to.

Success Criteria

SELinux is configured and running in enforcing mode on the OpenStack deployment under test.

Additional resources

- For more information on SELinux in RHEL, see SELinux Users and Administrators Guide .

8.3. DIRECTOR_UNDERCLOUD TEST

The Director_undercloud test, also known as **openstack/director**, ensures that the **deployment-under-test** is originally installed using Red Hat OpenStack Platform Director. This test is required for all OpenStack software certifications.

Red Hat OpenStack Platform Director is the supported toolset for installing and managing a Red Hat OpenStack Platform environment in production. It helps in easy installation of a lean and robust OpenStack cloud. It is specifically targeted for enterprise cloud environments where updates, upgrades, and infrastructure control are critical for underlying OpenStack operations.

Success Criteria

The deployment under test is originally installed using Red Hat OpenStack Platform Director.

Additional resources

- For more information on installing Red Hat OpenStack Platform Director, see Director Installation and Usage Guide.

8.4. BARE METAL TEST

The following sub-tests comprise the bare metal test. The tests perform enrolling, inspection and deployments to validate the bare metal node.

8.4.1. Bare Metal InstackStackrc validation

Validates the **instackenv.json** and **stackrc** files.

Success Criteria

- Checks if the **instackenv.json** and **stackrc** files exist in the specified location and validate the content of **instackenv.json** file, and
- Requires validation check if the file is a valid json file and the specified BMC IPs are reachable.

8.4.2. Bare Metal driver validation

Compares the drivers configured on the HUT with the drivers supported by Red Hat. If a driver mismatch occurs the subtest generates a *Review* state and exits.The drivers supported by Red Hat are part of the test suite

Success Criteria

- The specified driver should match with the driver in **instackenv.json** file, and
- If the drivers do not match the test will exit with a *Review* state. In this scenario, the Red Hat certification team will manually check the **instackenv.json** file and the specified driver to validate if the drivers are supported drivers.

8.4.3. Bare Metal undercloud validation

Checks if tests are running from the undercloud node. If the tests are not running from this node, the test fails and you need to rerun the test.

Success Criteria

Testing undercloud artifacts to check if the test ran from the undercloud node.

NOTE

The undercloud node is the valid node.

8.4.4. Bare Metal enrolling test

Checks if the bare-metal driver is successfully able to enroll the hardware node using the BMC IP. The enrollment process requires driver to communicate properly with BMC IP. The BMC changes the **Power state** and **Provisioning state** of the enrolled nodes to **off** and **available**.

The test also checks if the stack overcloud exists and if the nodes are already added. It deletes the stack and nodes if they exist, and then tries to enroll nodes based on the **instackenv.json** file. The test is failed if any of the stages fail.

Success Criteria

Enrolled nodes are expected to be in **Power** and **Provisioning** state.

8.4.5. Bare Metal inspecting test

Once the operator sets the required **driver_info** fields, BareMetalInspectingTest allows **Bare Metal** service to discover required node properties.

Success Criteria

Node properties should be correctly populated so that BMC can gather hardware details based on the instructions provided by the driver.

8.4.6. Bare Metal deploying test

Once the inspection is completed successfully,the Bare Metal Deploying Test will try to **nova boot** two virtual machines by creating and assigning a custom flavor to the nodes. This helps to check if BMCs can provide instances with the required boot images, and then try to boot up the instances.

Success Criteria

Start of VMs' with **Active** status attached to them.

8.4.7. Bare Metal redeploying test

Tries to redeploy nova instances.

Success Criteria

All the stages covered previously should pass in the redeploy too. The test enrolls and inspects the hardware instances, deploys the instances based on the enroll and inspect stages.