

What is claimed is:

1. A bare metal resource comprising:

a trusted portion including a processing circuit, a clearance manager, and an image repository; and

5 an untrusted portion including untrusted software that includes a basic input/output system (BIOS),

wherein the clearance manager is executable by the processing circuit during bootup of the bare metal resource prior to the BIOS to perform a clearance process on the untrusted portion, the clearance process including
10 deleting the BIOS in the untrusted portion and loading a trusted BIOS from the image repository on a storage device storing the untrusted software, to place the bare metal resource in a trusted state.
2. The bare metal resource of claim 1, wherein to perform the
15 clearance process, the clearance manager wipes the untrusted software and data from storage devices of the untrusted portion, and loads at least one trusted image, including the trusted BIOS, from the image repository to at least one of the storage devices of the untrusted portion.
- 20 3. The bare metal resource of claim 2, wherein the at least one trusted image comprises at least one of a device driver and firmware.

4. The bare metal resource of claim 2, wherein to perform the clearance process, the clearance manager sets a state of a real-time clock to a valid default value.
- 5 5. The bare metal resource of claim 1, wherein the bare metal resource is a computing resource available to a tenant of a cloud provider, and the untrusted portion is accessible by the tenant via a network after the bare metal resource is placed in the trusted state.
- 10 6. The bare metal resource of claim 5, wherein the bare metal resource is communicatively coupled to a trusted infrastructure device in a control plane of the cloud provider via an out-of-band channel, and the bare metal resource is configured to receive a signal from the trusted infrastructure device to invoke the clearance process.
- 15
7. The bare metal resource of claim 6, wherein the bare metal resource is configured to receive a second signal from the trusted infrastructure device via the out-of-band channel, after the trusted infrastructure device verifies the bare metal resource is in the trusted state, to cause the bare metal
- 20 resource to boot from the trusted BIOS loaded in the untrusted portion.

8. The bare metal resource of claim 6, wherein the trusted infrastructure device runs a timer to determine whether the clearance process is stalled.
- 5 9. The bare metal resource of claim 6, wherein the trusted infrastructure device is a rack controller, and the out-of-band channel comprises a wired connection between the rack controller and a connector on a system board of the bare metal resource.
- 10 10. The bare metal resource of claim 1, wherein the trusted portion and the untrusted portion are not simultaneously operational.
11. A bare metal resource in a pool of computing resources, the bare metal resource comprising:
- 15 a trusted portion including a memory storing a clearance manager, an image repository storing known good images, and a processing circuit to execute the clearance manager, wherein the trusted portion is inaccessible to a tenant;
- an untrusted portion, accessible to the tenant when the bare metal
- 20 resource is provisioned to the tenant, including hardware and untrusted software that comprises a basic input/output system (BIOS); and

a communication interface communicatively coupled to a trusted infrastructure device of a cloud provider via an out-of-band channel,

wherein in response to receiving a signal from the trusted infrastructure device via the out-of-band channel, the bare metal resource is
5 configured to boot from the clearance manager, and the clearance manager is configured to perform a clearance process on the untrusted portion, including deleting the BIOS in the untrusted portion and loading a trusted BIOS from the image repository on a storage device in the untrusted portion, to place the bare metal resource in a trusted state.

10

12. The bare metal resource of claim 11, wherein the bare metal resource is configured to receive a second signal from the trusted infrastructure device via the out-of-band channel to cause the bare metal resource to boot from the trusted BIOS loaded in the untrusted portion after the bare metal
15 resource is in the trusted state.

13. A method comprising:
receiving, from a trusted infrastructure device of a cloud provider, a signal at a bare metal resource operable to be provisioned to a tenant of the
20 cloud provider;

triggering a boot of the bare metal resource from a trusted portion of the bare metal resource responsive to the signal;

performing, by a clearance manager in the trusted portion, a clearance process to wipe storage devices of an untrusted portion of the bare metal resource and to load a known good image of a basic input/output system (BIOS) from an image repository of the trusted portion of the bare metal resource to the untrusted portion; and

rebooting the bare metal resource from the BIOS loaded on the untrusted portion from the image repository.

14. The method of claim 13, wherein the trusted infrastructure device transmits the signal to the bare metal resource responsive to an indication that the bare metal resource is being released from the tenant or an indication that the bare metal resource is in a non-operational state.

15. The method of claim 13, wherein rebooting the bare metal resource is in response to receiving a second signal from the trusted infrastructure device, wherein the trusted infrastructure device transmits the second signal to the bare metal resource after verifying the clearance process is successfully completed.