CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

~~under the control of one or more computer systems configured with executable instructions,~~

storing, in a secure store on a host computing device of a multi-tenant computing environment, one or more credentials, the host computing device including a recovery image capable of utilizing the one or more credentials stored in the secure store, the multi-tenant computing environment including a plurality of remote computing devices for use in performing a task in the multi-tenant computing environment;

rebooting the host computing device;

determining, during the rebooting, a set of conditions relating to a prior shutdown of the host computing device;

contacting the plurality of remote computing devices to determine a status of the plurality of remote computing devices, the status indicating that an abnormal shutdown occurred on each of the plurality of remote computing devices;

determining, based at least in part on the status and the set of conditions, that an unexpected ~~a~~ failure resulting in abnormal shutdown likely occurred on the host computing device prior to rebooting the host computing device;

loading the recovery image onto the host computing device; and

providing the recovery image running on the host computing device with access to the one or more credentials stored in the secure store, wherein the one or more credentials are used to initiate one or more services on the host computing device.

2. The computer implemented method of claim 1, wherein the credentials stored in the secure store further comprise a first cryptographic key capable of being used to decrypt a second cryptographic key, the second cryptographic key capable of being used to decrypt the recovery image.

3. The computer implemented method of claim 1, wherein the credentials stored in the secure store further comprise a cryptographic key used to decrypt the recovery image.

4. The computer implemented method of claim 1, wherein determining that the unexpected ~~a~~ failure likely occurred on the host computing device is performed by firmware operating on the host computing device~~, the firmware configured to analyze a set of conditions and determine, based at least in part on the set of conditions, that the host computing device was terminated abnormally~~.

5. The computer implemented method of claim 4, wherein loading the recovery image further comprises:

obtaining a boot firmware measurement of the firmware operating on the host computing device;

verifying the firmware operating on the host computing device by comparing the boot firmware measurement with a reference firmware measurement stored in the secure store;

providing the firmware with access to a cryptographic key stored in the secure store, wherein the firmware is configured to decrypt the recovery image using the cryptographic key; and

loading the decrypted recovery image onto the host computing device.

6. The computer implemented method of claim 1, wherein providing the recovery image running on the host computing device with access to the one or more credentials stored in the secure store further comprises:

obtaining a boot firmware measurement of the loaded recovery image;

verifying that a correct version of the recovery image has been loaded based on the obtained boot firmware measurement; and

providing the recovery image with access to the one or more credentials in response to verifying that the correct version of the recovery image has been loaded.

7. The computer implemented method of claim 1, further comprising:

receiving, the host computing device, the one or more credentials from a remote host computing device; and

storing the received one or more credentials into the secure store.

8. The computer implemented method of claim 1, wherein the secure store is a trusted platform module (TPM) on the host computing device.

9. The computer implemented method of claim 1, wherein the host computing device hosts one or more virtual machines provisioned for a user, the one or more virtual machines executing at least one application accessible by the user over a network by using an application programming interface (API).

10. The computer implemented method of claim 1, wherein the host computing device is configured to use the one or more credentials to authenticate the host computing device to one or more remote devices over a network connection.

11. A computing device of a multi-tenant computing environment, the multi-tenant computing environment including a plurality of remote computing devices for use in performing a task in the multi-tenant computing environment, comprising:

a secure store;

at least one processor; and

memory including instructions that, when executed by the at least one processor, cause the computing device to:

store one or more credentials in the secure store;

boot the computing device;

determine, ~~based on~~ a set of conditions relating to a prior shutdown of the computing device during the booting;

contacting the plurality of remote computing devices to determine a status of the plurality of remote computing devices, the status indicating that an abnormal shutdown occurred on each of the plurality of remote computing devices;

determining, based at least in part on the status and the set of conditions, that an unexpected ~~a~~ failure resulting in abnormal shutdown likely occurred on the computing device prior to booting the computing device;

load the recovery image into the memory of the computing device; and

provide the recovery image with access to the one or more credentials stored in the secure store, wherein the one or more credentials are used to initiate one or more services on the computing device.

12. The computing device of claim 11, wherein determining that the unexpected ~~a~~ failure likely occurred on the computing device is performed by firmware operating on the

computing device~~, the firmware configured to analyze a set of conditions and determine, based at least in part on the set of conditions, that the computing device terminated abnormally~~.

13. The computing device of claim 12, wherein loading the recovery image further comprises:

obtaining a boot firmware measurement of the firmware operating on the computing device;

verifying the firmware operating on the computing device by comparing the boot firmware measurement with a reference firmware measurement stored in the secure store;

providing the firmware with access to a cryptographic key stored in the secure store, wherein the firmware is configured to decrypt the recovery image using the cryptographic key; and

loading the decrypted recovery image into the memory of the computing device.

14. The computing device of claim 11, wherein providing the recovery image running on the computing device with access to the one or more credentials stored in the secure store further comprises:

obtaining a boot firmware measurement of the loaded recovery image;

verifying that a correct version of the recovery image has been loaded based on the obtained boot firmware measurement; and

providing the recovery image with access to the one or more credentials in response to verifying that the correct version of the recovery image has been loaded.

15. The computing device of claim 11, wherein the memory further includes instructions executed by the at least one processor to cause the computing device to:

receive the one or more credentials from a remote host computing device; and

store the received one or more credentials into the secure store.

CLAIMS

What is claimed is:

1. A computer implemented method, comprising:

storing, in a secure store on a host computing device of a multi-tenant computing environment, one or more credentials, the host computing device including a recovery image capable of utilizing the one or more credentials stored in the secure store, the multi-tenant computing environment including a plurality of remote computing devices for use in performing a task in the multi-tenant computing environment;

rebooting the host computing device;

determining, during the rebooting, a set of conditions relating to a prior shutdown of the host computing device;

contacting the plurality of remote computing devices to determine a status of the plurality of remote computing devices, the status indicating that an abnormal shutdown occurred on each of the plurality of remote computing devices;

determining, based at least in part on the status and the set of conditions, that an unexpected failure resulting in abnormal shutdown likely occurred on the host computing device prior to rebooting the host computing device;

loading the recovery image onto the host computing device; and

providing the recovery image running on the host computing device with access to the one or more credentials stored in the secure store, wherein the one or more credentials are used to initiate one or more services on the host computing device.

2. The computer implemented method of claim 1, wherein the credentials stored in the secure store further comprise a first cryptographic key capable of being used to decrypt a second cryptographic key, the second cryptographic key capable of being used to decrypt the recovery image.

3. The computer implemented method of claim 1, wherein the credentials stored in the secure store further comprise a cryptographic key used to decrypt the recovery image.

4. The computer implemented method of claim 1, wherein determining that the unexpected failure likely occurred on the host computing device is performed by firmware operating on the host computing device.

5. The computer implemented method of claim 4, wherein loading the recovery image further comprises:

obtaining a boot firmware measurement of the firmware operating on the host computing device;

verifying the firmware operating on the host computing device by comparing the boot firmware measurement with a reference firmware measurement stored in the secure store;

providing the firmware with access to a cryptographic key stored in the secure store, wherein the firmware is configured to decrypt the recovery image using the cryptographic key; and

loading the decrypted recovery image onto the host computing device.

6. The computer implemented method of claim 1, wherein providing the recovery image running on the host computing device with access to the one or more credentials stored in the secure store further comprises:

obtaining a boot firmware measurement of the loaded recovery image;

verifying that a correct version of the recovery image has been loaded based on the obtained boot firmware measurement; and

providing the recovery image with access to the one or more credentials in response to verifying that the correct version of the recovery image has been loaded.

7. The computer implemented method of claim 1, further comprising:

receiving, the host computing device, the one or more credentials from a remote host computing device; and

storing the received one or more credentials into the secure store.

8. The computer implemented method of claim 1, wherein the secure store is a trusted platform module (TPM) on the host computing device.

9. The computer implemented method of claim 1, wherein the host computing device hosts one or more virtual machines provisioned for a user, the one or more virtual machines executing at least one application accessible by the user over a network by using an application programming interface (API).

10. The computer implemented method of claim 1, wherein the host computing device is configured to use the one or more credentials to authenticate the host computing device to one or more remote devices over a network connection.

11. A computing device of a multi-tenant computing environment, the multi-tenant computing environment including a plurality of remote computing devices for use in performing a task in the multi-tenant computing environment, comprising:

a secure store;

at least one processor; and

memory including instructions that, when executed by the at least one processor, cause the computing device to:

store one or more credentials in the secure store;

boot the computing device;

determine, a set of conditions relating to a prior shutdown of the computing device during the booting;

contacting the plurality of remote computing devices to determine a status of the plurality of remote computing devices, the status indicating that an abnormal shutdown occurred on each of the plurality of remote computing devices;

determining, based at least in part on the status and the set of conditions, that an unexpected failure resulting in abnormal shutdown likely occurred on the computing device prior to booting the computing device;

load the recovery image into the memory of the computing device; and

provide the recovery image with access to the one or more credentials stored in the secure store, wherein the one or more credentials are used to initiate one or more services on the computing device.

12. The computing device of claim 11, wherein determining that the unexpected failure likely occurred on the computing device is performed by firmware operating on the computing device.

13. The computing device of claim 12, wherein loading the recovery image further comprises:

obtaining a boot firmware measurement of the firmware operating on the computing device;

verifying the firmware operating on the computing device by comparing the boot firmware measurement with a reference firmware measurement stored in the secure store;

providing the firmware with access to a cryptographic key stored in the secure store, wherein the firmware is configured to decrypt the recovery image using the cryptographic key; and

loading the decrypted recovery image into the memory of the computing device.

14. The computing device of claim 11, wherein providing the recovery image running on the computing device with access to the one or more credentials stored in the secure store further comprises:

obtaining a boot firmware measurement of the loaded recovery image;

verifying that a correct version of the recovery image has been loaded based on the obtained boot firmware measurement; and

providing the recovery image with access to the one or more credentials in response to verifying that the correct version of the recovery image has been loaded.

15. The computing device of claim 11, wherein the memory further includes instructions executed by the at least one processor to cause the computing device to:

receive the one or more credentials from a remote host computing device; and

store the received one or more credentials into the secure store.