Once critical infrastructure is in place, working, and live, the cost or risk often may seem to outweigh the benefit of changing the system. The problems involved in making changes to live IT systems or environments can create substantial and at times catastrophic problems for users or entities that rely on these systems. At the very least, the amount of time it takes to trouble shoot and fix failures or problems occurring during change management may require substantial resources of time, personnel and money. The technical problems potentially created when changes are made to live environments can have cascading effects and may not be solved solely by undoing the changes made. Many of these issues contribute to inability to expeditiously rebuild a system if there are failures during the change management.

Furthermore, a bare metal cloud node or resource within an IT system may be vulnerable to security issues, compromised, or accessed by a rogue user. A hacker, attacker or rogue user may pivot off of that node or resource to access or hack into any other portions of the IT system or networks coupled to the node. A baremetal cloud node or a controller of an IT system may also be vulnerable through a resource connected to an applications network that may expose system to security threats or otherwise compromise the system. According to various example embodiments disclosed herein, an IT system may be configured to improve security in bare metal cloud nodes or resources interfacing the internet or from application networks whether or not connected to an external network.

Summary of Invention

According to a first aspect of the present invention, there is provided an information technology (IT) computer system comprising:

a controller;

a resource for connection to the controller, wherein the resource comprises a first service and a second service, wherein the first and second services have dependency with respect to each other, wherein the first service comprises a dependency service with respect to the second service, and wherein the second service comprises a dependent service with respect to the first service; and

an application programming interface (API) that interfaces the first and second services with each other and with the controller; and

wherein the controller is configured to manage an interoperability of the first service with respect to the second service.

According to a second aspect of the present invention, there is provided an information technology (IT) method for use with a computer system comprising a controller, a resource connected to the controller, wherein the resource comprises a first service and a second service, wherein the first and second services have dependency with respect to each other, wherein the first service comprises a dependency service with respect to the second service, and wherein the second service comprises a dependent service with respect to the first service, the method comprising:

interfacing the first and second services with each other and with the controller via an application programming interface; and

the controller managing an interoperability of the first service with respect to the second service.

According to example embodiments, an IT system comprises a bare metal cloud node or physical resource. When the bare metal cloud node or physical resource is turned on, set up, managed or used, if it may be connected to a network with nodes that other people or customers may be using, the in band management may be omitted, switchable, disconnectable or filtered from the controller. In addition, an application or applications network within a system may be disconnected, disconnectable, switchable, or filtered from the controller by way of resource(s) to which the application network is coupled to a controller.

A physical resource that comprises a virtual machine or hypervisor may also be vulnerable to security issues, compromised or accessed by a rogue user where the hypervisor may be used to pivot to another hypervisor that is a shared resource. An attacker may break out of the virtual machine and may have network access to management and or administration systems by way of the controller. According to various example embodiments disclosed herein the IT system may be configured to improve security where one or more physical resources that comprise a virtual resource on a cloud platform may disconnected, disconnectable, filtered, filterable or not connected to a controller by way of in-band management connection.

WHAT IS CLAIMED IS:

1. An information technology (IT) computer system comprising:

a controller;

a resource for connection to the controller, wherein the resource comprises a first service and a second service, wherein the first and second services have dependency with respect to each other, wherein the first service comprises a dependency service with respect to the second service, and wherein the second service comprises a dependent service with respect to the first service; and

an application programming interface (API) that interfaces the first and second services with each other and with the controller; and

wherein the controller is configured to manage an interoperability of the first service with respect to the second service.

2. The system of claim 1 wherein the second service is configured to issue a call on the first service through the API for the first service to perform an operation.

3. The system of any of claims 1-2 wherein the first service is configured to ask the controller to validate the second service in order to perform an operation for the second service.

4. The system of claim 3 wherein the controller is further configured to validate the second service based on at least one of mutual tls authentication, public key authorization, and/or network-based validation.

5. The system of any of claims 1-4 wherein the first service is configured to perform an operation for the second service contingent on a permission from the controller.

6. The system of any of claims 1-5 wherein the controller is further configured to provision encryption keys to the first and second services for use in validation of the first and second services.

7. The system of claim 6 wherein the encryption keys comprise different key pairs for each of the first and second services, each key pair comprising a public key and a private key.

8. The system of claim 7 wherein the controller is further configured to delete its copies of the private keys after provision of the private keys to the first and second services, and wherein the controller is configured to manage validation of the first and second services based on the public keys.

9. The system of any of claims 1-8 wherein the controller is further configured to disconnect the resource from any external networks when the first and/or second service is being configured by the controller.

10. The system of claim 9 wherein the controller is further configured to re-connect the resource to any disconnected external networks after the first and/or second service has been configured by the controller.

11. The system of any of claims 9-10 further comprising at least one of an in band connection, an out of band connection, and/or a storage area network connection between the resource and the controller, and wherein the controller is further configured to disconnect the resource from the in band connection, out of band connection, and/or storage area network connection when the first and/or second service is being configured by the controller.

12. The system of claim 11 wherein the controller is further configured to re-connect the resource to the disconnected in band connection, out of band connection, and/or storage area network connection after the first and/or second service has been configured by the controller.

13. The system of any of claims 1-12 wherein the controller is further configured to resolve dependencies between the first and second services.

14. An information technology (IT) method for use with a computer system comprising a controller, a resource connected to the controller, wherein the resource comprises a first service and a

second service, wherein the first and second services have dependency with respect to each other, wherein the first service comprises a dependency service with respect to the second service, and wherein the second service comprises a dependent service with respect to the first service, the method comprising:

interfacing the first and second services with each other and with the controller via an application programming interface; and

the controller managing an interoperability of the first service with respect to the second service.

15. The method of claim 14 further comprising:

the second service calling on the first service through the API for the first service to perform an operation.

16. The method of any of claims 14-15 further comprising:

the first service asking the controller to validate the second service in order to perform an operation for the second service.

17. The method of claim 16 further comprising:

the controller validating the second service based on at least one of mutual tls authentication, public key authorization, and/or network-based validation.

18. The method of any of claims 14-17 further comprising:

the first service performing an operation for the second service contingent on a permission from the controller.

19. The method of any of claims 14-18 further comprising:

the controller provisioning encryption keys to the first and second services for use in validation of the first and second services.

20. The method of claim 19 wherein the encryption keys comprise different key pairs for each of the first and second services, each key pair comprising a public key and a private key.

21. The method of claim 20 further comprising:

the controller deleting its copies of the private keys after provision of the private keys to the first and second services; and

controller managing validation of the first and second services based on the public keys.

22. The method of any of claims 14-21 further comprising:

the controller disconnecting the resource from any external networks when the first and/or second service is being configured by the controller.

23. The method of claim 22 further comprising:

the controller re-connecting the resource to any disconnected external networks after the first and/or second service has been configured by the controller.

24. The method of any of claims 22-23 wherein the resource is connected to the controller via at least one of an in band connection, an out of band connection, and/or a storage area network connection between the resource and the controller, the method further comprising:

the controller is further disconnecting the resource from the in band connection, out of band connection, and/or storage area network connection when the first and/or second service is being configured by the controller.

25. The method of claim 24 further comprising:

the controller re-connecting the resource to the disconnected in band connection, out of band connection, and/or storage area network connection after the first and/or second service has been configured by the controller.

26. The method of any of claims 14-25 further comprising:

the controller resolving dependencies between the first and second services.