

CONFIGURATION AND VERIFICATION BY TRUSTED PROVIDER

CROSS-REFERENCE TO RELATED APPLICATIONS

[0001] This application claims the benefit of U.S. Patent Application No. 13/784,276, filed March 4, 2013, the disclosure of which is incorporated herein by reference in its entirety.

BACKGROUND

[0002] A data center is a facility that houses computer systems and various networking, storage, and other related components. Data centers may, for example, provide computing services to businesses and individuals as a remote computing service or to provide “software as a service” (e.g., cloud computing). The computing resources provided by a data center may include various types of resources, such as data processing resources, data storage resources, data communication resources, and the like.

[0003] To facilitate increased utilization of data center resources, virtualization technologies may allow a single physical computing machine to host one or more instances of virtual machines that appear and operate as independent computer machines to a connected computer user. With virtualization, the single physical computing device can create, maintain, or delete virtual machines in a dynamic manner. When a customer of a data center requests a new virtual machine instance, the data center may provide a virtual machine management service that identifies a “slot” for executing the new instance. Customers may sometimes request a virtual machine instance with a particular configuration. In some cases, the configuration may include software and data that is provided by the customer or by a third party supplier.

SUMMARY OF INVENTION

[0003a] According to a first aspect of the present invention, there is provided a computing system configured to manage virtual machine instances on behalf of a plurality of users, the computing system comprising: at least one computing device; and at least one memory in communication with the at least one computing device, the at least one memory having stored thereon computer readable instructions that, when executed by the computing system, cause the computing system to at least: receive a request for ~~an~~ one or more virtual machine instances; in response to receiving the request for the one or more virtual machine instances, ~~instantiating the a requested virtual machine instance~~, wherein ~~instantiating the requested virtual machine instance~~ includes ~~loading operating system software or data~~ associated with a configuration for the virtual machine instance; ~~auditing the instantiated virtual machine instance~~ to generate a record of the ~~loaded operating system software or data~~; ~~computing a configuration integrity verifier based on the record of loaded operating system the software or data and a the configuration for the instantiated virtual machine instance~~; and in

response to a request for verification of the ~~operating system~~ software or data, providing the configuration integrity verifier, information regarding the audited instantiated virtual machine instance, and the record of loaded ~~operating system~~ software or data as a trusted third party verification that the ~~operating system~~ software or data were used to instantiate the instance.

[0003b] According to a second aspect of the present invention, there is provided a method for verifying a computing configuration by a provider network providing virtualized computing resources to a plurality of users, the method comprising: receiving a request for ~~a one or more virtualized computing resources~~, wherein providing the one or more virtualized computing resources includes loading of code ~~or and~~ data; in response to receiving the request for ~~the one or more virtualized computing resources~~, instantiating ~~the requested a virtualized computing resource by including~~ loading ~~said code or and data associated with the instantiated virtualized computing resource~~; auditing said loaded code ~~or and~~ data associated with the instantiated virtualized computing resource to generate a record of the loaded code ~~or and~~ data associated with the instantiated virtualized computing resource; computing a configuration integrity verifier based on the record of the loaded code ~~or and~~ data associated with the instantiated virtualized computing resource; and sending the configuration integrity verifier in response to a request for verification of the loaded code ~~or and~~ data associated with the instantiated virtualized computing resource, the configuration integrity verifier being usable as a trusted verification of the loaded code ~~or and~~ data associated with the instantiated virtualized computing resource.

BRIEF DESCRIPTION OF DRAWINGS

[0004] Throughout the drawings, reference numbers may be reused to indicate correspondence between referenced elements. The drawings are provided to illustrate example embodiments described herein and are not intended to limit the scope of the disclosure.

[0005] Figure 1 is a diagram illustrating a mechanism for providing a configuration verification service in accordance with the present disclosure;

[0006] Figure 2 is a diagram illustrating an example computer system that may be used in some embodiments.

[0007] Figure 3 is a diagram illustrating a mechanism for providing a configuration verification service in accordance with the present disclosure;

CLAIMS

WHAT IS CLAIMED IS:

1. A computing system configured to manage virtual machine instances on behalf of a plurality of users, the computing system comprising:
 - at least one computing device; and
 - at least one memory in communication with the at least one computing device, the at least one memory having stored thereon computer readable instructions that, when executed by the computing system, cause the computing system to at least:
 - receive a request for ~~an~~ one or more virtual machine instances;
 - in response to receiving the request for the one or more virtual machine instances, ~~instantiating the a requested virtual machine instance~~, wherein instantiating the ~~requested virtual machine instance~~ includes loading ~~operating system~~ software or data associated with a configuration for the virtual machine instance;
 - auditing the instantiated virtual machine instance to generate a record of the loaded ~~operating system~~ software or data;
 - ~~compute~~ing a configuration integrity verifier based on the record of ~~loaded operating system~~ the software or data and ~~a the~~ configuration for the instantiated virtual machine instance;
 - and
 - in response to a request for verification of the ~~operating system~~ software or data, ~~provide~~ing the configuration integrity verifier, information regarding the audited instantiated virtual machine instance, and the record of loaded ~~operating system~~ software or data as a trusted third party verification that the ~~operating system~~ software or data were used to instantiate the instance .
2. The system according to claim 1, wherein the configuration integrity verifier comprises a checksum.
3. The system according to claim 1, wherein the request for verification of the ~~operating system software or data~~ is received from a provider of the configuration or a user of the instance.
4. The system according to claim 1, wherein a provider of the configuration integrity verifier is validated by a verification service.
5. The system according to claim 1, wherein the configuration integrity verifier is validated by a digital certificate in a public-key infrastructure.
6. The system according to claim 1, wherein permission to provide verification of ~~operating system or data~~ the software is authorized by a requestor of the instance.

7. A method for verifying a computing configuration by a provider network providing virtualized computing resources to a plurality of users, the method comprising:

receiving a request for a-one or more virtualized computing resources, wherein providing the one or more virtualized computing resources includes loading of code ~~or~~ and data;

in response to receiving the request for the one or more virtualized computing resources, ~~instantiating the requested~~ a virtualized computing resource by including loading ~~said code or~~ and data associated with the instantiated virtualized computing resource;

auditing said loaded code ~~or~~ and data associated with the instantiated virtualized computing resource to generate a record of the loaded code ~~or~~ and data associated with the instantiated virtualized computing resource;

computing a configuration integrity verifier based on the record of the loaded code ~~or~~ and data associated with the instantiated virtualized computing resource; and

sending the configuration integrity verifier in response to a request for verification of the loaded code ~~or~~ and data associated with the instantiated virtualized computing resource, the configuration integrity verifier being usable as a trusted verification of the loaded code ~~or~~ and data associated with the instantiated virtualized computing resource.

8. The method of claim 7, wherein the request is received in a computing environment comprising a plurality of computing devices providing computing resources.

9. The method of claim 7, wherein the virtualized computing resource is a virtual machine.

10. The method of claim 7, wherein the configuration integrity verifier is sent to a provider of the code ~~or~~ and data in response a request from the provider of the code ~~or~~ and data for verification of the code ~~or~~ and data.

11. The method of claim 7, wherein the configuration integrity verifier is sent to a user of the code ~~or~~ and data in response a request by the user of the computing resource for verification of the code ~~or~~ and data.

12. The method of claim 7, wherein the configuration integrity verifier is sent to a provider of the code ~~or~~ and data prior to a user of the computing resource accessing the computing resource.

13. The method of claim 7, wherein the configuration integrity verifier comprises a checksum.

14. The method of claim 7, wherein the configuration integrity verifier is validated by a digital certificate in a public-key infrastructure.

15. The method of claim 7, wherein the configuration integrity verifier is sent to a service provider authorized by a provider of the code ~~or~~ and data.