CLAIMS

1. A method for reducing attack surface by selectively collocating applications on host computers, the method comprising:

measuring system resources utilized by each application running in a plurality of host computers of a data processing environment;

determining which applications running in the plurality of host computers utilize similar system resources; and

collocating those applications utilizing similar system resources on respective host computers, wherein the collocating comprises:

determining a greatest amount of attack surface reduction in each respective host computer based on placement of a particular set of applications having a similar system resource utilization footprint on a particular host computer and removal of a determined set of unused system resources corresponding to that particular host computer running that particular set of applications;

assigning each respective set of applications having the similar system resource utilization footprint to a specified host computer that has the greatest determined amount of attack surface reduction; and

placing each respective set of applications having the similar system resource utilization footprint on its assigned host computer in the data processing environment.

2. The method of claim 1 further comprising:

determining unused system resources not used by resident applications running on a set of host computers in the plurality of host computers; and

removing the unused system resources corresponding to each respective host computer in the set of host computers to reduce the attack surface in the data processing environment, wherein the determining the unused system resources not used by the resident applications comprises:

obtaining a list of system resources corresponding to each respective host computer in the plurality of host computers;

identifying a set of used system resources in the list of system resources corresponding to each respective host computer being utilized by a running resident application; and

determining a set of unused system resources corresponding to each respective host computer by subtracting the set of used system resources from the list of system resources corresponding to each respective host computer.

3. The method of claim 1 further comprising:

performing a boot strap operation on the plurality of host computers in the data processing environment;

profiling the applications running on the plurality of host computers to obtain a system resource utilization footprint of each respective application, wherein a system resource utilization footprint identifies a pattern of system resource usage by a particular application running on a host computer; and

identifying a plurality of different sets of applications having similar system resource utilization footprints based on the profiling of the applications.

4. The method of claim 1 wherein the collocating comprises placing the those applications utilizing similar system resources together on a same host computer.

5. The method of claim 1 further comprising:

placing a new application on a server;

profiling the new application to determine a system resource utilization footprint of the new application;

obtaining system resource availability of each respective host computer in the plurality of host computers;

identifying any host computer that has available system resources to run the new application based on the system resource utilization footprint of the new application; and

determining whether any host computers have available system resources to run the new application.

6. The method of claim 5 further comprising:

responsive to determining that a set of host computers in the plurality of host computers has available system resources to run the new application, assigning the new application to a host computer in the set having one or more running resident applications with similar resource utilization footprints as the new application; and

placing the new application on the host computer having the one or more running resident applications with similar resource utilization footprints as the new application.

7. The method of claim 5 further comprising:

responsive to determining that no host computer in the plurality of host computers has available system resources to run the new application, selecting a host computer in the plurality of host computers that has a fewest number of running resident applications;

migrating resident applications from the selected host computer to the server;

resetting the selected host computer to an initial default state to form a reset host computer;

migrating previously migrated applications from the selected host computer back to the reset host computer from the server;

placing the new application on the reset host computer; and

removing system resources not utilized by running resident applications on the reset host computer to decrease an attack surface on the reset host computer.

8. The method of claim 1 further comprising:

responsive to determining that a defined time interval expired, obtaining a list of available system resources corresponding to each host computer in a plurality of host computers included in the data processing environment monitored;

obtaining system resource utilization of resident applications running on each host computer in the plurality of host computers;

determining whether unused system resources exist on any host system based on the list of available system resources corresponding to each respective host computer and the system resource utilization of the resident applications running on each respective host computer; and

responsive to determining that unused system resources do exist on one or more host systems, removing the unused system resources existing on the one or more host systems to decrease an attack surface of those host systems in the data processing environment.

9. The method of claim 1, wherein the attack surface is a sum of different points where an unauthorized user can attempt to gain access to computer resources in the plurality of host computers, and further comprising:

identifying and analyzing all possible application and host computer combinations in the plurality of host computers; and

selecting application collocation assignments where a sum of all sets of unused resources in the plurality of host computers is greatest to maximize unused resource reduction across all host computers in the plurality.

10. The method of claim 1, wherein the collocating includes removing applications from a first client host computer and installing the applications on a second client host computer.

11. The method of claim 1, wherein the system resources comprise a runtime environment that include host computer resources and network resources, and wherein the host computer resources and network resources are selected from a group consisting of libraries, kernel system calls, kernel subsystems,

hypervisors, network services, internet protocol addresses, port numbers, sensitive network user accounts with elevated access privileges, and sensitive network applications with elevated access privileges.

12. The method of claim 1, wherein the data processing environment is one of a group consisting of a cluster and a cloud environment.

13. A computer system for reducing attack surface by selectively collocating applications on host computers, the computer system comprising:

a bus system;

a storage device connected to the bus system, wherein the storage device stores program instructions; and

a processor connected to the bus system, wherein the processor executes the program instructions to:

measure system resources utilized by each application running in a plurality of host computers of a data processing environment;

determine which applications running in the plurality of host computers utilize similar system resources; and

collocate those applications utilizing similar system resources on respective host computers, wherein the collocate comprises:

determine a greatest amount of attack surface reduction in each respective host computer based on placement of a particular set of applications having a similar system resource utilization footprint on a particular host computer and removal of a determined set of unused system resources corresponding to that particular host computer running that particular set of applications;

assign each respective set of applications having the similar system resource utilization footprint to a specified host computer that has the greatest determined amount of attack surface reduction; and

place each respective set of applications having the similar system resource utilization footprint on its assigned host computer in the data processing environment.

14. The computer system of claim 13, wherein the processor further executes the program instructions to:

determine unused system resources not used by resident applications running on a set of host computers in the plurality of host computers; and

remove the unused system resources corresponding to each respective host computer in the set of host computers to reduce the attack surface in the data processing environment, wherein the determine the unused system resources not used by the resident applications comprises:

obtain a list of system resources corresponding to each respective host computer in the plurality of host computers;

identify a set of used system resources in the list of system resources corresponding to each respective host computer being utilized by a running resident application; and

determine a set of unused system resources corresponding to each respective host computer by subtracting the set of used system resources from the list of system resources corresponding to each respective host computer.

15. The computer system of claim 13, wherein the processor further executes the program instructions to:

perform a boot strap operation on the plurality of host computers in the data processing environment;

profile the applications running on the plurality of host computers to obtain a system resource utilization footprint of each respective application, wherein a system resource utilization footprint identifies a pattern of system resource usage by a particular application running on a host computer; and

identify a plurality of different sets of applications having similar system resource utilization footprints based on the profiling of the applications.

16. The computer system of claim 13, wherein the collocate comprises placing the those applications utilizing similar system resources together on a same host computer.

17. A computer program product for reducing attack surface by selectively collocating applications on host computers, the computer program product comprising a computer readable storage medium having program instructions embodied therewith, the program instructions executable by a computer to cause the computer to perform a method comprising:

measuring system resources utilized by each application running in a plurality of host computers of a data processing environment;

determining which applications running in the plurality of host computers utilize similar system resources; and

collocating those applications utilizing similar system resources on respective host computers, wherein the collocating comprises:

determining a greatest amount of attack surface reduction in each respective host computer based on placement of a particular set of applications having a similar system resource

utilization footprint on a particular host computer and removal of a determined set of unused system resources corresponding to that particular host computer running that particular set of applications;

assigning each respective set of applications having the similar system resource utilization footprint to a specified host computer that has the greatest determined amount of attack surface reduction; and

placing each respective set of applications having the similar system resource utilization footprint on its assigned host computer in the data processing environment.

18. The computer program product of claim 17 further comprising:

determining unused system resources not used by resident applications running on a set of host computers in the plurality of host computers; and

removing the unused system resources corresponding to each respective host computer in the set of host computers to reduce the attack surface in the data processing environment, wherein the determining the unused system resources not used by the resident applications comprises:

obtaining a list of system resources corresponding to each respective host computer in the plurality of host computers;

identifying a set of used system resources in the list of system resources corresponding to each respective host computer being utilized by a running resident application; and

determining a set of unused system resources corresponding to each respective host computer by subtracting the set of used system resources from the list of system resources corresponding to each respective host computer.

19. The computer program product of claim 17 further comprising:

performing a boot strap operation on the plurality of host computers in the data processing environment;

profiling the applications running on the plurality of host computers to obtain a system resource utilization footprint of each respective application, wherein a system resource utilization footprint identifies a pattern of system resource usage by a particular application running on a host computer; and

identifying a plurality of different sets of applications having similar system resource utilization footprints based on the profiling of the applications.

20. The computer program product of claim 17 wherein the collocating comprises placing the those applications utilizing similar system resources together on a same host computer.

21. The computer program product of claim 17 further comprising:

placing a new application on a server;

profiling the new application to determine a system resource utilization footprint of the new application;

obtaining system resource availability of each respective host computer in the plurality of host computers;

identifying any host computer that has available system resources to run the new application based on the system resource utilization footprint of the new application; and

determining whether any host computers have available system resources to run the new application.

22. The computer program product of claim 21 further comprising:

responsive to determining that no host computer in the plurality of host computers has available system resources to run the new application, selecting a host computer in the plurality of host computers that has a fewest number of running resident applications;

migrating resident applications from the selected host computer to the server;

resetting the selected host computer to an initial default state to form a reset host computer;

migrating previously migrated applications from the selected host computer back to the reset host computer from the server;

placing the new application on the reset host computer; and

removing system resources not utilized by running resident applications on the reset host computer to decrease an attack surface on the reset host computer.