

Access Control In Virtual Environments

A FoxT White Paper

Rapid growth in the use of virtualization tools means system administrators are now able to isolate processes in exclusive run-time environments. While helping reduce issues stemming from program conflicts, software compatibility, and security concerns... this trend is also multiplying access control and user provisioning problems in the data center. Without centralized identity management and access control, the productivity gains made through virtualization are easily reverted.

The growth in use of virtual servers is heralded by many as a positive development because it is seen to save companies money and resources. A global survey of 1,221 enterprises by Forrester Research found that 33 percent were using virtualization, and 13 percent planned to implement pilot programs within the year. The highest adoption rate was in North America, with 41 percent of enterprises already implementing or planning pilot server virtualization programs. In another key finding, 60% of those using virtualization said they plan to increase use of the technology in the next 12 months.

Gartner has predicted that more than 40% of new operating systems will be deployed on virtual machines by 2009, and this figure may prove to be conservative. The widespread use of virtualization technologies is predicted to expand from the server space to include desktops, thin clients and mobile devices.

Virtualization is also becoming a key aspect in both software and hardware design. Chip manufacturers Intel and AMD are developing CPU extensions designed to simplify the creation of virtual machines, while VMWare, Microsoft, IBM and HP are among the major vendors currently developing their offering in the server virtualization space.

The benefits of server virtualization include:

- Cost reduction through hardware consolidation
- Cost reduction through savings in power, space, cooling
- Cost reduction through reduction in admin staff – less physical machines to look after
- Tailor provisioning of processing power to the applications that need it, when they need it

- Optimize storage resources for data retention and archiving
- Segregate applications without needing to invest in more hardware
- Business agility – can grow/shrink virtual machines, move virtual machines
- Disaster recovery

Tools such as VMotion from VMWare even enable organizations to move a running virtual machine from one physical server to another without any disruption to operations. The business agility benefits of such capabilities are obvious – but they do not come without management challenges.

Virtualization offers great opportunities for consolidation, but also requires a paradigm shift in how enterprises manage their server infrastructure. And with IDC predicting that the number of installed servers worldwide will hit 45 million by 2010, enterprises are having to work fast to find a way of addressing the new virtual server world.

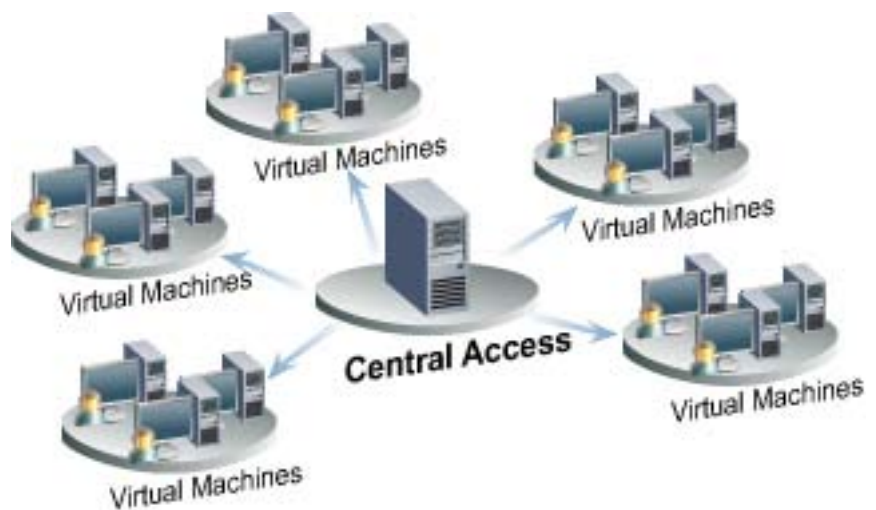
As it is easier to create a virtual machine than to set up a physical machine in the enterprise, machines can be set up very quickly, and brought online and offline as required. However, this ease of creating servers can lead to a proliferation of virtual machines in the enterprise and compound access control challenges. In fact, organizations experiencing this well-known ‘virtual machine (VM) sprawl’ phenomenon are validating that user provisioning and access control challenges are made even harder in the post-virtualization enterprise. Organizations battling “VM sprawl” are concerned about a lack of structured controls over user accounts that are harbored on these virtual machines.

Organizations are fast learning that while less hardware is positive from some points of view, that the core tasks of user provisioning and access control remain whether servers are real or virtual. How do you control exploding populations of user identities on virtual machines in your network when you have performance SLAs, security policies, compliance regulations, and IT auditing requirements to worry about?

Recognizing the challenges of virtualization, FoxT is committed to extending the access control management and auditing benefits provided by BoKS Access Control for Servers to work on virtual platforms. FoxT has recently introduced support for VMWare ESX server, IBM virtual I/O server, and zLinux running on IBM z-Series mainframes. This enables organizations using BoKS Access Control for Servers to extend the management facilities BoKS offers to their virtual servers:

- Centrally manage user populations on virtual servers from the BoKS Manager administration console

- Automatically provision users to virtual machines by adding the machines to managed host groups
- For virtual machines used sporadically, dynamically register and de-register the hosts in BoKS and automate updating of user password updates
- Enforce common access and authentication policies for virtual and non-virtual servers alike
- Centrally scan virtual machines for vulnerabilities with BoKS integrity checking
- Centrally monitor configurable files across the network for changes, including files residing on virtual machines
- Centrally log user access to virtual machines



FoxT brings clarity to your virtual domain, where access controls, identity management and user provisioning can be centrally managed on virtual machines. With the FoxT solution, hosts can be dynamically added to and removed from managed host groups to create a sustainable identity management and access control environment that spans virtual and non-virtual machines.

This enables organizations to maintain control over their user populations while taking advantage of the many business benefits of server virtualization.



FoxT
883 North Shoreline Blvd.
Building D, Suite 210
Mountain View, California 94303
www.foxt.com
650.687.6300

Copyright © FoxT. All rights reserved.
The document is provided for informational purposes only and the contents herein are subject to change without notice. This document is not warranted to be error-free, nor subject to any other warranties or conditions, whether expressed orally or implied in law, including implied warranties and conditions of merchantability or fitness for a particular purpose. We specifically disclaim any liability with respect to this document and no contractual obligations are formed either directly or indirectly by this document. The document may not be reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, without our prior permission.

FoxT logo is a trademark of FoxT, Inc. Other product and company names herein may be registered trademarks and trademarks of their respective owners.