IBM PowerSC Technical Overview

IBM Redbooks Solution Guide

Security control and compliance are some of the key components that are needed to defend the virtualized data center and cloud infrastructure against ever evolving new threats. Security control and compliance are also becoming more vital to many organizations that must adhere to regulatory requirements that safeguard personal data and enterprise information from security attacks.

In addition, security guidelines are implemented to address security exposures to virtual machines (VM) in the data center, for example, are the VMs directly facing an Internet connection or are they running a back-office database? Based on the various levels of vulnerabilities, regulatory compliance requirements group the virtual machines into separate entities, called security zones.

But today, where IT technologies, like cloud computing, allow dynamic live relocations of virtual machines on physical machines, the physical security zone boundaries tend to blur. Many organizations struggle to ensure that their security zones are isolated always, and that their security policies are enforced. As security zones are implemented by network segregation, as shown in Figure 1, IBM® PowerSC™ Trusted Surveyor can monitor network configuration drift and report on the network compliance posture for all the virtual machines in the data center.

IBM PowerSC Trusted Surveyor can provide an independent audit and governance of the virtualized network infrastructure, which helps ensure consistent and controlled configuration change management. The information that Trusted Surveyor provides can lower administration costs by automating the network compliance monitoring for the virtualized data center.

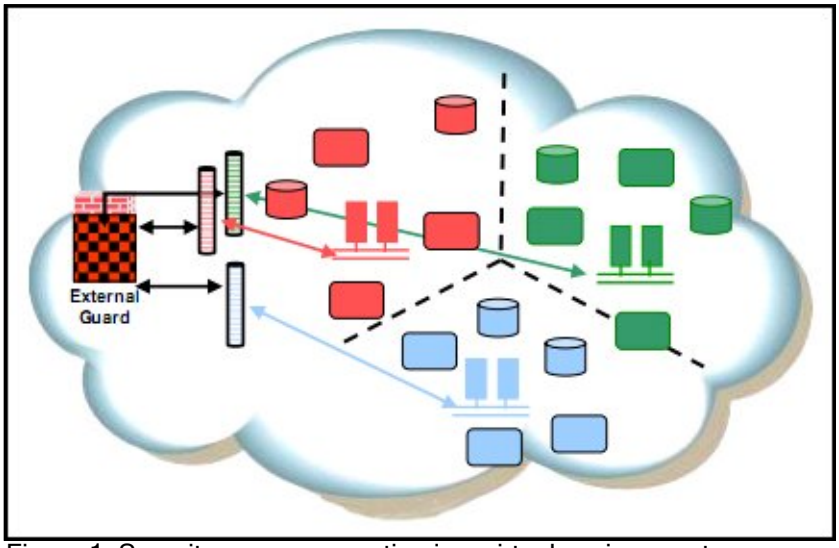

Figure 1. Security zone segregation in a virtual environment

Did you know?

The Center for the Protection of National Infrastructure (CPNI) recommends Network Boundary Defense Control and Secure Network Engineering Control within its top critical controls for effective cyber defense.

The Payment Card Industry requires that Cardholder Data Environment (CDE) virtual machines be separated from non-CDE virtual machines. PCI DSS requirement 2.4 allows shared hosting providers to host multiple customer environments on a single server while requiring that "... shared hosting providers must protect each entity's hosted environment and cardholder data" (Source: https://www.pcisecuritystandards.org/security_standards/). However, PCI DSS requires that appropriate controls must be in place to prevent one virtual system from increasing the risk to cardholder data on another virtual system to mitigate the specific risks that come with shared hosting. The Cardholder Data Environment (CDE) and its inherent network segregation must be maintained and monitored always in order to be enforced in the data center.

The National Institute of Standards and Technology (NIST) defines, in their document *NISTIR 7628 Guidelines for Smart Grid Cyber Security v1.0 – Aug 2010*, inadequate Network Segregation as one of the six biggest vulnerabilities. The NIST defines that "Network architectures often do a poor job of defining security zones and controlling traffic between security zones, thus providing what is considered a flat network wherein traffic from any portion of the network is allowed to communicate with any other portion of the network" and give the two following examples: *Failure to define security zones*, and *failure to control traffic between security zones* (Source: http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf). It is highly recommended to employ a “zoning model” to differentiate and segregate servers from business to operational ones according to system and data content and associated risk.

Business value and solution overview

IBM PowerSC Trusted Surveyor is a stand-alone offering in the PowerSC family that provides a consolidated view of the virtual data center's virtual machine network isolation landscape. It extracts configuration data from multiple virtualized environments, and transforms the data into a normalized graph representation for subsequent analysis of its security properties.

A report is created by securely probing all of the Hardware Management Consoles (HMCs) in the virtual data center. The results are displayed in a web browser, but also can be saved externally so that this data can be used by other tools, such as Microsoft Excel. Trusted Surveyor takes snapshots of a virtual data center either on demand or at predetermined intervals. Snapshots are used to validate LPAR isolation by VLAN IDs and physical systems so that you can verify and monitor configuration changes in the virtual data center.

Trusted Surveyor is implemented as a stand-alone web server-based product that is installed on a single server. The information is gathered through interrogating the HMC. Trusted Surveyor normalizes the configuration data of each virtual system and presents an overall view of the data center’s security isolation and interconnects. The report Trusted Surveyor generates displays VM groups and highlights group interconnects that violate security policy. Policy enforcement is based on a static (built-in) set of rules that are provided with the tool. Parameterized data that is provided by the user completes the static rule set.

Business and compliance security requirements are described by the IT security department in the form of written security policy and guidelines. The administrators read these policies and manually configure their OS, virtual system, or network accordingly. For example, the Payment Card Industry (PCI) Data Security Standard mandates that all IT systems that process credit card Primary Account Numbers (PANs) are isolated and protected. These IT systems must be on a separate network or VLAN. This requirement must be described in the IT security department’s written policy. If there are three PCI LPARs that are dedicated to credit card processing, they must be on their own VLAN. It is difficult to know whether another LPAR on a separate physical system, under a different HMC and administered by a different virtual administrator, is configured incorrectly to be on the same VLAN as the PCI LPARs.

Trusted Surveyor brings the entire Power based virtual data center configuration into a single automated view with a Microsoft Excel report that shows every LPAR and VLAN. It can take a snapshot of the virtual data center VLAN interconnect, establish a baseline policy, and highlight any change or incorrect configuration that violates the policy and poses a security risk.

Solution architecture

Trusted Surveyor is installed and configured on a server that runs the IBM AIX® operating system. A report is generated when a probe connects to an HMC to query and identify the systems and their virtual configurations that are managed by that HMC. All defined and enabled probes for the current domain are run when a snapshot acquisition is triggered for that domain. All of the available report options are based on the snapshots that are available for an identified domain. The resulting report identifies all of the LPARs, their associated physical systems, the VLANs to which they are connected, and the isolation zones that are created by these VLANs. Isolation zones are the separation of the resources that are created to control access to resources.

These reports are used to ensure that the current configuration meets the requirements for the isolation and protection of LPAR groups. When the initial compliance requirements are established, the reports and the snapshot can be used to provide an approved version or gold master compliance policy. By setting up regularly scheduled probes, snapshots can be created for additional reports. The approved snapshot can be compared to the current snapshot to identify changes that might cause noncompliant situations by highlighting the differences between the snapshots. The dynamic nature of cloud and virtual environments makes this type of change control and monitoring necessary.

Most resources that are used in Trusted Surveyor are given a name for identification when you use the command line. In some cases, you can use the commands to provide your own name for the resources.

Before we explain these concepts in more detail, see Figure 2 for an overview.

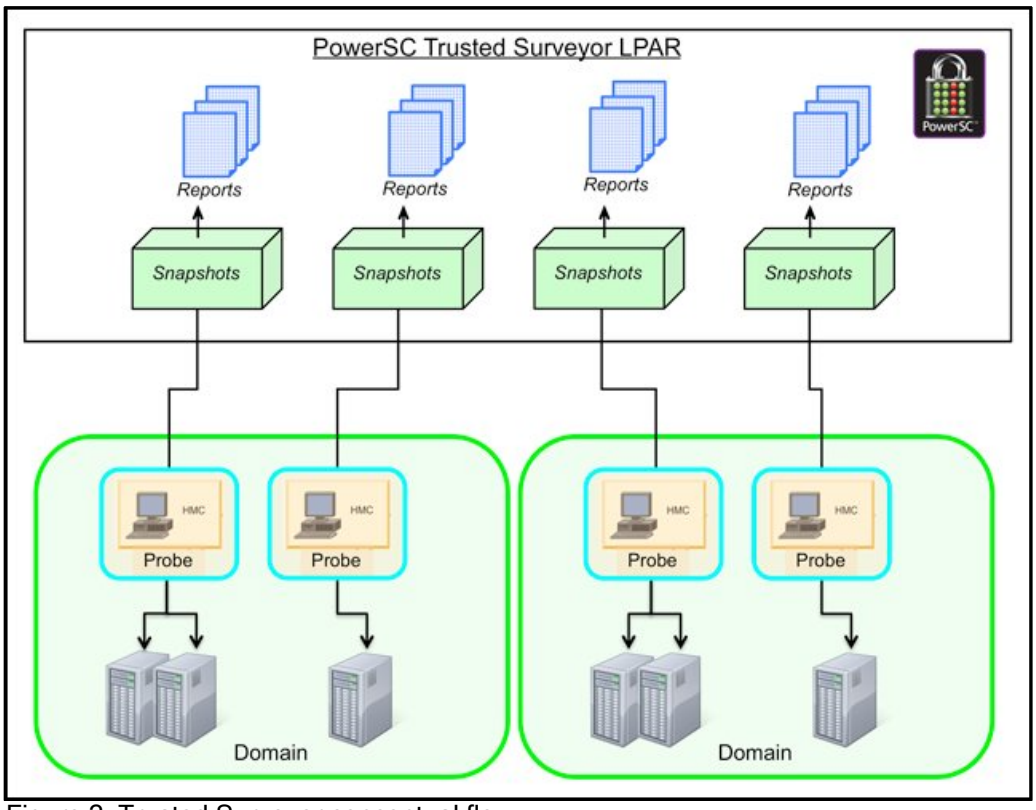

Figure 2. Trusted Surveyor conceptual flow

Domains
Domains represent the main environment in which you work when you use Trusted Surveyor. Some configurations are simple enough to require only a single domain, which is created when you install Trusted Surveyor. It is not necessary to create additional domains.

More complex configurations might benefit from the creation of additional domains. Data center resources can be grouped into domains. Because you can access only one domain at a time, it is helpful to group similar resources together.

Probes
Trusted Surveyor uses probes to query information from a virtual management console, such as an HMC. Probes gather information about the configuration of the data center or the cloud. Then, this information is filtered and consolidated into a snapshot that represents the configuration.

Snapshots
Snapshots are representations of the environment that are created by consolidating the information that is captured by the probe acquisitions. Snapshots can be used to provide a detailed representation of a data center. Two snapshots can also be used to see how the environment changed in the time between the creation of the two snapshots.

When you work with snapshots, a snapID variable is used to identify a specific snapshot. The snapID can be either the name that is assigned to the snapshot with the command-line interface (CLI) or the graphical interface, or the unique integer name that is provided by Trusted Surveyor in the format of snapshot-ID.

Basic components
The following basic components are required for Trusted Surveyor:

- Web server

  The Trusted Surveyor software is installed on an AIX LPAR. This LPAR must be a dedicated web server for Trusted Surveyor. The web server uses a Secure Shell (SSH) network connection to communicate with the virtual management console.

- Web browser

  The web browser uses a secure Hypertext Transfer Protocol Secure (HTTPS) connection to connect to the Trusted Surveyor web server. The following browsers are supported:

  - Mozilla Firefox version 14 or later
  - Microsoft Internet Explorer versions 8 and 9 (running in Standard mode)

- Virtual management console

  The virtual management console or HMC provides the data that the Trusted Surveyor uses to create the security and isolation reports. During probe configuration, Trusted Surveyor creates a secure read-only account on the virtual management console, which it uses to access the data.

System requirements
An LPAR, dedicated to Trusted Surveyor only, must be created with an AIX operating system that contains adequate resources. The amount of memory and storage that is associated with this LPAR is determined by the amount of snapshot data to be kept and the speed of processing that is expected from Trusted Surveyor. Generally, Trusted Surveyor requires little storage, little memory, and few processing cycles.

This LPAR requires network connectivity for the SSH protocol to the virtual management consoles and HTTPS connectivity to a browser for the Trusted Surveyor users.

The following software must be installed on the Trusted Surveyor LPAR before you install Trusted Surveyor:

- IBM AIX V7 with Technology Level 2 or later or IBM AIX V6 with Technology Level 8 or later
- OpenSSH Version 5.8
- Java SE 6

Usage scenarios

The Trusted Surveyor solution is often implemented when the complexity and cost to monitor and maintain the inventories of all servers' VLANs and servers' virtual machines become fastidious, time-consuming, and prone to errors.

Additionally, Trusted Surveyor can create reports of your data center for regulatory compliance auditors and security officers automatically in either text or CSV format. Auditing a virtualized data center has never been easier and more reliable, as Trusted Surveyor can automate the reports and track any change for you. Here are some example scenarios:

- Scenario 1 – Payment Card Industry Cardholder Data Environment
  An organization can check and monitor in real time that the PCI in-scope virtual machines are still defined on the correct VLANs, no additional VLANs have been added or deleted, and the server locations are correct. The network segregation can be demonstrated and compliance enforced, as any change to the base policy is detected by Trusted Surveyor.

- Scenario 2 – Data center configuration monitoring
  An organization can check and monitor in real time which LPARs or virtual machines have been added, deleted, or relocated, and on which physical servers within the data center they are deployed. Trusted Surveyor can automatically compare any change within the network and server policies for several HMCs and hundreds of virtual machines in a few minutes. Data center configuration can be monitored and audited automatically.

Supported platforms

Trusted Surveyor must be licensed for all HMCs that are monitored. The Trusted Surveyor is licensed by managed Hardware Management Console (HMC). Trusted Surveyor requires a dedicated AIX LPAR that runs the Trusted Surveyor web application, which discovers and monitors the virtualized infrastructure. Typically, a customer needs only one instance of this application per enterprise.

Trusted Surveyor offering (5765-PSE) supports the following items:

- IBM systems that run the IBM POWER6® and POWER7® processors
- IBM AIX V7 with Technology Level 2 or later or IBM AIX V6 with Technology Level 8 or later
- OpenSSH Version 5.8
- Java SE 6
- HMC 7042-CR6 and 7042-CR7 only and later

Ordering information

Machine-readable materials are only available on CD-ROM. To receive a shipment of machine-readable materials, your order needs to include SPO 5692-A6P. Ordering information is shown in Table 1.

Table 1. Ordering part numbers and feature codes

Program name	PID number	Charge unit description
IBM PowerSC Trusted Surveyor	5765-PTS	Per HMC
SW Maintenance Registration/Renewal 1 Year	5660-PTS	Per HMC
SW Maintenance After License 1 Year	5661-PTS	Per HMC
SW Maintenance Registration 3 Year	5662-PTS	Per HMC
SW Maintenance After License 3 Year	5664-PTS	Per HMC
IBM PowerSC Trusted Surveyor DVD	5692-A6P	Feature 3345-1100 or 3345 -1101

Related information

For more information, see the following documents:

- IBM Redbooks® publication *Managing Security and Compliance in Cloud or Virtualized Data Centers Using IBM PowerSC*, SG24-8082:
  http://www.redbooks.ibm.com/abstracts/sg248082.html
- The PowerSC website:
  http://www.ibm.com/systems/power/software/security/index.html
- IBM Offering Information page (announcement letters and sales manuals):
  http://www.ibm.com/common/ssi/index.wss?request_locale=en

  On this page, enter IBM PowerSC, select the information type, and then click **Search**. On the next page, narrow your search results by geography and language.

Notices

This information was developed for products and services offered in the U.S.A.

IBM may not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service. IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing, IBM Corporation, North Castle Drive, Armonk, NY 10504-1785 U.S.A.

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you. This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you. Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products. This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs.

This document was created or updated on May 8, 2013.

Send us your comments in one of the following ways:

- Use the online **Contact us** review form found at:
  ibm.com/redbooks
- Send your comments in an e-mail to:
  redbook@us.ibm.com
- Mail your comments to:
  IBM Corporation, International Technical Support Organization
  Dept. HYTD Mail Station P099
  2455 South Road
  Poughkeepsie, NY 12601-5400 U.S.A.

This document is available online at http://www.ibm.com/redbooks/abstracts/tips0980.html .

Trademarks