close window

Web Exclusive

Print

Security and PowerSC Trusted Surveyor

March 2015 | by Jaqui Lynch

Anyone reading the news today is aware that server and network security has become more important than ever. As companies bring in more Power Systems servers connected through hardware management consoles (HMCs), it's critical to be able to have visibility into the virtual networks in use. That's the purpose behind PowerSC Trusted Surveyor, which was introduced in October 2012.

PowerSC Trusted Surveyor queries all the HMCs for VLAN and LPAR configuration information and creates snapshots of the current configuration. This can be used not only for documentation purposes but also for highlighting changes between snapshots.

The Challenge

Technologies such as cloud computing and live partition mobility allow for live (or even inactive) migrations of LPARs to separate physical machines. This provides a challenge with respect to ensuring that security zones are still isolated. Additionally security policies need to be enforced. The challenge isn't just ensuring that LPARs are in the correct network zone but that you can prove it—auditors want to know which network zones (test, prod, etc.) LPARs are in and whether they're internal only or open to the outside. It's very easy to end up in the wrong VLAN with complex networking.

Additionally, there are regulations requiring the separation of cardholder data environment (CDE) virtual machines from non-CDE virtual machines

The first recommendation is to always try to keep things simple. Just because you can have a multitude of VLANs doesn't mean you should. Use additional VLANs and networks where they're needed to ensure compliance and isolation, remembering that the more VLANs you add, the more complex the environment becomes and the more likely you are to get network configuration drift, especially during migrations.

How Does Trusted Surveyor Help?

PowerSC Trusted Surveyor provides a consolidated view of the virtual machine (LPAR) network isolation landscape. It securely queries all of the HMCs in the environment and then produces reports that can be viewed in a Web browser or downloaded in Excel format. Trusted Surveyor can be set up to take snapshots on demand or at set times. These snapshots can be used to look at current LPAR isolation via VLAN IDs and can also be used to monitor configuration changes. The monitoring can be used to verify changes went in as well as to confirm they didn't lead to any network isolation breakdowns. Because Trusted Surveyor queries all the HMCs, it can be used to ensure VLANs that are supposed to be isolated for CDE data aren't accidentally used on servers controlled by other HMCs where different administrators may be involved.

Trusted Surveyor runs in an AIX LPAR and is configured to query the HMCs that it can access. A report is generated when a probe connects to an HMC to query and identify the systems and the virtual configurations managed by that HMC. The report produced identifies all of the LPARs, the servers, VLANs that LPARs are connected to and the isolation zones for those VLANs. If HMCs are on completely separate physical networks then it may be necessary to install Trusted Surveyor on an LPAR in each network. A license is required for each HMC that Trusted Surveyor will be monitoring. Other requirements include POWER6 or higher, AIX v6.1 tl8 or AIX v7 tl2 or higher, OpenSSH 5.8 and Java SE 6. HMCs must be 7042-CR6 or higher. Trusted Surveyor can handle AIX, Linux and IBM i virtual machines.

The Trusted Surveyor LPAR must be dedicated to Trusted Surveyor. It requires at least OpenSSH 5.8 as SSH is used to communicate with the HMC. Thus the HMC must be enabled for SSH access. On demand or at select intervals Trusted Surveyor will probe the HMC for information on everything it sees, using a secure read-only account on the HMC that's created by Trusted Surveyor during probe configuration.

Trusted Surveyor comes with pre-built profiles that provide security and compliance automation. At initial setup compliance requirements are established, the resulting reports and snapshots can then be used to check for compliance to security policies.

When working with Trusted Surveyor, it's important to understand three key concepts—domains, probes and snapshots. Domains are the group of resources that an iteration of Trusted Surveyor monitors. Only one domain can be accessed at a time so it makes sense to group similar resources together. Probes are used to acquire data from the HMCs. There's at least one probe per HMC and they access the HMC in read-only mode via SSH. Probes can be created and run on demand, run at fixed intervals or left disabled so they can be used later. Snapshots are the output from a probe. They are moment-in-time detailed representations of what the HMC sees. Two snapshots can be compared to check for changes in the configuration, which provides useful auditing information. The 20 most recent snapshots are retained, although it's possible to make a particular snapshot persistent if so required.

Installation of Trusted Surveyor is simple. You install one fileset (powersc.ts) plus any updates to it. This creates a userid called tsadmin and a group called ts. The installation also registers the Trusted Surveyor server with the system resource controller in the AIX LPAR so it will start at boot time. Additionally role-based access control is used to create two roles—ts.admin and ts.monitor. ts.admin provides full control of Trusted Surveyor whereas ts.monitor is used to generate reports. These roles can be provided to an individual userid as needed. A userid must be created with the ts.admin role to configure Trusted Surveyor. This can be done using a command similar to:

```
mkuser default_roles=ts.admin roles=ts.admin username
```

Once configured, define a domain and create a probe, by connecting to Trusted Surveyor using https to the LPAR. An initial domain is defined for you so it may not be necessary to add any. Next a probe is defined so that Trusted Surveyor can set up the connection to the HMC to acquire information and create snapshots. Chapter 9 of the Cloud PowerSC Redbook (SC24-8082) provides extensive information on configuring Trusted Surveyor along with setting up secure keys between Trusted Surveyor and the HMC. Typically the Web browser is used for all configuration and deployment activity, however CLI commands are also available, which allows for scripting.

A Useful Tool

PowerSC Trusted Surveyor is another great addition to your security toolbox. It's a standalone tool that documents and monitors the compliance of virtual networks to network isolation policies, providing an overall view of the virtual network from the HMCs, servers and LPARs. This can be used to ensure that LPARs are properly isolated within the infrastructure. For those who have business and audit requirements around isolation of LPARs across networks, Trusted Surveyor is a very useful tool to monitor compliance and to document the network setup and isolation for the auditors.

IBM Systems Magazine is a trademark of International Business Machines Corporation. The editorial content of IBM Systems Magazine is placed on this website by MSP TechMedia under license from International Business Machines Corporation.

©2019 MSP Communications, Inc. All rights reserved.

IBM Systems Magazine - Security and PowerSC Trusted Surveyor http://ibmsystemsmag.com/ibmi/administrator/security/security-trusted-s...

RESOURCES VIDEO SOLUTIONS EDITION BLOGS WEBINARS SUBSCRIBE ABOUT US

Systems

Connect With Us:

Magazine Archives

AIX LINUX ON POWER MAINFRAME POWER

Search

IBM i ADMINISTRATOR DEVELOPER TRENDS TIPS & TECHNIQUES CASE STUDIES STORAGE PRODUCT NEWS ENDPGM

References

< Return to main article

ADVERTISEMENT

POWER SYSTEMS EXTRA

Maximize your IT investment with weekly information from THE source… Power Systems EXTRA eNewsletter.

SIGN UP TODAY

Read Previous Issues

Print Email

For more information on PowerSC Trusted Surveyor, check out the following reading materials:

Regulations on Separating Data

https://www.pcisecuritystandards.org/security_standards/ http://csrc.nist.gov/publications/nistir/ir7628/nistir-7628_vol3.pdf

Managing Security and Compliance in Cloud or Virtualized Data Centers using IBM PowerSC (2013)

Cloud Security Guidelines for IBM Power Systems (2015)

IBM PowerSC Website

PowerSC Technical Overview

2014 PowerSC Trusted Surveyor 1.1 Announcement Letter

< Return to main article

IBM Systems Magazine is a trademark of International Business Machines Corporation. The editorial content of IBM Systems Magazine is placed on this website by MSP TechMedia under license from International Business Machines Corporation.

©2019 MSP Communications, Inc. All rights reserved