Protect Your SAP HANA Environment

Q&A with **Jason Delaune**, SAP Solution Lead at Hitachi, and **José Betancourt**, Senior Architect at SUSE

Cybersecurity is a topic that's at the forefront of every business these days. Companies want to know how to keep their infrastructures secure — especially SAP customers, as they begin to move to new technologies like SAP HANA. During a recent SAPinsider Live Q&A, Jason Delaune, SAP Solution Lead at Hitachi, and José Betancourt, Senior Architect at SUSE, answered questions from attendees regarding encryption, security maintenance, patch updates, and more.

Below is an abridged transcript of the SAPinsider Live Q&A conversation where Jason and José discussed best practices for protecting SAP HANA infrastructures. The full transcript is available on SAPinsider Online at bit.ly/ProtectHANA.

Q: What steps can businesses take to secure their SAP HANA environments?

Jason Delaune (JD): There is a lot of good information in the SAP HANA Security Guide on the initial steps to take when receiving SAP HANA hardware from a vendor. The guide then covers a lot of other areas that security and Basis personnel should review to properly secure the SAP HANA instance. As a first step, I would give that document a look.

Q: What are best practices for SAP HANA database passwords?

JD: I would certainly follow corporate guidelines on password policies — such as minimum number of characters, upper and lower case, number, special characters, and so on. Configuring both the SAP application tier and the SAP HANA tier to adhere to the corporate policy will make life much easier come audit time.

Q: Does SAP HANA support data encryption, and should companies use secure sockets layer (SSL) protocol for SAP HANA connections?

JD: SAP HANA 1.0 supports data volume encryption (I believe as of support package stack [SPS] 08). With SAP HANA 2.0, administrators can now enable redo log encryption. In the event that a network is not protected by firewalls, then I would strongly recommend encrypting SAP HANA connections with SSL. If companies use firewalls to protect their SAP HANA instance (and they are locked down according to SAP's best practices), it's up to them if they want to enable SSL on the SAP HANA connections. It certainly adds another layer of security, and with the increase in malicious users out there coming up with new ways to breach a company's systems, it's better to be safe than sorry.

Q: How can Hitachi support data encryption with SAP HANA?

JD: SAP HANA encryption by itself can protect both the data areas and the redo log areas (if using SAP HANA 2.0); however, database traces and backups are not encrypted on disk (unless you have third-party back-up software that encrypts the backup). So, this can lead to security vulnerabilities if someone were to get access to the server or storage array.

With Hitachi arrays, we offer the ability to encrypt the entire array. Each controller, disk, and back-end director (BED) has a key, so this increases security should one or more of these components find their way into the wrong hands. Also, there's no overhead on the controllers of the array, so performance is comparable to that of an unencrypted array. With SAP HANA encryption, there is a performance penalty with reads/writes while the data is unencrypted/encrypted. However, the data is fully unencrypted in memory, so there's no performance impact during normal in-memory operations.

Q: How does Hitachi architect SAP systems to increase uptime for security maintenance?

JD: We have a number of ways to help businesses achieve uptime depending on their SAP HANA environment. I always recommend that customers have local high availability (HA) using SUSE Linux High Availability Extension with SAP HANA system replication. This way, they can patch one node while the other node is still running the production environment. Then, they can failover to the standby to do the work on the other node, minimizing downtime since everything will be running in a local, synchronized fashion.

I also recommend that customers have a production-like environment for a quality assurance/test system. Testing the failover/maintenance procedures before actually getting to the production maintenance day is a best practice. A cluster adds another layer of complexity to an environment, so testing ahead of time ensures production maintenance goes smoothly for end users. Certainly with SUSE's new feature, SUSE Linux Enterprise Live Patching, this helps administrators with their monthly chores.

Q: What is delivered with service-level expectations for SAP HANA for HA configurations?

José Betancourt (JB): The SUSE Linux Enterprise Server for SAP applications product provides SUSE Linux High Availability Extension as part of the product itself. Equally important is the availability of the SAP HANA resource agents to facilitate the configuration of SAP HANA in an HA scenario. We provide the resource agent to configure three scale-up scenarios (performance, cost, and multi-tier), and the topology resource agent to gather information and status of all the members of the cluster.

Q: Is HA protection provided in an SAP HANA multi-tenant database container scenario?

JB: Yes, HA protection is available with a multi-tenant database container scenario. It can handle performance or cost-optimized failover scenarios. The way it works is via a takeover of the parent SAP HANA database. Another item to take into account is that all tenant database containers and associated services are impacted by the takeover/migration.

Q: Are live patches applicable to in-memory as well as to disk?

JB: When using SUSE Linux Enterprise Live Patching, companies have the option of applying the live patch to just memory (in which case the system will have to be patched again after reboot), or to both memory and disk. It really depends on how they want to apply the live patch.

Q: How far back in time are live patches available for the current kernel?

JB: Businesses can keep a system without reboot when using SUSE Linux Enterprise Live Patching for up to one year. For kernels older than one year, no live patches will be made available. There is an FAQ section for live patching on the SUSE website that covers this and other interesting questions.

Q: How often should companies patch their firmware?

JD: Firmware would normally be patched once or twice a year unless there is a critical security vulnerability that a hardware vendor has sent an alert about. As a best practice, I would do them in their own maintenance window instead of trying to combine with other maintenance activities. This way, if something goes wrong, it's easier to pinpoint the problem.

Q: What tools do you recommend for monitoring security best practices for SAP HANA?

JD: SAP's EarlyWatch Alert service helps detect when systems aren't adhering to SAP best practices (in the Security sub-heading), and SAP Solution Manager helps detect missing SAP Security Notes (released the second Tuesday of each month). SAP HANA cockpit, which has an SAP Fiori feel to it, has a Security section that displays a lot of good info about SAP best practices for securing SAP HANA. The cockpit also has links to the SAP Security Guide in case you need to dig into a particular area. There are probably a number of third-party tools that can also provide recommendations or best practices, but the ones I mentioned are included with existing SAP deployments — so they are free. ■

Jason Delaune is SAP Solution Lead – Americas Solutions & Products Group at Hitachi. In his current role, he is responsible for helping customers with their digital transformation journey from classic SAP systems based on traditional RDBMS platforms to those based on SAP HANA. You can reach him at jason.delaune@hds.com.

José Betancourt is a Senior Architect at SUSE where he works with global OEM partners to understand their business and technical requirements and make them successful with SUSE. His focus area is SUSE Linux Enterprise for SAP applications and SUSE Linux Enterprise Live Patching. You can reach him at jose.betancourt@suse.com.