Q&A Session for Power Systems VUG 2022-2-24 - PowerSC

Session number: 1452503536
Date: Thursday, February 24, 2022
Starting time: 9:41 AM

Q: Is MFA a separate license or has to be licensed on top of Standard Edition?

The MFA licensing is under PowerSC 2.0. Everything is now under PowerSC 2.0. If you want to use MFA, get the PowerSC 2.0 licensing. You can get PowerSC 2.0 under "standalone" or some of the other Power Licensing bundles, like AIX Enterprise Edition, Enterprise Cloud Edition with AIX or Enterprise Cloud Edition.

Q: PowerSC MFA includes all functions of standard edition also?

PowerSC Standard Edition and PowerSC MFA are now both bundled together under PowerSC 2.0. PowerSC 2.0 provides all PowerSC functionality.

Q: Are the new scanning components only on RHEL?

There is a new Port Scan attack detector that is only for RHEL 8.3 and above. This was made available starting in PowerSC 2.0.0.0, release Sept 2021.

Q: Is there no support for Ubuntu Linux?

Correct. There is no support for Ubuntu with PowerSC.

Q: Is PowerVC on the endpoints...1 per server? and also is that "agent" in a unique partition?

In order to leverage the centralized GUI management, you install the PowerSC GUI Server on one VM, and you install one PowerSC UI Agent on each VM you want to manage with PowerSC. So it is one agent per managed partition. A certificate corresponding to the hostname of each agent is installed on each managed endpoint so the PowerSC GUI Server and PowerSC GUI Agent can communicate with each other. A PowerSC GUI server can manage agents that are installed on multiple separate physical servers.

Q: Does the PowerSC RHEL agent work just for RHEL on Power, or does it also work for RHEL on x86_64 architecture?

Currently there is no support for PowerSC on intel. That MAY possibly change soon, i.e., possibly this year or next year. But there is nothing officially announced.

Q: Is there any plan to patch RHEL/SLES end-point in future using PowerSC?

There is no native patching solution provided by PowerSC for RHEL and SLES. You must use configure yum or zypper to patch those distros. Once yum and zypper is configured, PowerSC can run a generic check or update operation using those underlying native tools. I highly doubt PowerSC would develop a replacement for yum or zypper, since they are so ubiquitous to those distros.

Q: is an endpoint a partiton or a server?

An endpoint is a partition.

Q: Should be PowerSC server be standalone? Is is ok to run it on a NIM server? Environment is 5 frames and 80 LPARs.

You can run the PowerSC Server on a NIM Server. However, It is better to not run multiple application servers on the same VM for security reasons. This is a general virtualization security best practice. The reason why you don't want to run multiple application servers on the same VM is because a hacker obtaining privileged access to a partition that is running multiple application servers can easily attack the multiple applications servers running on the same host.

Q: Can the PowerSC GUI Server and the PowerSC TNC Server run on the same LPAR or do they need to run on separate LPARs? What size LPAR(s) are needed?

Yes the GUI Server and the TNC Server can run on the same partition. However for security reasons, it is better to run them on separate partitions.
Main Memory: 4-8 GB depending on number of NIM and TNC clients.
Disk: 20GB - 120GB, depending on number of Service Packs you have to support
CPU: one virtual cpu at .5 entitlement using SMT 8 (minimum)

Q: We had a problem "simulate" already changed settings/files. Known Issue?

The simulate should not change anything on the endpoint you are

simulating against. If it does, open a support ticket for Rocket Software to debug the problem.

Q: Can you create your own profile with your specific rules without make it of a defined template?

Although difficult, It is technically possible to create your own profile and scripting without using the XML files and scripting provided by PowerSC. You can import an xml to PowerSC using the convertProileToBean.sh script. If you need a security hardening setting that is not implemented in PowerSC, you could open a ticket and ask Rocket Software to implement it for you. Other companies may benefit from your recommendation.

Q: When will a DOD xml be available for RHEL8?

I have heard nothing about that. Rocket is very aware of this request. Open a support ticket. Rocket Software will need to answer that.

Q: Will attendees be receiving a copy of this presentation?

-Joe Armstrong (IBM) - 10:45 AM
A: The presentation materials are available on the Power Systems VUG wiki - ibm.biz/powersystemsvug-

---

Q: Had to remove /var/adm from rtcd_policy.conf file due to numerious emails for clock.

You sometimes have to tune the RTC configuration before you get the right level of notifications. In general, it works well, but sometimes it can create a lot of unnecessary messages. For example, if you install a new service pack level and forget to turn OFF the RTCD Daemon. In general, most customers can get to a place where RTC works well for them.

Q: Will reporting be improved?
In general, in my opinion, the reporting is good. If you want something different, open a support ticket to request a new feature. In my experience, Rocket Software has been very responsible and proactive in providing requests from customers.

Q: maybe not only daily to the same recpipinets but also weekly to another group

That is a design request. This is a good feature request. You can open a ticket and request a new feature for what you are indicating. I will also send a note to Rocket Software about this request.

Q: So AIX Enterprise has PoweSC at no additional cost?

-Joe Armstrong (IBM) - 11:18 AM
A: that is correct. It is part of the bundle.-

Q: can PMFA be integrated for application login or is it there only for unix/linux user login?
If your application PAM-enabled then you can specify the PMFA Pam module to be used with your PAM-enabled application. If your application is not PAM-enabled, I believe it is technically possible for an application to be modified to support PowerSC PMFA. You would need to have the source code of the application. If your application is not Pam-based and you have access to change the source code, you can open a support ticket to find out how exactly to modify your application to support PowerSC MFA.

Q: If you update systems and forget to stop RTC/trustchk you may get hundreds of messages per client. Is it possible to hide this events in one step? if you have to do it on a per server base it takes very long.
That is a design request. This is a good feature request. You can open a ticket and request a new feature for what you are indicating. I will also send a note to Rocket Software about this request.

Q: Do you know if/when AIX development will offer a master tsd file list or a method to determine the list? This seems to be a large shortcoming of TE, i.e., not being able to determine what the original ownership/file permissions are/were/should be.

That is a design request. This is a good feature request. You can open a ticket and request a new feature for what you are indicating. I will also send a note to AIX Security Development about this request.

Q: can the pscxpert read and apply the native aixpert xml file?

Yes it should. However, it is better to stick with using XMLs actually developed by Rocket Software. The CIS xmls are a great option for most customers.

Q: TE: if I installed PowerSC on AIX the TE DB was not updated correctly. The files from powersc had different permissions than it added to the DB. Therefore I had to update the DB manually. common issue?

I have seen that issue. Please open a ticket and report it to Rocket Software.

Q: Works with NIM, but does it also support the NIM alt_disk patch?

Yes PowerSC TNC does support alt_disk installations for ifixes, service packs, open source packages and technology levels.

Q: Am I correct in assuming a PowerSC LPAR can (or should) replace my NIM server LPAR?

Possibly, but it depends. TNC only provides for the following:
For AIX endpoints: install ifixes, service packs, open package items or technology levels.
For VIOS endpoints: install ifixes, open package items
PowerSC only uses NIM for the updates indicated above. If you use NIM for other things, then you need to retain your existing NIM server deployment. A NIM server can do numerous other types of functions beyond what is listed above. PowerSC only uses a subset of NIM server functionality to deploy security fixes as described above.
When customers adopt TNC, they typically use PowerSC TNC on top of their existing NIM Server, so there is no loss of function.

Q: When will EDR functionaility be supported on AIX?

It is already active on AIX. Very powerful functionality for AIX is currently available. EDR functionality was release in the PowerSC 2.0.0.0 release, Sept 2021.

Q: can PowerSC protect Linux endpoint running on x86 server?

Currently PowerSC doesn't support intel endpoints. That MAY change in the future. Nothing has officially been announced.

Q: How is EDR data kept up to date?

You have to correctly implement the underlying tools that feed EDR events to the PowerSC GUI. Then you have to decide how to implement the EDR event notifications. Once you configure an EDR scheme for a single partition, you can copy that scheme to any PowerSC group of partitions. After this, you can use the Event Analysis Report tool to drill into the data to identify critical subsets of security events of interest.

Q: If I am on IBM power cloud, do i get Power SC 2.0 free or i need to pay extra $?

You must pay extra to obtain PowerSC licensing on the IBM Cloud.

Q: Is yum not supported on AIX?

-Joe Armstrong (IBM) - 11:22 AM
A: not positive, but I do believe yum is supported on the AIX toolbox.-

---

Q: dnf is provided as part of the aix linux toolbox. So dnf not yum

---

Q: So, if NIM is on a seperate server, does PowerSC control the NIM server when it performs the update downlaods and automation? Or does it use its own nim server? In which case you are basilly running on the same server.

I will provide an example to help you understand the TNC Topology.
Let's say prior to adopting TNC you have an AIX environment that consists of 100 VMs. In that environment you are already using 1 NIM server to manage the remaining 99 AIX VMs. If you wanted to add TNC to that environment what you have then is the following:
1. Take your existing NIM server and simply add the TNC Patch Management component (TNCPM). When you do this you will be setting up a new daemon to communicate with the internet to retrieve ifixes, service packs and open package software. The TNCPM will only update AIX VMs when the TNCS commands it to update an AIX VM. Since the TNCPM is retrieving updates from the internet automatically, it will be the patch repository for all update files.
2. Create a new lpar and run the TNC Server component (TNCS) on it. The TNCS is the command center for TNC. The TNC Admin will login to the TNCS VM and run TNC server commands in order to verify and update partitions. The TNCS will command the TNCPM when updates need to be performed
3. On your existing 99 standard AIX VMS, you will install the TNC Client component (TNCC). The client reports what filesets are installed on the Client to the TNCS.
4. This is Optional, but if you want to perform a subset of critical TNC admin operations via the PowerSC GUI, you should then create a new VM to run the PowerSC GUI Server. If you add the GUI Server, you would then also need to add PowerSC Agents on the 99 AIX endpoint VMs.

NOTE: The TNCPM, TNCS, and PowerSC GUI can all run on the same VM, but it is not good security practice to do that. Please separate them.

Q: In other words, does PowerSC use its own NIM server? or does it use a NIM server that is already in place.?

Typically, customers leverage the NIM servers that are already in place and add the TNCPM component to the same VM running the existing NIM Server. However, for an existing NIM server to become a TNC patch management server, it will need to have either firewall exceptions to retrieve updates from the internet, or it will need to use a HTTPS proxy to retrieve updates.
It is technically possible to have one general NIM server that is not

enabled for TNC and then have a different NIM Server that is TNC enabled that handles security updates. However, in this case you would have to reconfigure the NIM clients to be able to retrieve the TNC updates from the NIM server that has the TNC Patch Management component configured. A case can be made for this complicated method but it's probably not the best option for most customers.

Q: Need 'Run Script" to be automatic, not manual

This is probably in respect to TNC configuration. This is a design request. This is a good feature request. You can open a ticket and request a new feature for what you are indicating. I will also send a note to Rocket Software about this request.