ManageEngine

PAM MASTERCLASS TRAINING 2022

WEBINAR
Q&A
MAY 12, 2022

1. We operate a heavily segregated network, with deny as default fire-wall rules. How do you deal with that?

You will have to create a firewall such all the connections are allowed only from the PAM360 server. From the users machine to PAM360 server, a browser based session will be launched to PAM360 server using port 8283 and from the PAM360 server to the target machines it is going to native ports for RDP(3389), SSH(22), Telnet(23), etc. So, you can very well have the deny firewall rules in place and allow the connections only from PAM360 server. Also, all the connection will be recorded and audited.

2. Can you elevate a user to a domain group? If so, how do you update the Kerberos tickets on the client?

Yes. We can elevate domain user to domain admin group using Just-In-Time privilege elevation, for which we make use of ManageEngine ADManager Plus. More information on Just-In-Time privilege is available here: https://www.manageengine.com/privileged-access-management/help/password-access-control-workflow.html#privilegeelevation.

Since, we elevate the complete account before launching the connection, there is no need to update the Kerberos tickets.

3. How can I give a domain account access to a specific server without giving them access to the domain controller itself?

Click on the resource actions next to the **Domain Controller resource -> Edit Resource** and check the box **"Restrict RDP to this resource"** and click save. This should restrict the access.

4. Can you or will you be demonstrating how Password Manager Pro works as a replacement for Microsoft LAPS?
Can you provide URLs to all related documentation on your website? How to configure, features, etc.

Yes. Password Manager Pro can very well do the job of LAPS. Using Password Manager Pro, you can manage all the local accounts of Windows Server, as well as, you can manage the passwords of more resource types. More information on remote password reset is available here: https://www.manageengine.com/privileged-access-management/help/remote_password_reset.html

5. We use identity based rules for network access. What account does the does PAM SSH or PAM RDP use?

You can either create generic accounts PAM SSH or PAM RDP and allow users to make use of this commonly shared account for privileged access. Alternatively, you can also allow users' own domain accounts to gain privilege access. Regardless, the idea is to provide privilege access only using PAM360. This way, each and every action performed is audited and recorded.

6. How do you update the Kerberos tickets on the client? Otherwise group membership doesn't take effect for many services such as file access.

With Just-In-Time elevation, we can elevate the user privilege and then login, so the Kerberos ticket update is not required. Alternatively, using Self-Service Privilege Elevation, we login and elevate only the user privileges for a particular application, and so in this case, PAM360 does not support Kerberos ticket update.

7. I want to put the PAM server into the vlan for servers and block all ports both in and out on PAM server. I want to just open needed ports to establish SSH and RDP connections through PAM, and if I configure a firewall rule which ports must be open.

From the user's machine, a browser-based session will be launched to the PAM360 server using port 8283, and from the PAM360 server to the target machines, it will reach the native ports—RDP(3389), SSH(22), Telnet(23,) etc. This way the connections are tunnelled through PAM360.