Deployment procedure

Introduction

PAM is the process that determines who has access to what types of information as it creates an integrated view of risk, threats, and controls.

Implementing a policy of least privilege minimizes unnecessary privilege allocation to ensure access to sensitive data is available only to those users who really need it.

Soffid provides a complete PAM solution. So, we want to describe in detail the Soffid PAM solution deployment procedure.

Prerequisites

First of all, you should install and config the Soffid PAM solution. To do that, you need to install the Jump servers and then configure them on Soffid Console.

> A jump server, jump host or jump box is a system on a network used to access and manage devices in a separate security zone. A jump server is a hardened and monitored device that spans two dissimilar security zones and provides a controlled means of access between them. (*)

You can follow the defined steps in the PAM Install & config book.

Deployment procedure

1. Networks

`Main Menu > Administration > Resources > Networks`

You need to add your company networks or the networks you want to manage, on Soffid Console. To do that you need to create those networks on the Networks page.

Once you have created your networks, you could continue with the next step.

> You can find more information on the Networks page.

2. Config Network discovery

`Main Menu > Administration > Resources > Network discovery`

When you open the Network discovery page, Soffid will display all the networks create on Soffid Console.

The network discovery process can be launched for each network, to do that, you need to configure the potential administrator accounts to connect to the hosts for each network.

You can add one or more potential administrator accounts to try to connect to the network hosts. These can be new accounts or existing accounts on Soffid. Also, you can remove accounts from the accounts to probe list. If you remove an account from the list, that account will continue to exist on Soffid.

> You can find more information on the Network discovery page.

Once you have configured the Network discovery parameter for a network, you could execute the process to begin to search or you could schedule the process execution.

3. Launch Network discovery

`Main Menu > Administration > Resources > Network discovery`

The Network discovery process is an unattended process. You could launch it, and it will be working until it will finish, even you close your Soffid session.

The Network discovery process could be a long process, depending on the network size, the number of hosts, and the firewalls as well.

> You can find more information on the Network discovery page.

3.1. Agent definition

When the network discovery process is launched, as the process finds hosts, it will try to connect to them using the defined credentials. When it gets to connect to the host with one credential, it will not try again with others.

If it gets to connect to the host, it will create automatically a Soffid agent with the proper attributes and connector parameters, also with the necessary account metadata.

3.2. Accounts / Account protected services

Then, the reconciliation process of the created agent will be launched and it will try to recover the information about the accounts defined on the host. Also, it will try to recover the information about the account protected services.

3.4. Entry points

The Network discovery process will create, in possible cases, a new entry point to the host with the basic attributes, and the proper executions to run it.

That entry point will display on the Application access tree page.

4. Password vault

`Main Menu > Administration > Resources > Password vault`

When the network discovery process finishes, it will be really important to determine what are the critical accounts. Those critical accounts should be located in protected storage, the Password vault.

On the password vault, you can locate the accounts, especially the critical account used to access critical systems. Password vault allows you to handle the access control list to these accounts, here you can define who are the owners, the managers, and the SSO users.

You need to configure in the right way the control access list, to allow only the proper users to change and view the passwords.

> You can find more information on the Password vault page.

5. Authorization processes

Soffid allows you to define and add approval processes to manage the use of critical accounts, where the manager or authorized user will approve or deny using them.

To define and configure approval workflows, you can use the Soffid BPM editor

`Main Menu > Administration > Configure Soffid > Workflow settings > BPM editor`

> You can visit the BPM Editor book to find more information.

One you have defined the approval process, you need to establish the relationship between the workflow and the account or accounts, to do that you need to configure the XACML Policy Management and the XACML PEP configuration.

6. XACML

> For detailed information about XACML, you can visit the XACML book.

6.1. XACML Policy Management

Using XACML Soffid can be able to add more complex and restricted rules to the authorizations. Here you can define policy sets and policies to describe general access control requirements.

Also, you can define some obligations as actions that have to be returned with response XACML. Here you can indicate the use of an authorization process.

`Main Menu > Administration > Configure Soffid > Security settings > XACML Policy Management`

6.2. XACML PEP configuration

You will need to enable and configure the Password vault Policy Enforcement Point (PEP). That is the way that Soffid provides to establish the relationship between the Authorization processes and the Password vault.

Be in mind, you only can configure one Password vault PEP, the policy set that you define, can contain more policy sets and policies to cover all your company needs.

`Main Menu > Administration > Configure Soffid > Security settings > XACML PEP configuration`

7. PAM policies and PAM rules

Using PAM all the sessions will be recorded (Screen, KeyBoard, Clipboard, and File transfers).

Soffid allows you to configure policies based on rules, so when each one of the rules is fulfilled, one or more actions will be triggered according to the configuration.

The available actions are to close the session, lock the account, open an issue on a ticketing system and notify the breaking rule. You can find more information visiting the and the.

7.1. PAM rules

`Main Menu > Administration > Configure Soffid > Security settings > PAM rules`

You can define rules to detect commands executed on a server. When a user launches a command defined on a rule, Soffid will detect it.

> For detailed information about PAM Rules, you can visit the PAM Rules page.

7.2. PAM policies

`Main Menu > Administration > Configure Soffid > Security settings > PAM policies`

You can define policies made up of several rules. For each rule, you could select the action to perform when Soffid detects that rule is accomplished.

On the Password Vault page, you can assign a PAM policy to each folder, depending on your needs.

> For detailed information about PAM Policies, you can visit the PAM Policies page.

(*) https://en.wikipedia.org/wiki/Jump_server

Revision #26
Created 17 August 2021 10:30:21 by pgarcia@soffid.com
Updated 1 December 2022 12:00:24 by pgarcia@soffid.com