
Proyecto

PAM cloud (v.3)

Actores

Soffid : sroujac ; gbuades

Cliente : Solarig : dsanchez@solarig.com ; cesarlafuente@solarig.com

Partner : Getronics

Arquitectura

MV Madrid

- sync server proxy
- jump server

MV Soria

- jump server

Consola : <https://solarig.prod.soffid.net/>

Configuraciones

General

Carga de usuarios : Agente AD en read only + eris

Incluye sincronización y rotación de contraseñas.

Principalmente configuraciones de los menus de acceso y del vault.

Cuentas compartidas

Todas las cuentas AD adm* tienen asociadas el usuario normal como owner para que solo la pueden usar.

Otros componentes

- Break glass
- ESSO

IDP & SP

⊖ Federation

- ⊖ Cloud providers
 - ⊖ Identity Providers
 - Afegir proveïdor d'identitat
 - ⊖ Service Providers
 - urn:federation:MicrosoftOnline - Azure
 - Afegir Service Provider
- ⊖ Soffid
 - ⊖ Identity Providers
 - ⊖ <http://idp.prod.soffid.net/solarig> - Soffid identity provider
 - Afegir proveïdor d'identitat virtual
 - Afegir proveïdor d'identitat
 - ⊖ Service Providers
 - <https://solarig.prod.soffid.net/soffid-iam-console> - Soffid
 - Afegir Service Provider
 - Afegir grup

Soffid IDP config :

- mtd d'autenticació pw + OTP
- perfils : ESSO + openidProfile
- SP SAML

Autenticació avançada

Permetre als usuaris recuperar les contrasenyes : ☐ No

Register OTP when required : ☒ Si ☐ No

Permetre als usuaris auto-registrar : ☐ No

Registre identitats identificades per IdPs externo : ☐ No

Emmagatzemar l'últim nom d'usuari al navegador : ☐ No

Habilitar el servei reCaptcha v3 : ☐ No

SP Azure :

Identificació

Tipus : SAML

Identificador : urn:federation:MicrosoftOnline

Nom : Azure

Configuració del servei

Metadades : <EntityDescriptor ID= "...18ad59a9-d87e-409a-9532-eee40c7c88af" entityID= "urn:federation:MicrosoftOnline" xmlns= "urn:oasis:names:tc:SAML:2.0:metadata" ...

NameID format : Email

Regles d'inici de sessió

Permetre suplantacions : Target application URL

Guió UID : log.info(".....> " + accountName);
return "adm" + accountName + "soffid";

Config Autenticació

Proveïdor d'identitat SAML extern

S

III

Habilitat

URL de metadades de la federació SAML:

java.com.soffid.iam.addons.federation.service.impl.InternalMetad:

Límit de la memòria cau (segons):

60

Proveïdor d'identitat:

http://idp.prod.soffid.net/solarig

Atribut SAML que conté el nom d'usuari:

S

III

Activar el registre de depuració SAML

Sesiones PAM

Carpetas de departamentos del cliente : Redes, Cyber y Sistemas.

```
gbuades-soffid@srvitpamsoffid1:~$ docker ps
```

CONTAINER ID	IMAGE	COMMAND	CREATED	STATUS	PORTS
d5ab5cacia92	soffid/soffid-pasr-https	"/usr/local/bin/start"	26 minutes ago	Up 26 minutes	5500/tcp, 5900/tcp
104d009be725	soffid-pasr-15	"/bin/sh -c /opt/sof..."	5 weeks ago	Up 4 weeks	8080/tcp, 0.0.0.0:8443->8443/tcp, :::8443->8443/tcp, 0.0.0.0:443->8443/tcp, [::]:443
66ee00f6d441	soffid-pam-launcher-1	"/bin/sh -c /opt/sof..."	10 months ago	Up 4 weeks	
	soffid/iam-sync:3.6.38	"/bin/sh -c /opt/sof..."			
	syncserver				

```
gbuades-soffid@srvitpamsoffid1:~$ docker image ls
```

REPOSITORY	TAG	IMAGE ID	CREATED	SIZE
soffid/pam-ssh	latest	252c8d9e819b	6 weeks ago	1.73GB
soffid/soffid-pasr-http	latest	34b907131628	6 weeks ago	3GB
soffid/soffid-pasr-https	latest	34b907131628	6 weeks ago	3GB
soffid/soffid-pasr-rdp	latest	eb428ef4b145	6 weeks ago	1.24GB
soffid/soffid-pasr-ssh	latest	f2cdf214ae15	6 weeks ago	1.27GB
soffid/soffid-pasr-google-chrome	latest	e8ad1d447758	6 weeks ago	3GB
soffid/pam-launcher	latest	c566a4fb78ae	4 months ago	1.36GB
soffid/iam-sync	3.6.38	bf2baa5043ba	10 months ago	599MB
eu.gcr.io/soffid-cloud/breakglass	1.0.6	9df66af88762	21 months ago	555MB

Menus de acceso

OJO config diferente para Azure.

Customizing browser PAM.pdf

⊖	Redes
	VMWare Soria
	Crea una entrada nova
⊖	Cyber
	PROOFPOINT
	Proofpoint Zenguide
	Proofpoint ATO Human Risk
	Proofpoint PoD
	Crowdstrike
	Netskope
	Crea una entrada nova
⊖	Sistemas
	VEAM DATA CLOUD
	Azure
	Navision
	SharePoint
	AWS
	MS Fabric
	SRVWDC04
	Crea una entrada nova

Config Pw Vault

SSO users : rol SOFFID_PRIV para permitir ver la cuenta pero lanzar workflow de aprobaciones si no es owner de la cuenta.

SSO owners : usuario(s) propietario(s) de la cuenta

Workflows

- reservationAccount en el vault
 - Initiadores : rol SOFFID_PRIV
 - Abrobadores : SOFFID_SUPER de lunes a viernes y SOFFID_CC el finde
- Elevación de privilegios en equipos
 - Initiadores : usuarios ESSO que no tienen cuentas AD admin
 - Abrobadores : SOFFID_SUPER de lunes a viernes y SOFFID_CC el finde

Roles importantes

Soffid roles	Users	Permissions
SOFFID_PRIV	Usuarios con acceso a soffid vault	ver el vault, pedir permisiones y acceder a su sistemas y autorizaciones PAM
SOFFID_CC	Centro de control de solarig	Validadores de workflow durante el finde
SOFFID_SUPER	Departamiento IT	Validadores de workflow durante la semana
SOFFID_ACCESO_FINDE	usuarios con acceso a toda hora	usuarios con acceso de lunes a domingo
SOFFID_WEEK_ACCESS	usuarios con accesos solamente en horarios laborales	usuarios con acceso de 8h a 18h de lunes a viernes
SOFFID_ADMIN	dsanchez, mfandino & cesarlafuente	*
SOFFID_USER	Usuarios con acceso a soffid	Acceso consola

XACML Policies

Árbol del conjunto de políticas	Descripción
Filter	Filter
Set (2)	General policy set
SubSet (2)	Location
Type (1)	Connexion type
SetTime (1)	Need aproval
TimeDay (2)	Horarios permitidos
Out (1)	Out of times
Nuevo conjunto de políticas Nueva política Nueva referencia política Nueva referencia de conjunto de políticas	
SSOUsers (1)	SSOUsers need aproval
Nuevo conjunto de políticas Nueva política Nueva referencia política Nueva referencia de conjunto de políticas	
Location (1)	Reglas de ubicación
Nuevo conjunto de políticas Nueva política Nueva referencia política Nueva referencia de conjunto de políticas	
Nuevo conjunto de políticas Nueva política Nueva referencia política Nueva referencia de conjunto de políticas	