

# Bastion TMA

Interface d'admin :

Ajout des accès à des users à des serveurs non existants dans le bastion.

Ajout des serveurs:

Targets --> Devices --> Add

The screenshot shows the 'New' device configuration page in the Bastion TMA admin interface. The breadcrumb trail is 'Targets > Devices > New > General'. The 'General' tab is active, showing fields for 'Name \*', 'Alias', and 'IP address or FQDN \*'. Below these is a 'Description' section with a play icon. An 'Apply' button is at the bottom left.

Mettre le nom du serveur et son IP puis cliquer sur apply.

Ensuite aller sur l'onglet services et cliquer sur ADD puis RDP pour serveurs Windows (SSH pour serveurs Linux)

The screenshot shows the 'New service RDP' dialog box. It has a close button (X) in the top right. The 'Device' field contains 'PRD'. The 'Service name \*' field contains 'RDP' and has a red error message: 'This name is already used'. The 'Port \*' field contains '3389'. The 'Connection policy \*' dropdown is set to 'RDP'. On the right, the 'Global domains' section states 'A global domain is required to create targets for applications and clusters' with a dropdown menu. Below that, the 'Proxy options' section lists several checked items: RDP\_CLIPBOARD\_UP, RDP\_CLIPBOARD\_DOWN, RDP\_CLIPBOARD\_FILE, RDP\_PRINTER, RDP\_COM\_PORT, RDP\_DRIVE, RDP\_SMARTCARD, RDP\_AUDIO\_OUTPUT, and RDP\_AUDIO\_INPUT. At the bottom, there are 'Close' and 'Apply and close' buttons.

Faire apply and close. Ne pas prendre en compte l'erreur dans la PJ. La conf est déjà en place pour le serveur.

Création groupe de device :

Se rendre dans Targets --> Groups --> Add

Lui donner un nom puis apply

Aller sur l'onglet Session Management Targets puis interactive login:

## Add interactive login targets for session management

Group

From \*

Device \*

Services \*

Select at least one available entry

<input type="checkbox"/>	Service name	⬆ ⬇ 🔍	Already in group
<input type="checkbox"/>	RDP		✓

Penser à cocher RDP à chaque fois pour tous les serveurs.

Résultat final:

 Add

<input type="checkbox"/>	Application	Device	Service
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP
<input type="checkbox"/>	-	PRD-[REDACTED]	RDP

### Attribution des accès aux users:

Aller dans Authorizations --> Manage authorizations --> + Add an autorisation

User group \*:

Target group \*:

Name \*:

Description:

Accès aux nouveaux serveurs Exchange 2019

Critical targets:

Enable sessions:

Protocols/subprotocols \*:

Available Protocols/subprotocols

Q

RAWTCPIP

RLOGIN

SSH\_SHELL\_SESSION

SSH\_REMOTE\_COMMAND

SSH\_SCP\_UP

SSH\_SCP\_DOWN

SSH\_X11

SFTP\_SESSION

SSH\_DIRECT\_TCPIP

SSH\_REVERSE\_TCPIP

SSH\_AUTH\_AGENT

Select all

Selected Protocols/subprotocols

Q

Select and click

RDP

RDP\_AUDIO\_INPUT

RDP\_AUDIO\_OUTPUT

RDP\_CLIPBOARD\_DOWN

RDP\_CLIPBOARD\_FILE

RDP\_CLIPBOARD\_UP

RDP\_COM\_PORT

RDP\_DRIVE

RDP\_PRINTER

RDP\_SMARTCARD

Delete all

Enable session recording:

Enable password checkout:

Enable approval workflow:

Demander de tester les accès.

Attention il faut que le port RDP 3389 soit ouvert entre les serveurs et le bastion TMA.

Revision #1

Created 31 October 2024 19:40:46 by Cavallone

Updated 31 October 2024 19:52:42 by Cavallone