

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 form in the Bastion TMA admin interface. The breadcrumb trail is 'Targets > Devices > New > General'. The 'General' tab is active, with other tabs like 'Services', 'Local domains', 'Local accounts', 'Groups', 'Certificates', and 'Tags' visible. The form includes 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' followed by a redacted area. 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' and has a dropdown for 'Enter a global domain name'. 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 *: [REDACTED]

Target group *: [REDACTED]

Name *: [REDACTED]

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