Setup instructions

Define the perimeter

MFA Bastion

Currently the Bastion doesn't yet support SAML authentications.
The only question to ask for MFA is therefore the **source of the users**.
If there are users who are not in the **Active Directory**, it's best to go through **local Trustelem users**, and not local Bastion users.
This way you only have **one source of identity to maintain alongside the AD**.
Furthermore, Trustelem has powerful tools to manage these local users.
But if you need to have MFA for local Bastion users, it is still a possibility.

Population Active Directory users?

- MFA = login/pwd using AD + 2nd factor using Trustelem Radius
- **Import AD users** - read the page: Active Directory users - Trustelem ADConnect
- **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
  - *Choose an enrollment campaign by email if possible.*
- **Setup the Radius on Bastion for AD users** - read the chapters:
  - Install Trustelem Connect
  - Trustelem Radius on Bastion for AD users
- **Define the access rules** - read the page: Access rules
  - *The rule should be for Radius, with 2nd factor only.*

Population Trustelem users?

- MFA = login/pwd using Trustelem LDAP + 2nd factor using Trustelem Radius
- **Create Trustelem users** - read the page: Trustelem local users
- **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
  - *Choose an enrollment campaign by email if possible.*
- **Setup Trustelem LDAP on Bastion** - read the chapters:
  - Install Trustelem Connect

    - Trustelem LDAP on Bastion
      For the LDAP external authentication, the login/username attributes should be "mail".
      So to login to the Bastion you should use "trustelem_email@bastion_authentication_domain_name".
- **Setup the Radius on Bastion for Trustelem users** - read the chapter: Trustelem Radius on Bastion for Trustelem users
- **Define the access rules** - read the page: Access rules
    - *The rule should be 1 factor for LDAP and 2nd factor only for Radius.*

Population local Bastion users?

- MFA = login/pwd/2nd factor using Trustelem Radius
- **Create Trustelem users** - read the page: Trustelem local users
- **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
    - *Choose an enrollment campaign by email if possible.*
- **Setup the Radius on Bastion for Bastion users** - read the chapters:
    - Install Trustelem Connect
    - Trustelem Radius on Bastion for Bastion users
    - *Note: the Bastion local user login must match the login on Trustelem, so it has to be an email address.*
- **Define the access rules** - read the page: Access rules
    - *The rule should be for Radius, with 2 factors: on the Bastion, it is not possible to have local password + Radius*

MFA Access Manager

For the Access Manager, we must also ask the question of identity sources and, in the same way as for the Bastion, **favor local Trustelem users over local Access Manager users**.
For **Active Directory users**, it's also necessary to study the access method (**account mapping**, or **vault transformation rule**) in order to define whether it is better to go through a **SAML** or **Radius** configuration.

Population Active Directory users?

- Are you mainly using account mapping (same login for primary/secondary authentication)?
    - **YES**
        - MFA = login/pwd using AD + 2nd factor using Trustelem Radius
        - **Import AD users** - read the page: Active Directory users - Trustelem ADConnect

    - **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
        - *Choose an enrollment campaign by email if possible.*
    - **Setup Trustelem Radius on Access Manager for AD users** - read the chapter: Trustelem Radius on Access Manager for AD users
    - **Define the access rules** - read the page: Access rules
        - *The rule should be for Radius, with 2nd factor only.*
- **NO**
    - MFA = login/pwd/2nd factor using Trustelem SAML
    - **Import AD users** - read the page: Active Directory users - Trustelem ADConnect
    - **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
        - *Choose an enrollment campaign with automatic enroll during login.*
    - **Setup Trustelem SAML on Access Manager for AD users** - read the page: Trustelem SAML on Access Manager for AD users
    - **Define the access rules** - read the page: Access rules
        - *The rule should be 2 factors, for both internal and external zones.*

Population local Trustelem users?

- MFA = login/pwd/2nd factor using Trustelem SAML
- **Create Trustelem users** - read the page: Trustelem local users
- **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
    - *Choose an enrollment campaign with automatic enroll during login.*
- **Setup Trustelem LDAP on Bastion** - read the chapters:
    - Install Trustelem Connect
    - Trustelem LDAP on Bastion
      For the LDAP external authentication, the login/username attributes should be "mail".
      So to login to the Bastion you should use "trustelem_email@bastion_authentication_domain_name".
- **Setup the Radius on Bastion for Trustelem users** - read the chapter: Trustelem Radius on Bastion for Trustelem users
    - *You will use the LDAP setup to give Trustelem users access to targets. But it will also allow the authentication on the Bastion. It's why you need to secure this access with Radius.*
- **Setup Trustelem SAML on Access Manager for Trustelem users** - read the chapter: Trustelem SAML on Access Manager for Trustelem users

    - *The login attribute on Access Manager SAML setup should be "email".*
- **Define the access rules** - read the page: Access rules
    - *For Access Manager, the rule should be "2 factors" for both internal and external zones.**
    - *For the Bastion, the rules are 1 factor for LDAP and 2nd factor only for Radius.*

Population local Access Manager users?

- Do you want to keep their password or use Trustelem password instead?
    - **Keep their password**
        - MFA = login/pwd using AM + 2nd factor using Trustelem Radius
        - **Create Trustelem users** - read the page: Trustelem local users
        - **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
            - *Choose an enrollment campaign by email if possible.*
        - **Setup Trustelem Radius on Access Manager for AM users** - read the chapter: Trustelem Radius on Access Manager for AM users
            - *On Access Manager domain setup, in the field Associated Authenticators: Local database Factor 1 - Radius Authenticator Factor 2*
        - **Define the access rules** - read the page: Access rules
            - *The rule should be for Radius, with 2nd factor only.*
    - **Use Trustelem password**
        - MFA = login/pwd + 2nd factor using Trustelem Radius
        - **Create Trustelem users** - read the page: Trustelem local users
        - **Define the 2nd factors and the enrollment process** - read the page: Multi factors authentication
            - *Choose an enrollment campaign by email if possible.*
        - **Setup Trustelem Radius on Access Manager for AM users** - read the chapter: Trustelem Radius on Access Manager for AM users
            - *On Access Manager domain setup, in the field Associated Authenticators: Local database Factor Unused - Radius Authenticator Factor 1*
        - **Define the access rules** - read the page: Access rules
            - *The rule should be for Radius, with 2 factors.*

Define the other needs

- **Delegate Trustelem local users management** - read the page: Delegated Administration
- **Reset users password with Trustelem** - read the page: Self Service Password Reset
- **Use AzureAD users instead of AD users** - read the chapter: AzureAD users

Revision #39
Created 1 July 2022 10:10:25 by WALLIX Admin
Updated 16 July 2024 12:55:54 by WALLIX Admin