CA Privileged Access Management Use Cases

This document will attempt to describe and outline the steps and the logic behind a given use case. This is an attempt to explain the use case in a more logical fashion which connects all the “dots” to achieve a broader and more comprehensive understanding of CA Privileged Access Management (CA PAM).

Use Case Microsoft SQL Endpoint – Transparent Login

1. Log onto CA PAM UI with administrative privileges (super or a user with Global Administration Role) which can create/define all the following steps.
2. Define a ***Service***
    a. Select ***Services*** → ***TCP/UDP Services*** → ***Create TCP/UDP Service***
    b. ***Basic Info*** Section
        i. ***Service Name:*** Provide a unique name that can be easily identified and associated with the Service; i.e. ***MSSQL-TL***
        ii. ***Local IP:*** Leave the loop back IP in place.
        iii. ***Port(s)***: Define all the ports (separated by a space or comma), i.e. 3389
        iv. ***Protocol:*** Select the appropriate protocol; i.e. TCP
    c. ***Administration*** Section
        i. ***Enable:*** checked
        ii. ***Application Protocol:*** RDP
    d. Click ***Save***
3. Define a ***Device***
    a. Select ***Devices*** → ***Manage Devices*** → ***Create Device***
    b. ***Device Name:*** A display name for the MS SQL Server Studio that is helpful in identifying and searching the list; i.e. ***MSSQL-RDP-TL***
    c. ***Address:*** Provide the IP Address or FQDN (if resolvable) for the MS SQL server.
    d. ***Device Type:*** Check ***Access*** and ***Password Management***
    e. ***Description, Target Server Description1 - 2*** & ***Tags:*** Use these fields to provide appropriate information which will be helpful in searching.
    f. In the ***Access Methods*** section, click the ***RDP*** link
    g. Click ***Save***
4. Define an ***Application***
    a. Select ***Policy*** → ***Manage Passwords***
    b. On the new Tab, select ***Targets*** → ***Applications*** → ***Add*** to define a new application
    c. Across from the ***Host Name*** field, click the ***Find Server*** icon 🔍 on the right and select the device defined earlier. This will fill in both ***Host Name*** and ***Device Name*** fields.
    d. For ***Application Name***, enter a name that conveys the association of the Device and Application; i.e. ***MSSQL-RDP-App***
    e. For the ***Application Type***, select ***Generic***
    f. Click ***Save***

5. Define an ***Account***
    a. While in ***Password Management*** page; select ***Target*** → ***Accounts*** → ***Add*** to define a new account.
    b. For the ***Application Name*** field, click the ***Find Application*** icon 🔍 on the right and select the application that we defined earlier. This will fill in ***Host Name***, ***Device Name***, and ***Application Name*** fields.
    c. For the ***Account Name*** field, provide the User ID used to log onto this server. i.e. ***user-xyz***
    d. Enter the corresponding password in the ***Password*** field
    e. Click ***Save***
6. Define an access ***Policy***
    a. On the main page of PAM UI, select ***Policy*** → ***Manage Policies***
    b. In the ***User (Group)*** field, enter the name of the user which this policy will be applied to; i.e. ***user-xyz***
    c. In the ***Device (Group)*** field, select the device name created earlier; i.e. ***MSSQL-RDP-TL***
    d. Click ***Create Policy***
    e. In the ***Access*** section, click the ***Add*** link and check the ***RDP*** access method (i.e. RDP:3389) and the account associated with it (i.e. ***MSSQL-RDP-App – hostname\user-xyz***).
    f. If session recording is desired then in the ***Recording*** section, check the ***Graphical*** option.
    g. Click ***Save***
7. ***Access*** page
    a. At this point if we log onto the PAM UI (with the user we selected earlier) and move to the ***Access*** page, we should be able to see a line entry for MS SQL, ***RDP***, under the ***Access Methods*** Column.
    b. This will open a transparent login to the target Windows system; without prompting for login information.
    c. Click the ***RDP*** link and ensure the RDP access works as it is supposed to.
8. ***Learn Mode***
    a. We need to use the ***Learn mode*** to capture the steps necessary to launch the target application and input the necessary information for it to be used properly (transparently).
    b. On the ***Access*** page, hove over this newly created ***RDP*** access method to activate the sub-menu and select the ***Learn mode*** before clicking on the ***Launch*** button.
    c. This will open a transparent login to the target Windows system. You will notice that the ***Learn Tool*** is launched.
    d. Follow the direction outlined on the online documentation to capture this application specific launch information and save it to ***CA PAM Transparent Login Configs***. The online information can be found at:
        i. Go to https://docops.ca.com and login

ii. In the ***Select a product*** drop-down start typing ***CA Privileged Access***… and select the most recent version or the version that applies to your environment. At the time this document was being edited, version 2.8.1 was the most recent one.

iii. Select the right version

iv. In the Search box, type ***RDP connections***

v. You should be directed to the section called ***RDP Connections*** under the ***Implementing*** → ***Provision Your Server*** → ***Provisioning Devices*** → ***Set up Transparent Login***

vi. Ensure all the necessary steps are taken corresponding to your target system version.

9. Define a ***RDP Application***

a. On the CA PAM UI, select ***Services*** → ***RDP Applications***

b. Click the link for ***Transparent Login Configs*** (on the top right corner) and view the configurations available. You should see the configuration you created in the step above. Exit this view.

c. Once back in the ***Services*** → ***RDP Applications***, click ***Create RDP Application***

d. Provide a name in the ***RDP App Name*** field

e. Provide the correct/absolute path to the target application in the ***Launch Path*** field. i.e. C:\putty\PuTTY.exe

f. In the ***Administration*** section, select/check ***Enable*** and ***Transparent Login***

g. In the ***Transparent Login*** section

i. Provide the name for the ***Window Title*** field of whatever application you are launching. This needs to match the remote application title we plan to launch.

ii. Then click the ***Transparent Login Config*** field and select the corresponding configuration from the list.

iii. Also check the ***RDP Session*** box.

h. Click ***Save***

10. Modify the existing ***Device***

a. On the main page of PAM UI, select ***Devices*** → ***Manage Devices***

b. Find and select the target device we have worked on during this exercise.

c. In the ***Services*** section, click ***Add*** and select the ***RDP*** Application we defined above.

d. Click ***Save***

11. Modify the existing access ***Policy***

a. On the main page of PAM UI, select ***Policy*** → ***Manage Policies***

b. Look for the access policy we defined earlier and select it.

c. In the ***Services*** section, click ***Add*** and select the ***RDP*** Application we defined above. While in this field, also select the account associated with this application. Additionally, select the account to be used with the target application.

d. In the ***Transparent Login*** section, check ***Enabled*** option.

e. Click ***Save***

12. ***Access*** page

a. Go back to the CA PAM ***Access*** page
b. Click the ***Restart Session*** button on top right coroner of this page to ensure the latest policy changes are updated.
c. Now you should be able to see an entry for the MS SQL device under the ***RDP Applications*** column.
d. Click the link for MS SQL under ***RDP Applications*** to test the access.
e. If the RDP configuration is correct, this should log you onto the system and then launch the target app and log you on.