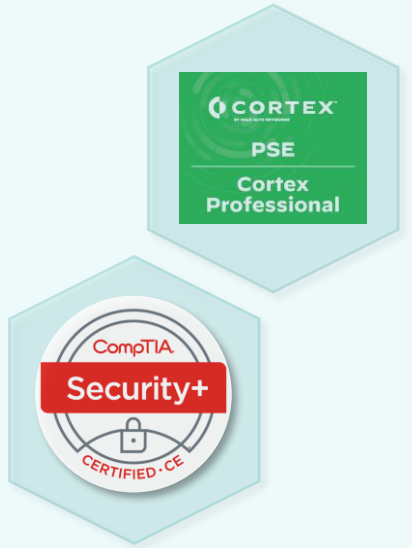
Jak se bezpečnost změnila, ale hesla zůstala v plaintextu



David Buřínský

System Engineer, System Security

david.burinsky@alef.com

ALEF

Vývoj bezpečnosti

Bezpečnostní principy

- Windows 11
  - Credential guard
  - TPM čip
- MFA
- XDR řešení
- Šifrování
- GDPR, ISO, NIS2
- Zero Trust

Zero Trust Princ

Verify explicitly

Use least privileged access

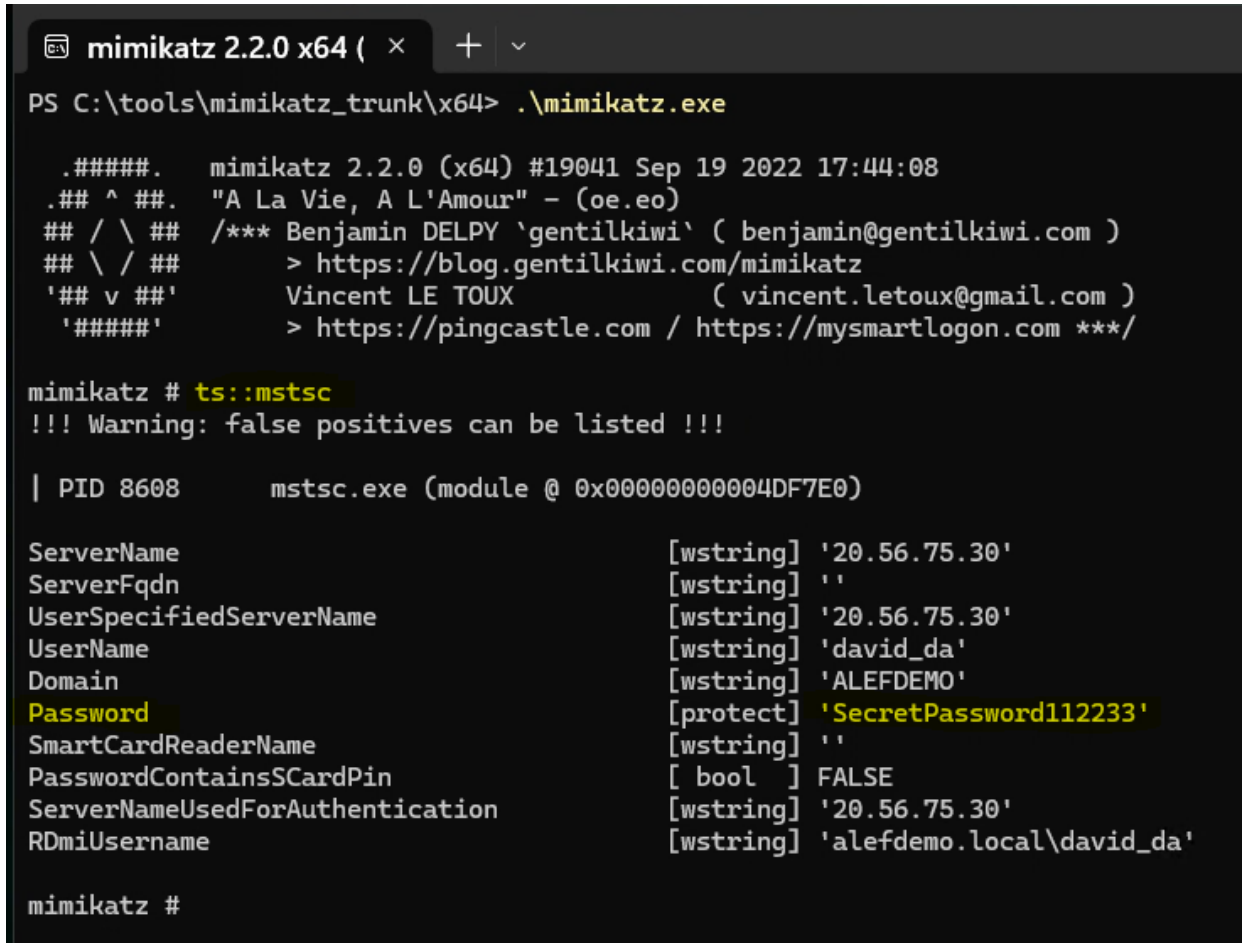
Algorithm	Typ			
RC4	Sym			
3DES	Sym			
IDEA	Sym			
MD5	Has			
SHA-1	Has			
DES	Sym			
RSA	Asy			
ECC	Asy			
ElGamal	Asy			
SHA-256	Has			
SHA-3	Has			
Diffie-Hellman	Key			
AES	Sym			
Blowfish	Sym			
Twofish	Symmetric	Active	128, 192, 256 bits	Successor to Blowfish; considered secure
ChaCha20	Symmetric	Active	256 bits	High performance; used in modern protocols like TLS 1.3


RDP
HESLO V
ČITELNÉ PODOBĚ
CREDENTIAL
GUARD
imgflip.com

Vzdálený přístup

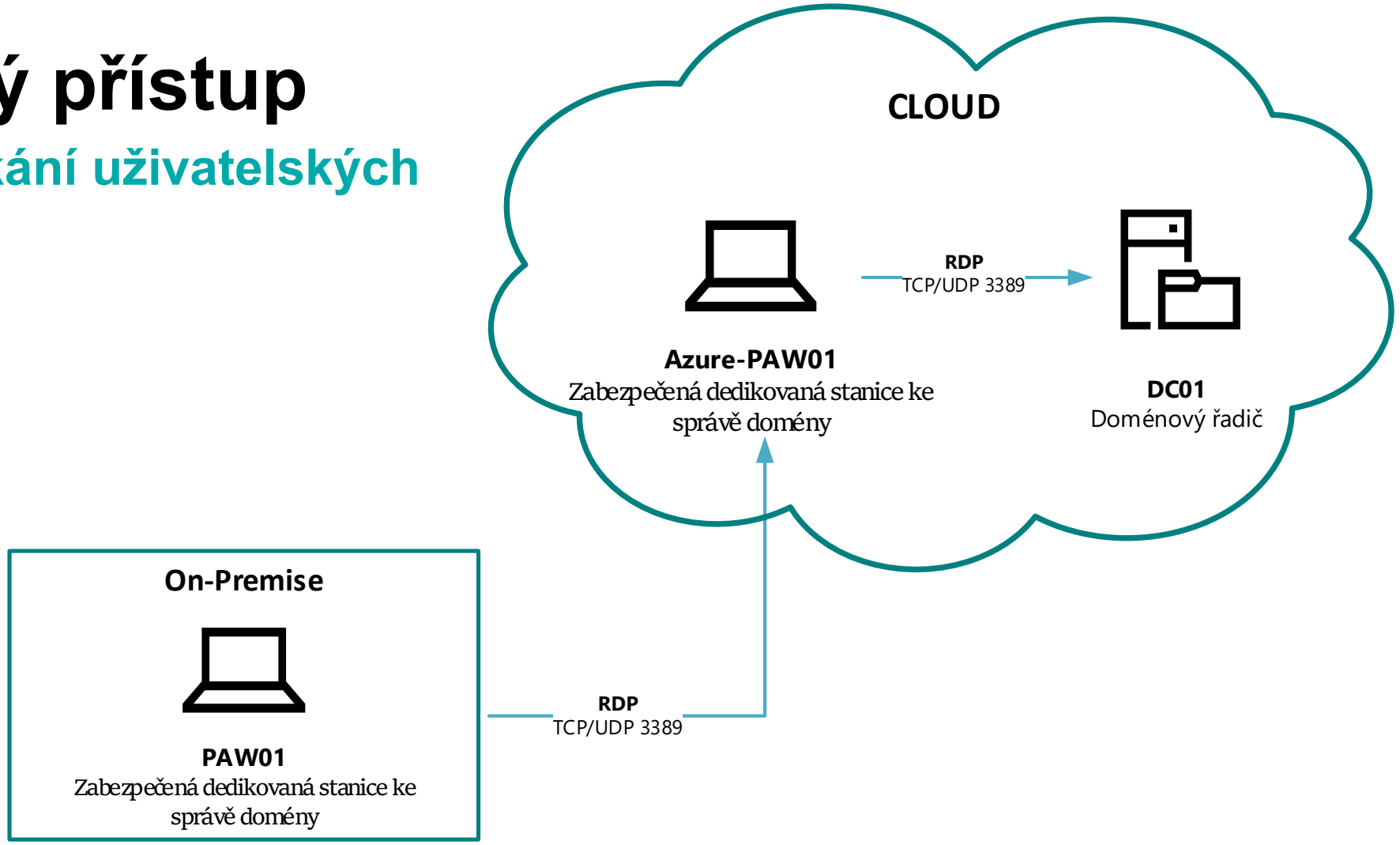
Teorie

- **Remote Desktop Protocol**
  - Klient-server vzdálené ovládání počítače
  - mstsc.exe
- **Mimikatz**
  - Benjamin Delpy
  - Silný nástroj pro extrakci uživatelských údajů z Windows systémů
  - Eskalace privilegií
  - Penetrační testování



Vzdálený přístup

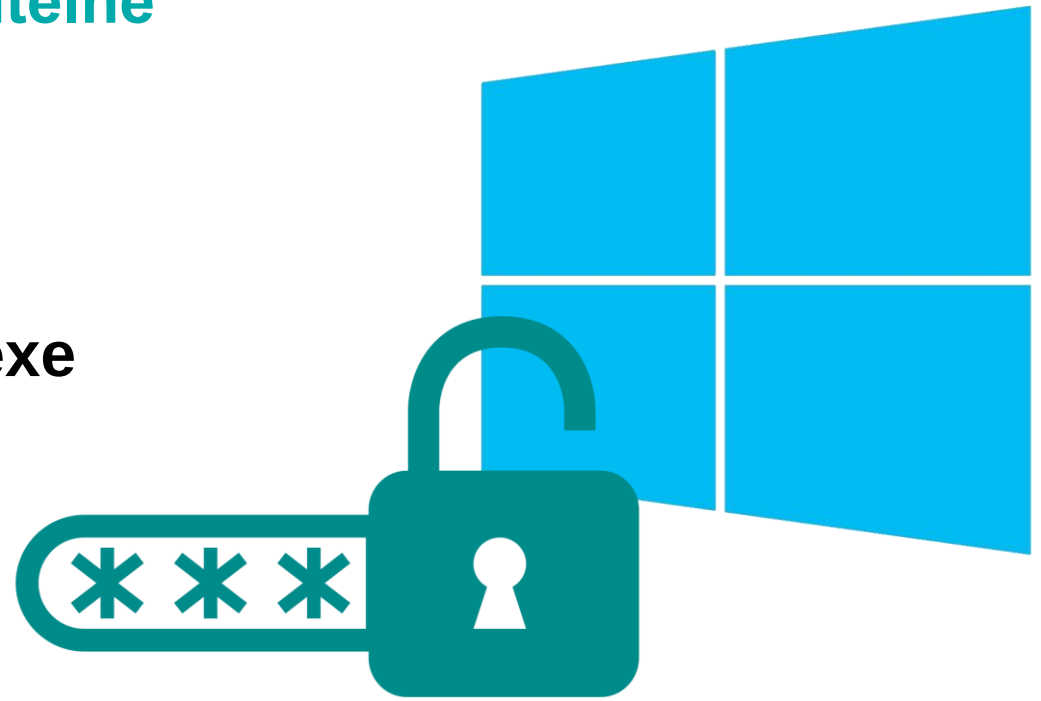
DEMO – získání uživatelských údajů

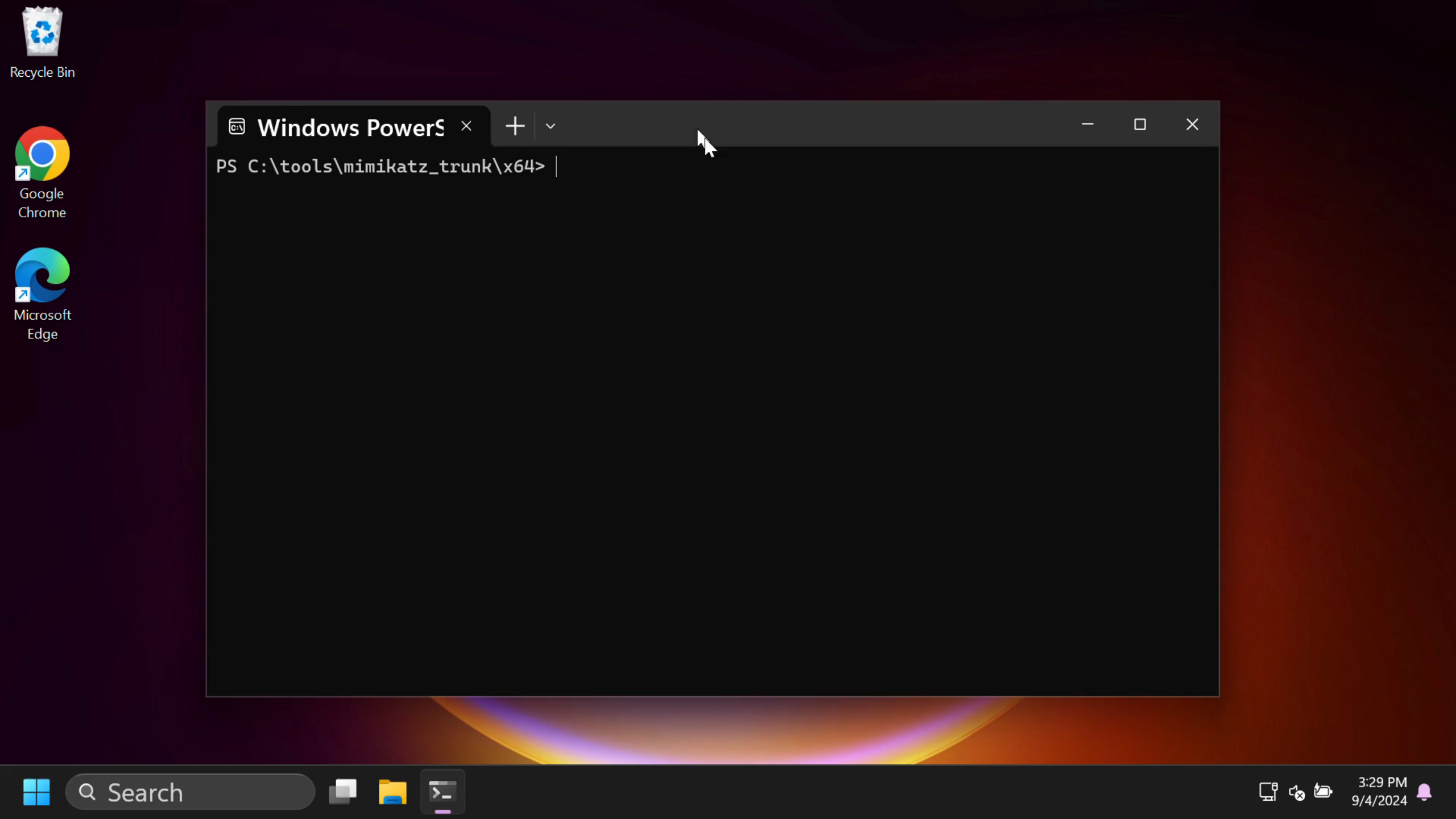


Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě

Mstsc.exe




Recycle Bin
Google Chrome
Microsoft Edge
Windows PowerS
PS C:\tools\mimikatz_trunk\x64>
Search
3:29 PM
9/4/2024

Vzdálený přístup a heslo v čitelné podobě

Mitigace

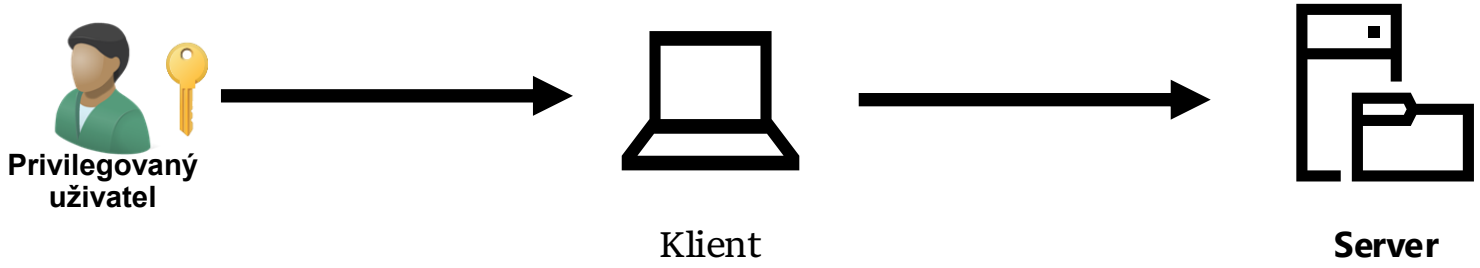
- ~~Windows 11~~
  - ~~Credential guard~~
  - ~~TPM čip~~
- MFA
- ~~XDR řešení~~
- ~~Šifrování~~
- ~~GDPR, ISO, NIS2~~
- Zero Trust

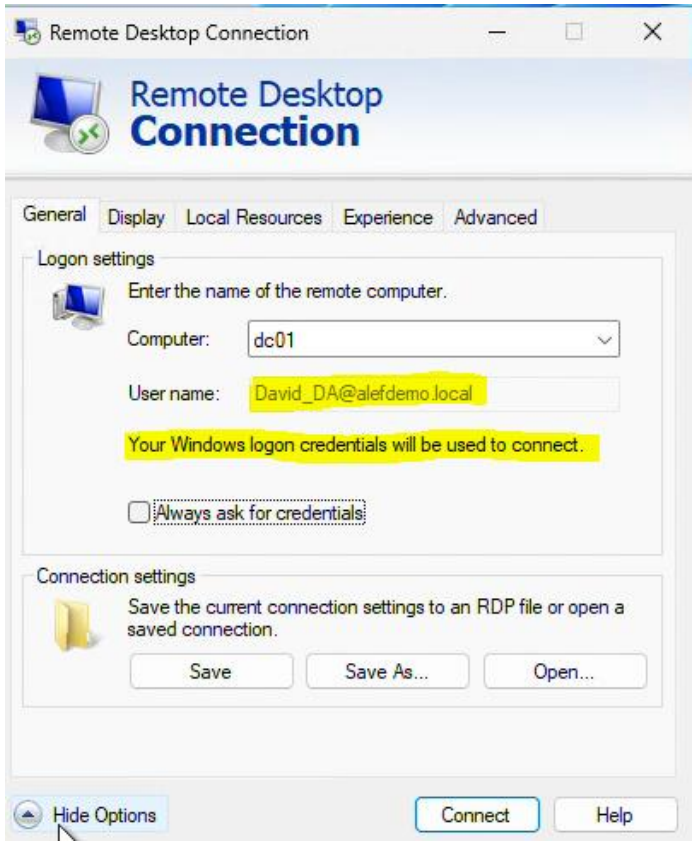
```
PS C:\tools\mimikatz_trunk\x64> .\mimikatz.exe

  .#####.   mimikatz 2.2.0 (x64) #19041 Sep 19 2022 17:44:08
 .## ^ ##.  "A La Vie, A L'Amour" - (oe.eo)
 ## / \ ##  /*** Benjamin DELPY `gentilkiwi` ( benjamin@gentilkiwi.com )
 ## \ / ##       > https://blog.gentilkiwi.com/mimikatz
 '## v ##'       Vincent LE TOUX             ( vincent.letoux@gmail.com )
  '#####'        > https://pingcastle.com / https://mysmartlogon.com ***/

mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 2628      mstsc.exe (module @ 0x000000000037F8A0)

ServerName                              [wstring] 'dc02.alefdemo.safe'
ServerFqdn                              [wstring] ''
UserSpecifiedServerName                 [wstring] 'dc02.alefdemo.safe'
UserName                                [wstring] 'T0-dburinsky'
Domain                                  [wstring] 'ALEFDEMO'
Password                                [protect] '123456'
SmartCardReaderName                     [wstring] ''
PasswordContainsSCardPin                [ bool  ] TRUE
ServerNameUsedForAuthentication         [wstring] 'dc02.alefdemo.safe'
RDmiUsername                            [wstring] 'ALEFDEMO\t0-dburinsky'
```

Vzdálený přístup a heslo v čitelné podobě

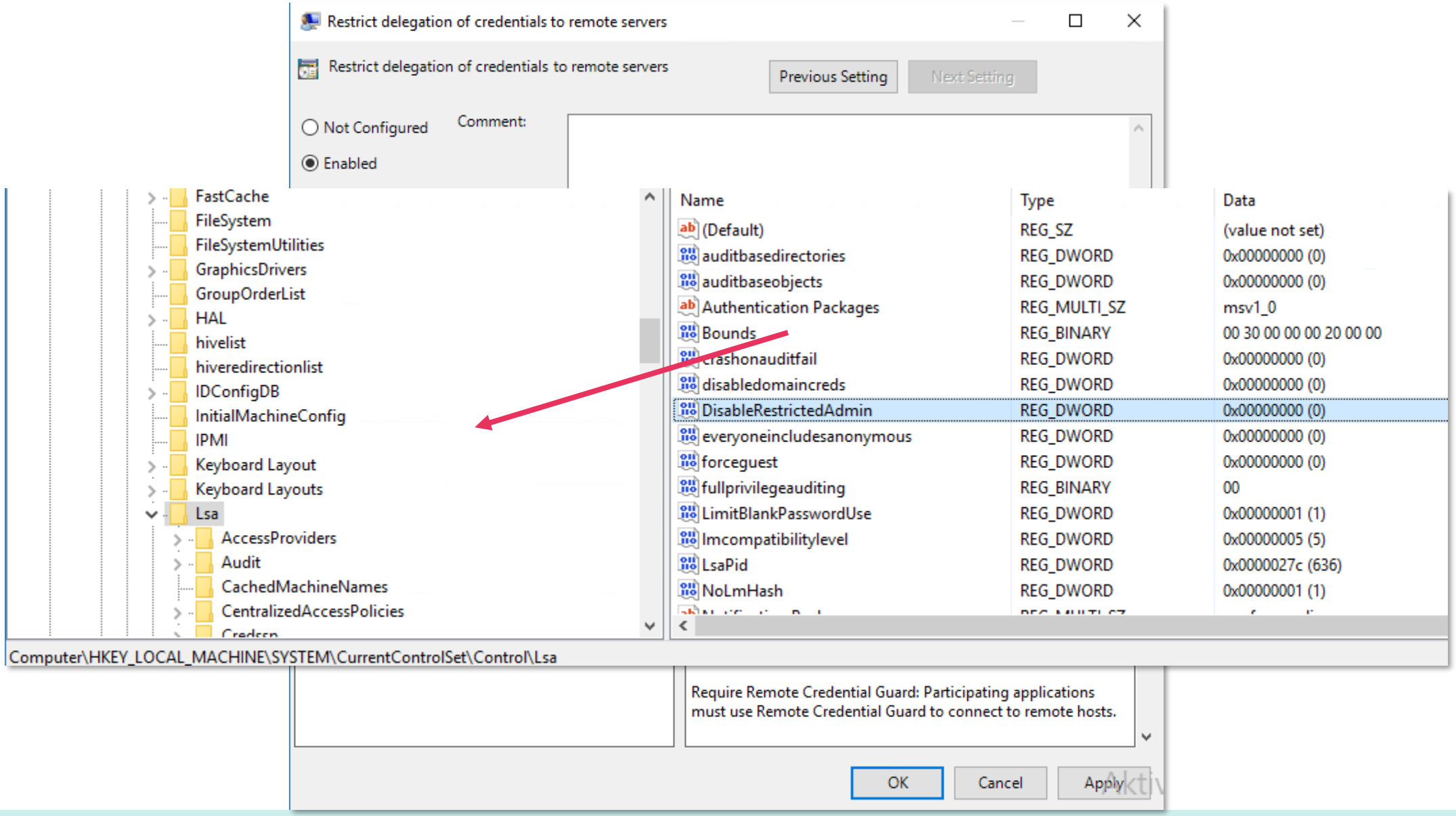
Mitigace

- **Restricted Admin Mode**
  - Dostupný výhradně pro členy skupiny **Administrators.**
  - **Nedochází k delegaci uživatelských údajů na cílový server.**
  - Povolení na straně serveru / možné vynucení na straně klienta.





Administrative Templates\System\Credential Guard



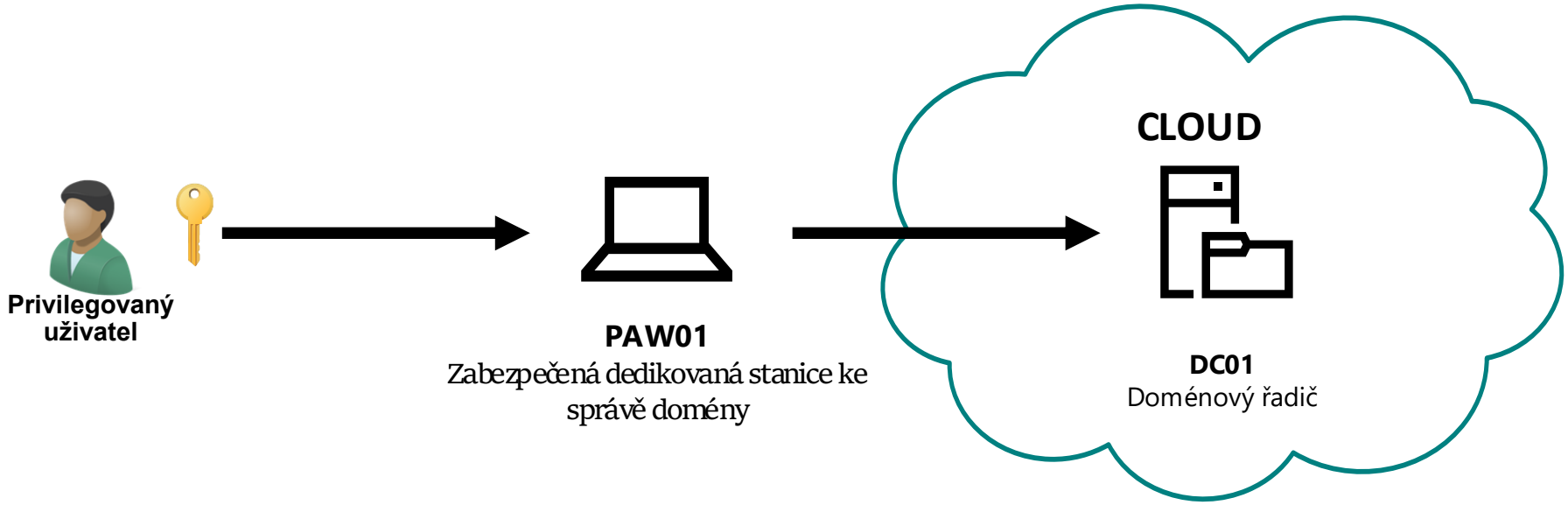
Vzdálený přístup a heslo v čitelné podobě

Mitigace

- **Restricted Admin Mode**
  - Dostupný výhradně pro členy skupiny **Administrators.**
  - **Nedochází k delegaci uživatelských údajů na cílový server.**
  - Povolení na straně serveru / možné vynucení na straně klienta.
- **Privileged Access Workstation**
  - **Dedikované** počítače pro správu infrastruktury.
  - Maximální koncentrace na **vyloučení** potenciálních **vektorů infiltrace**.
  - **Bezpečný bod kontaktu** s infrastrukturou.

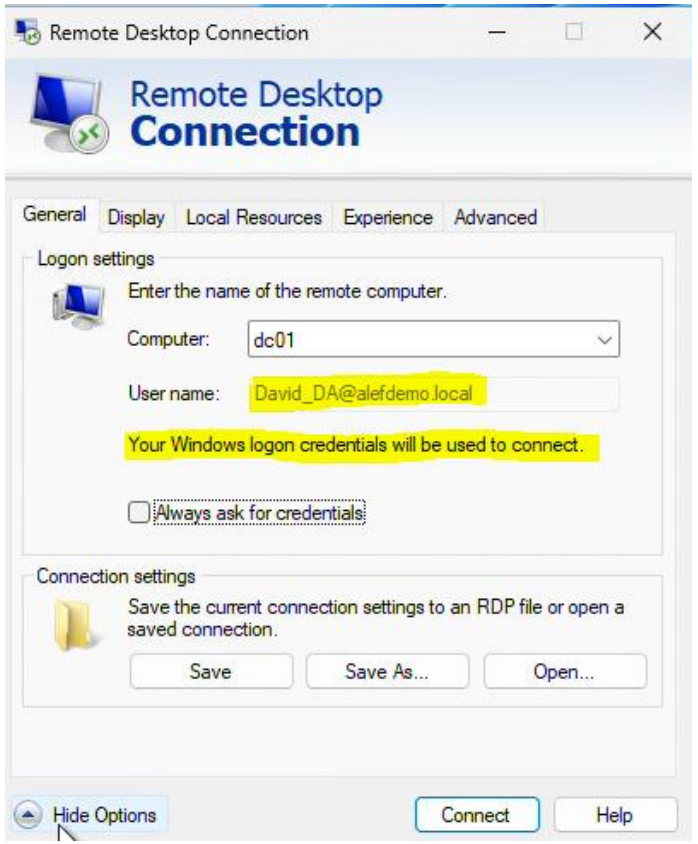
Vzdálený přístup

Mitigace – Restricted Admin Mode



Vzdálený přístup a heslo v čitelné podobě

Mitigace

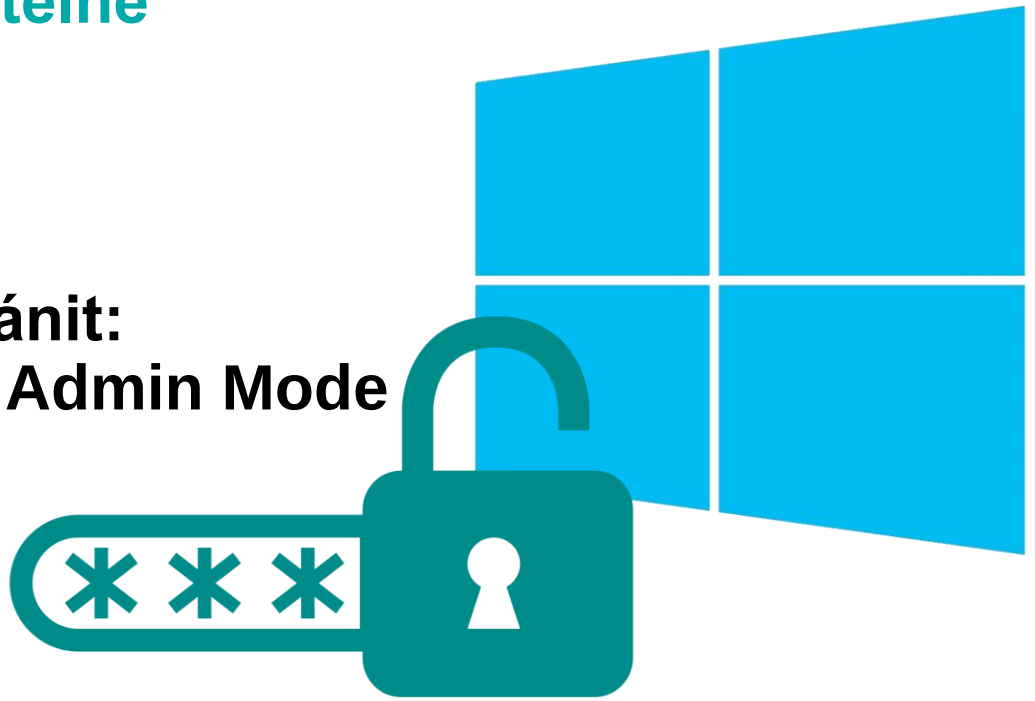


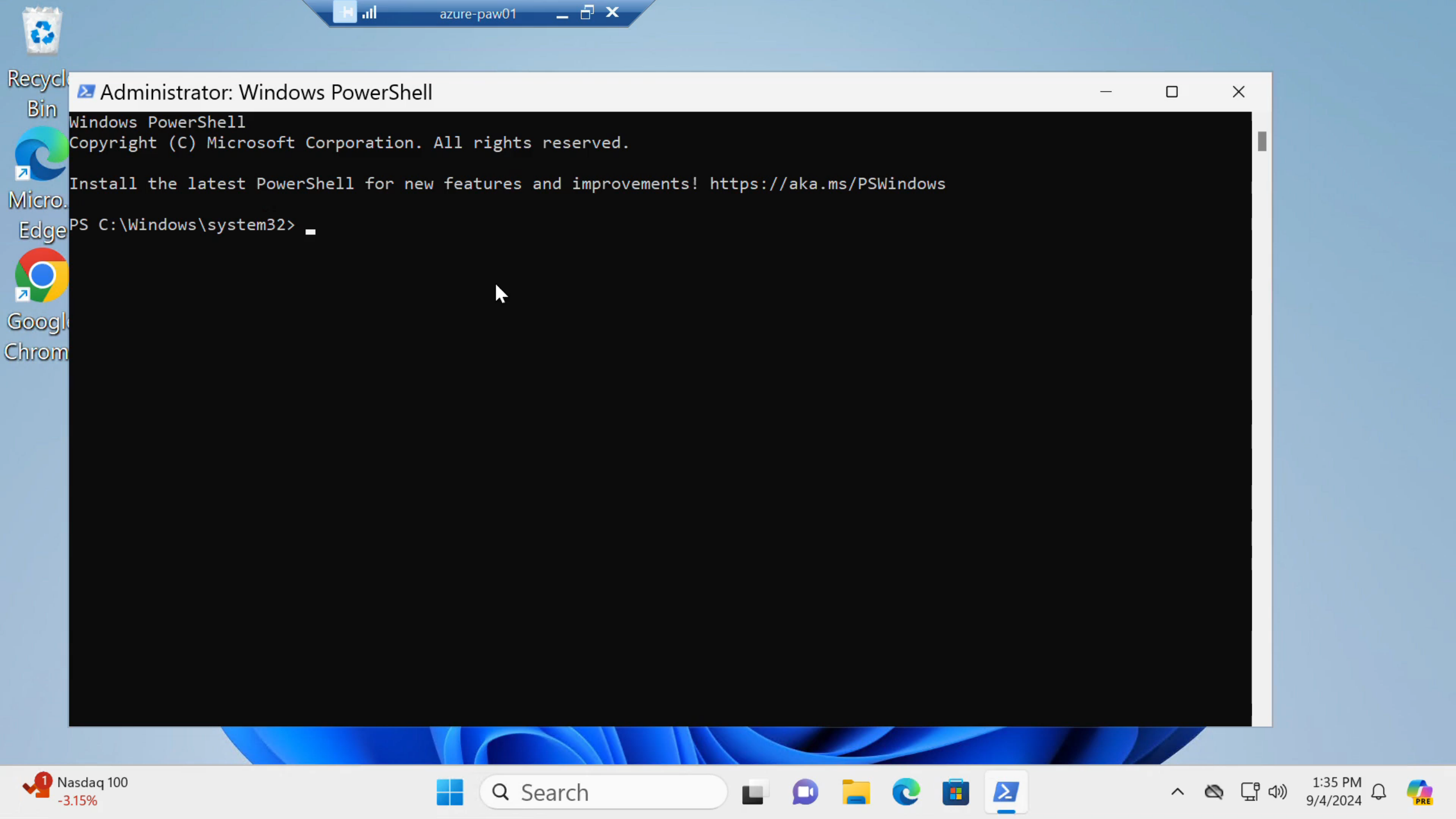

```
mimikatz # ts::mstsc
!!! Warning: false positives can be listed !!!

| PID 5756      mstsc.exe (module @ 0x00000000010DF8F0)

ServerName                              [wstring] 'dc01'
ServerFqdn                              [wstring] ''
UserSpecifiedServerName                 [wstring] 'dc01'
UserName                                [wstring] 'David_DA'
Domain                                  [wstring] 'ALEFDEMO'
Password                                [protect]
SmartCardReaderName                     [wstring] ''
PasswordContainsSCardPin                [ bool  ] FALSE
ServerNameUsedForAuthentication         [wstring] 'dc01'
RDmiUsername                            [wstring] 'ALEFDEMO\david_da'

mimikatz #
```

Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě

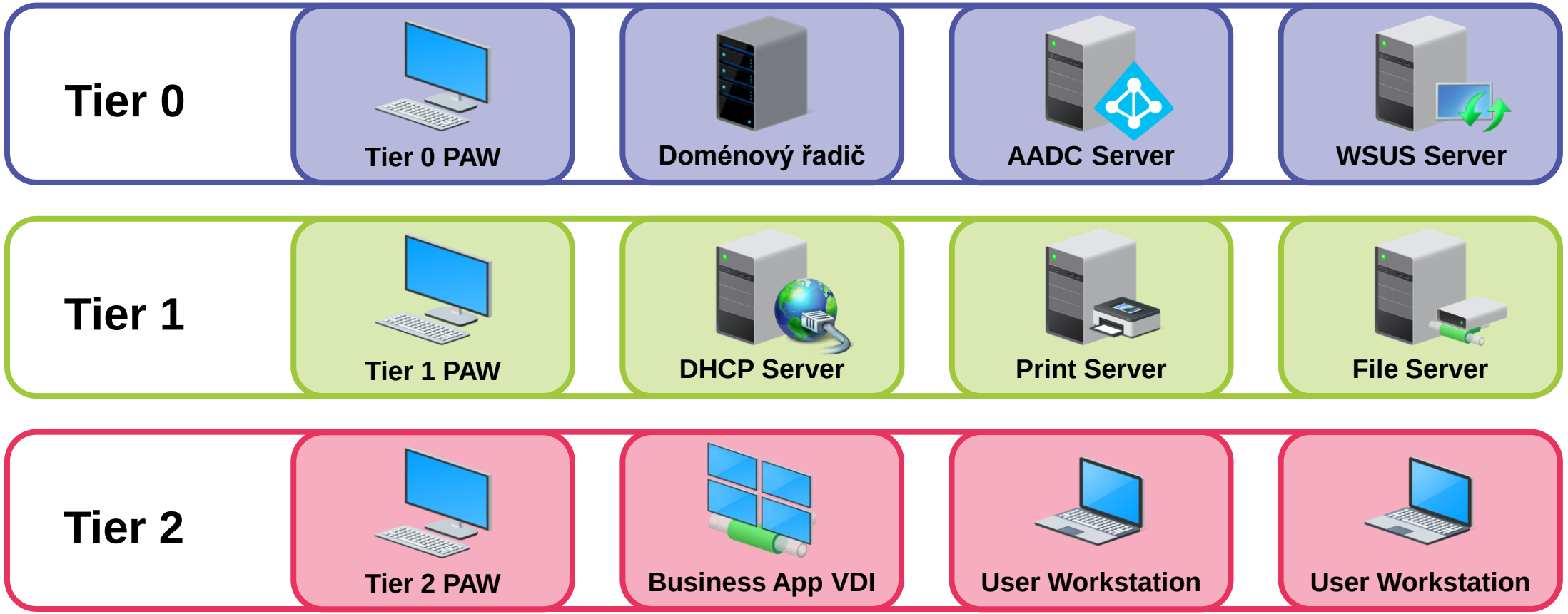
Jak se chránit:
Restricted Admin Mode




azure-paw01
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.
Install the latest PowerShell for new features and improvements! https://aka.ms/PSWindows
PS C:\Windows\system32>
Recycl
Bin
Micro.
Edge
Googl
Chrom
Nasdaq 100
-3.15%
Search
1:35 PM
9/4/2024

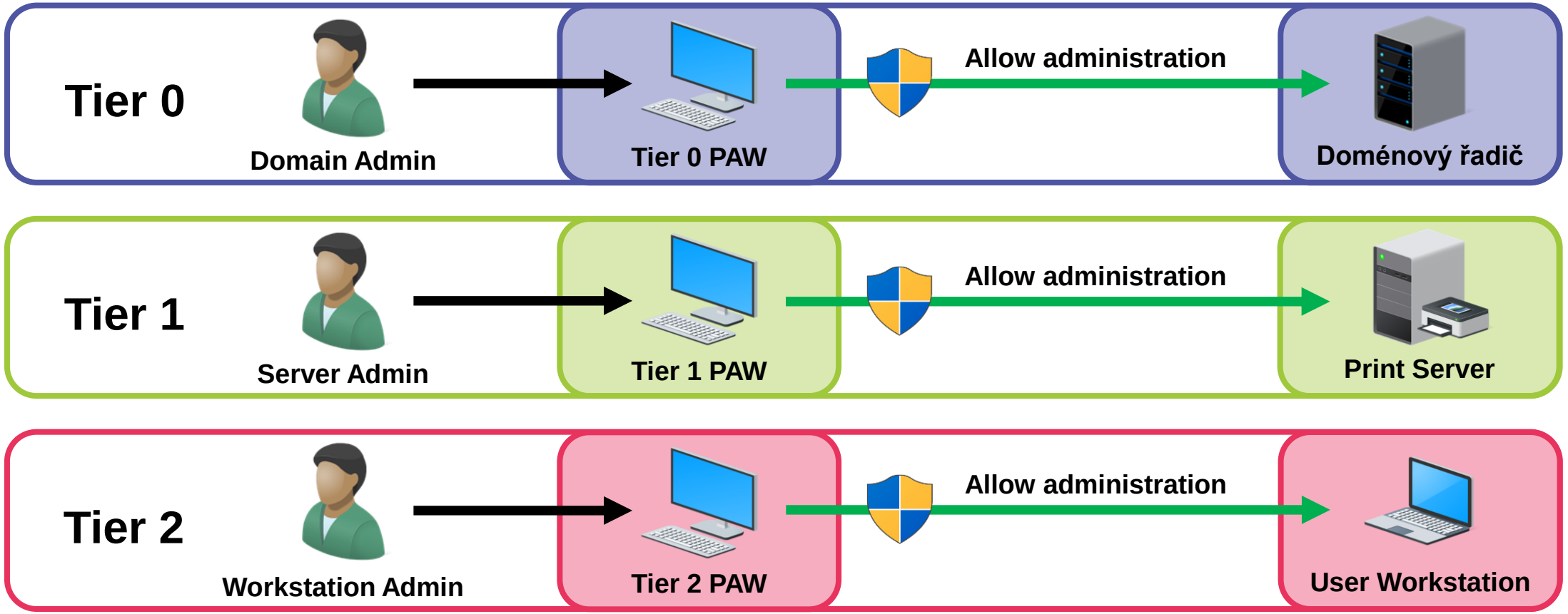
Mitigace

Koncept Tiering – On Premise



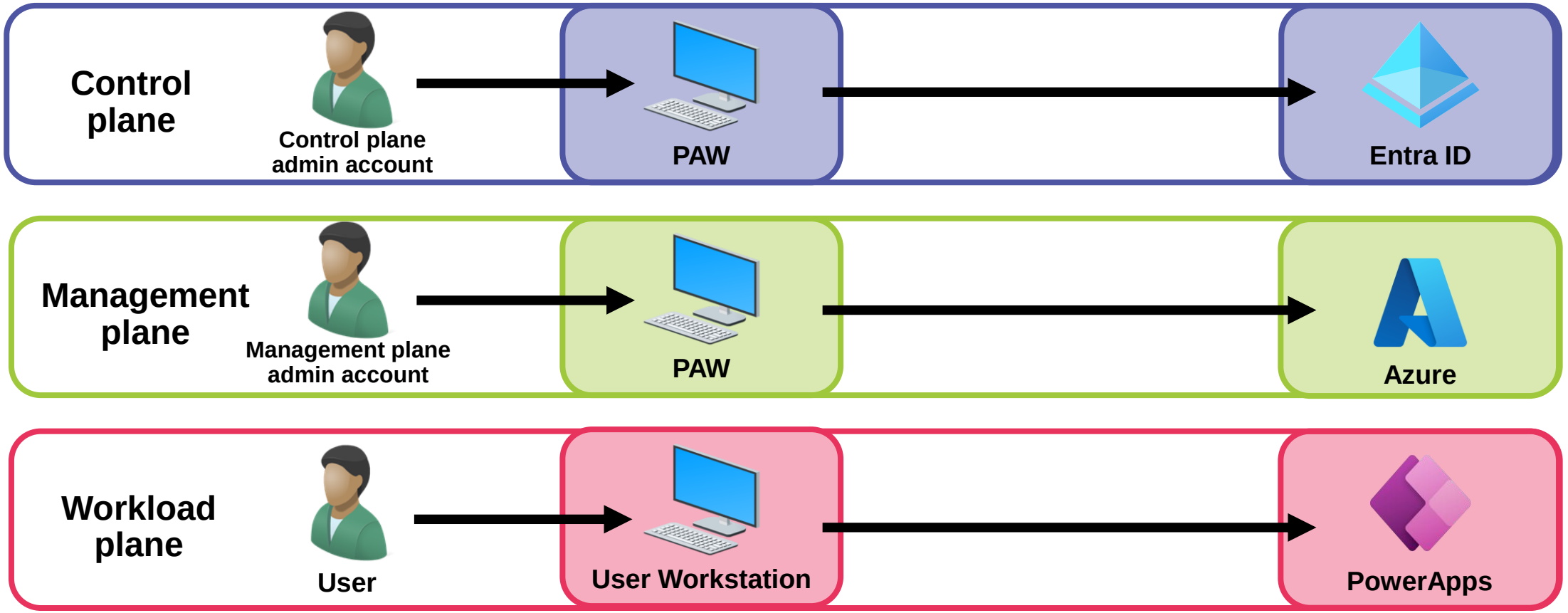
Mitigace

Koncept Tiering – On Premise



Mitigace

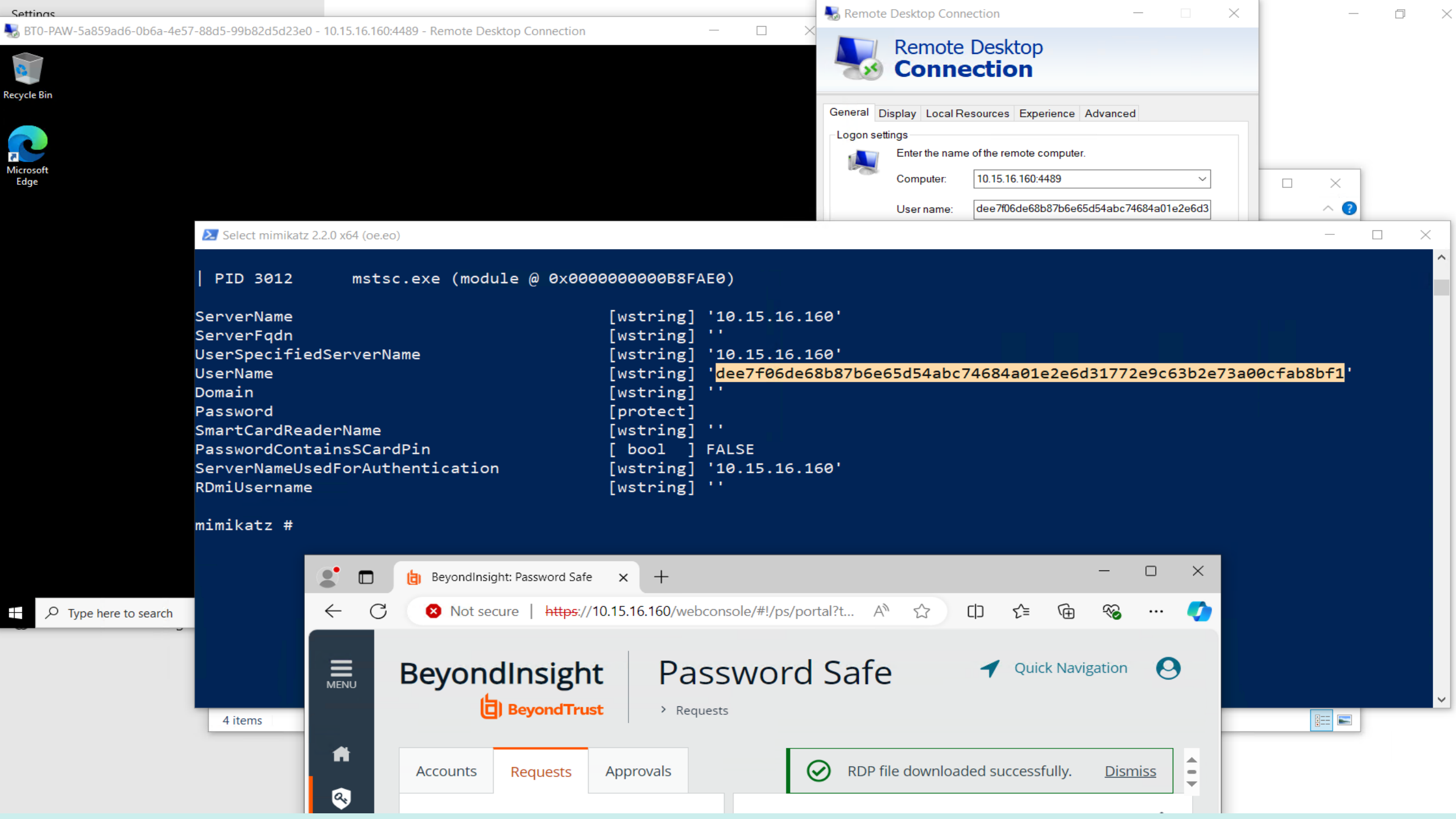
Koncept Tiering – Entra



Mitigace

Privileged Access Management

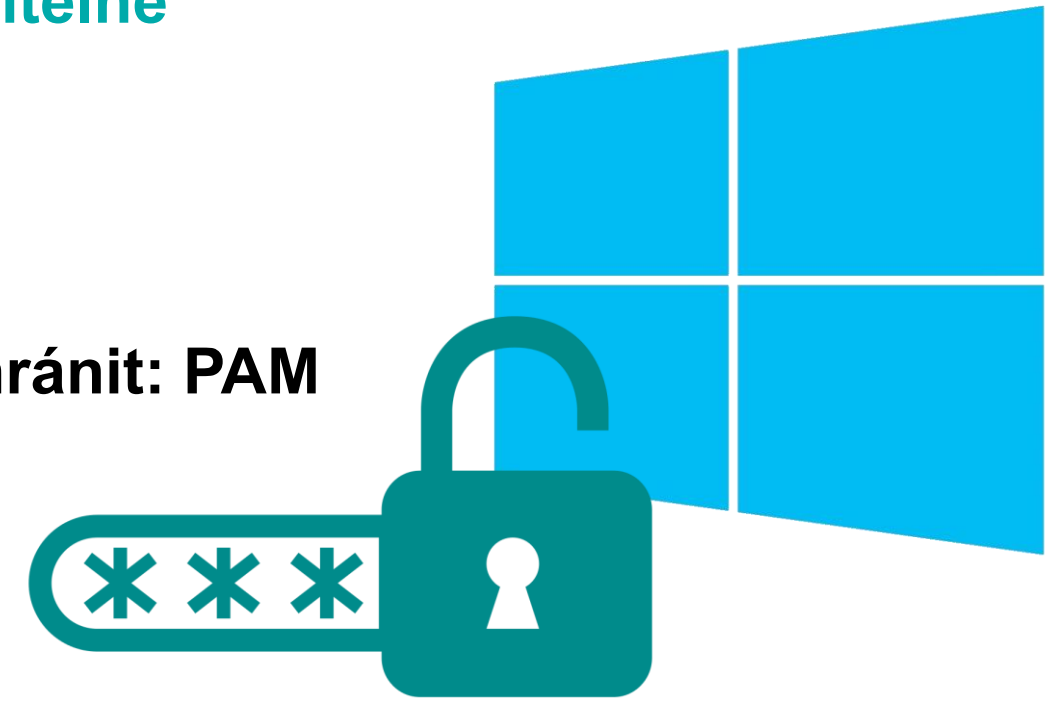
- Automatická změna hesel privilegovaných účtů
- Zabezpečení přístupu k privilegovaným účtům
- Automatizace bezpečnostních přístupů
- Detailní audit používání těchto účtů

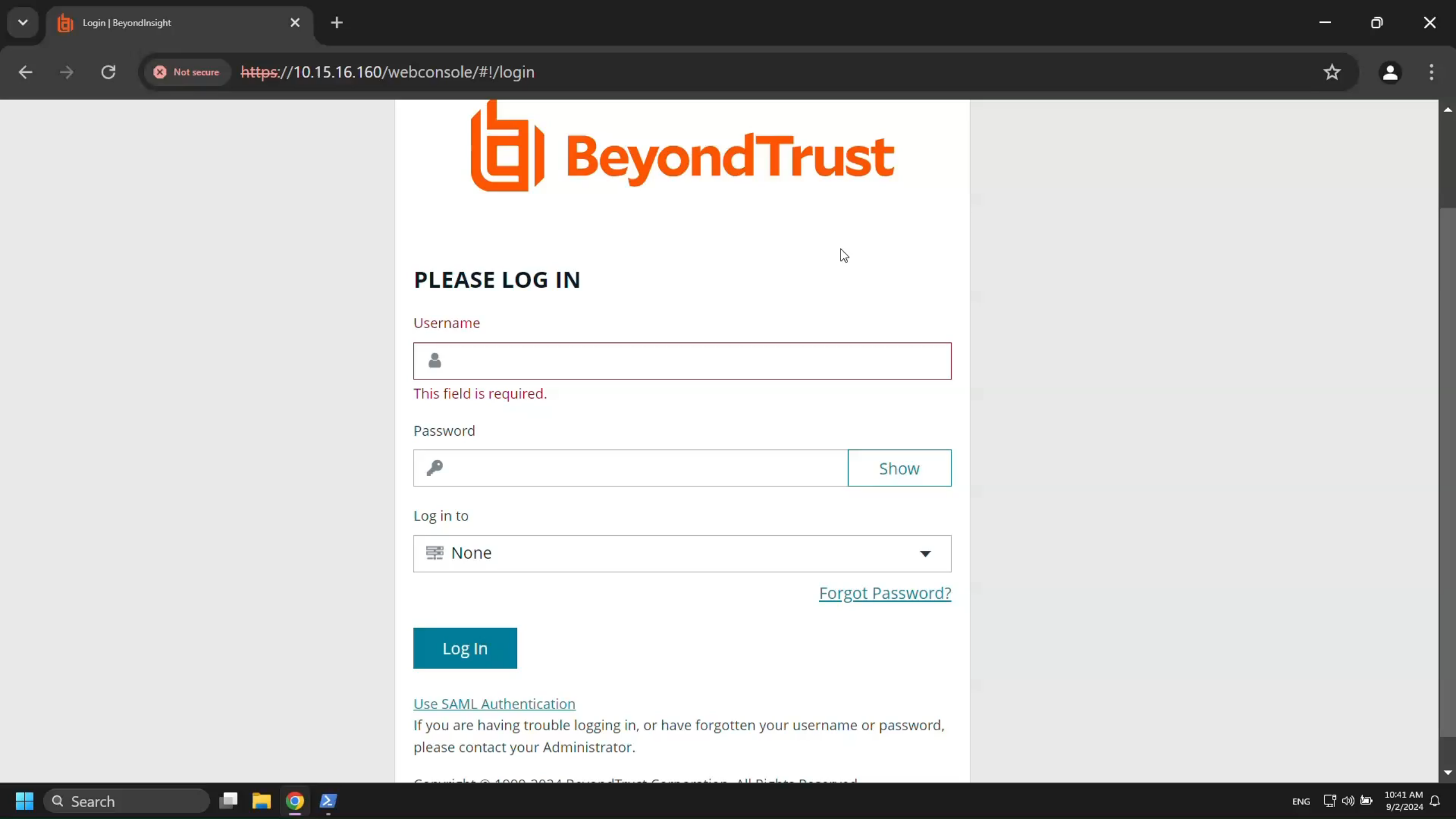

BT0-PAW-5a859ad6-0b6a-4e57-88d5-99b82d5d23e0 - 10.15.16.160:4489 - Remote Desktop Connection
Recycle Bin
Microsoft Edge
Remote Desktop Connection
Remote Desktop Connection
General
Display
Local Resources
Experience
Advanced
Logon settings
Enter the name of the remote computer.
Computer:
10.15.16.160:4489
User name:
dee7f06de68b87b6e65d54abc74684a01e2e6d3
Select mimikatz 2.2.0 x64 (oe.eo)
| PID 3012 mstsc.exe (module @ 0x0000000000B8FAE0)
ServerName [wstring] '10.15.16.160'
ServerFqdn [wstring] ''
UserSpecifiedServerName [wstring] '10.15.16.160'
UserName [wstring] 'dee7f06de68b87b6e65d54abc74684a01e2e6d31772e9c63b2e73a00cfab8bf1'
Domain [wstring] ''
Password [protect]
SmartCardReaderName [wstring] ''
PasswordContainsSCardPin [bool] FALSE
ServerNameUsedForAuthentication [wstring] '10.15.16.160'
RDmiUsername [wstring] ''
mimikatz #
Type here to search
4 items
BeyondInsight: Password Safe
Not secure | https://10.15.16.160/webconsole/#!/ps/portal?t...
MENU
BeyondInsight
BeyondTrust
Password Safe
Requests
Quick Navigation
Accounts
Requests
Approvals
RDP file downloaded successfully.
Dismiss

Vzdálený přístup

DEMO – ochrana před hesly v čitelné podobě

Jak se chránit: PAM




Login | BeyondInsight
Not secure
https://10.15.16.160/webconsole/#!/login
BeyondTrust
PLEASE LOG IN
Username
This field is required.
Password
Show
Log in to
None
Forgot Password?
Log In
Use SAML Authentication
If you are having trouble logging in, or have forgotten your username or password, please contact your Administrator.
Search
ENG
10:41 AM
9/2/2024

Závěr

- Vzdálená správa má svá rizika i ve velmi dobře zabezpečených infrastrukturách
- Implementace doporučených opatření je klíčová
  - Restricted admin
  - Tiering model
  - Privileged access workstation

Děkuji za pozornost

ALEF

David Buřínský
Systems Engineer

David.burinsky@alef.com
www.alef.com

ALEF NULA, a.s.
Pernerova 691/42
186 00 Praha 8
Czech Republic