
18
Win ays
Technology
Microsoft

Microsoft

Keep calm and secure Windows Server

Vladimir Stefanović
Superadmins - Belgrade

Who am I

- Vladimir Stefanović
- System Engineer @Superadmins
- Techical Trainer @ATC
- MCSA, MCSE, MCT, IAMCT Regional Lead, Speaker
- vladimir@superadmins.com
- www.tech-trainer.info

Windays 18

Microsoft

Agenda

- Security stats and approach
- Can we harden Windows and how
- Other tehniques and solutions
- Q & A

Security stats and approach

Traditional vs. Modern defense approach

Traditional

- *I'm not a target*
- *Attack can come only from outside*

Modern

- *Protect*
- *Detect*
- *Respond*

Attack Vectors

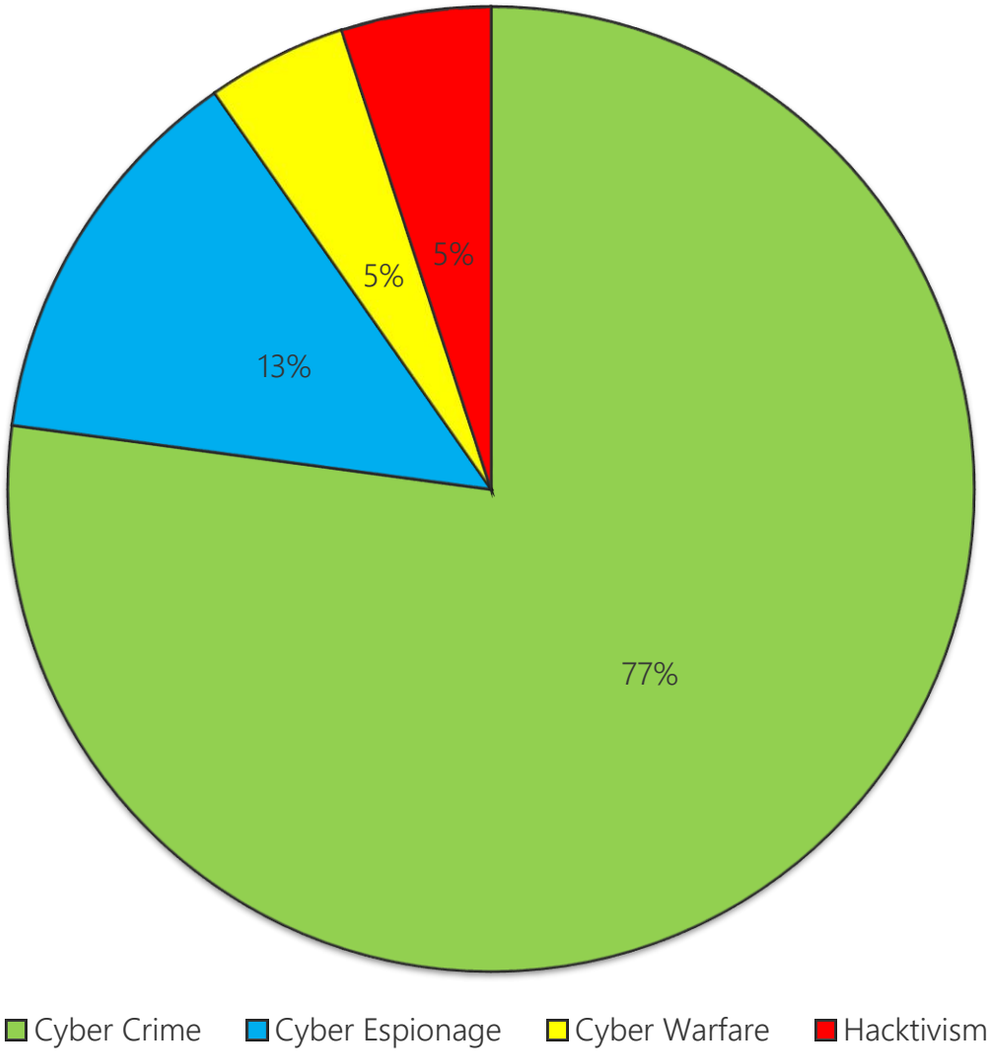
Threats

- *Compromise privileged accounts*
- *Exploit unpatched vulnerabilities*
- *Phishing attacks*
- *Malware infections (ransomware, trojans, logic bombs…)*

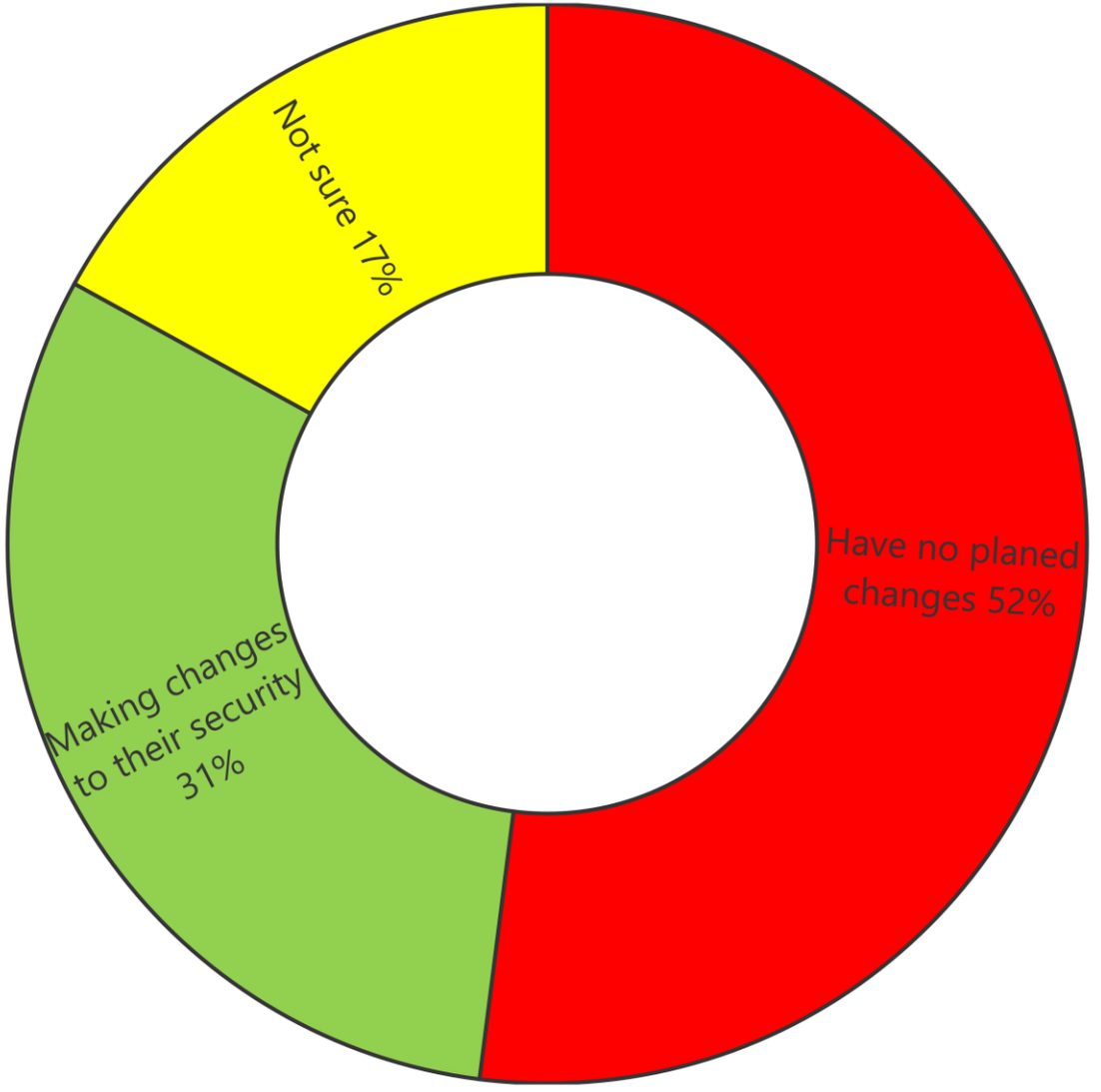
Motives for attack

- *Profit*
  - *By selling data*
  - *By ransoming data*
- *Destroying infrastructure*

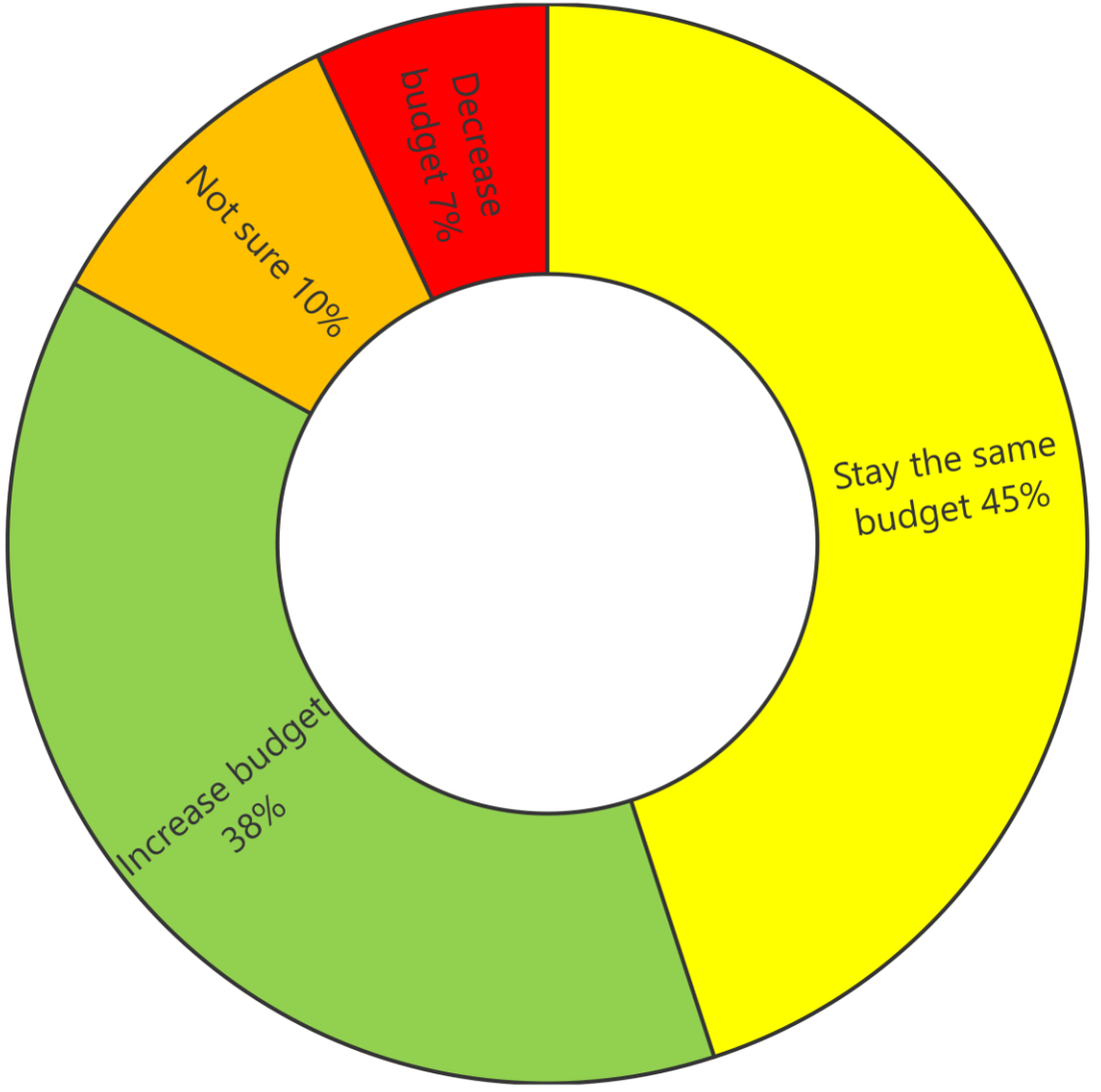
Statistics 2017 - Attack motives



Statistics 2017 - After attack plans



Statistics 2017 - After attack budget



Can we harden Windows infrastructure, and how?

LAPS - Overview

- Local administrator passwords are unique on each computer
- LAPS randomizes and changes local administrator passwords
- LAPS stores local administrator passwords and secrets securely inside active directory
- Access to passwords is configurable

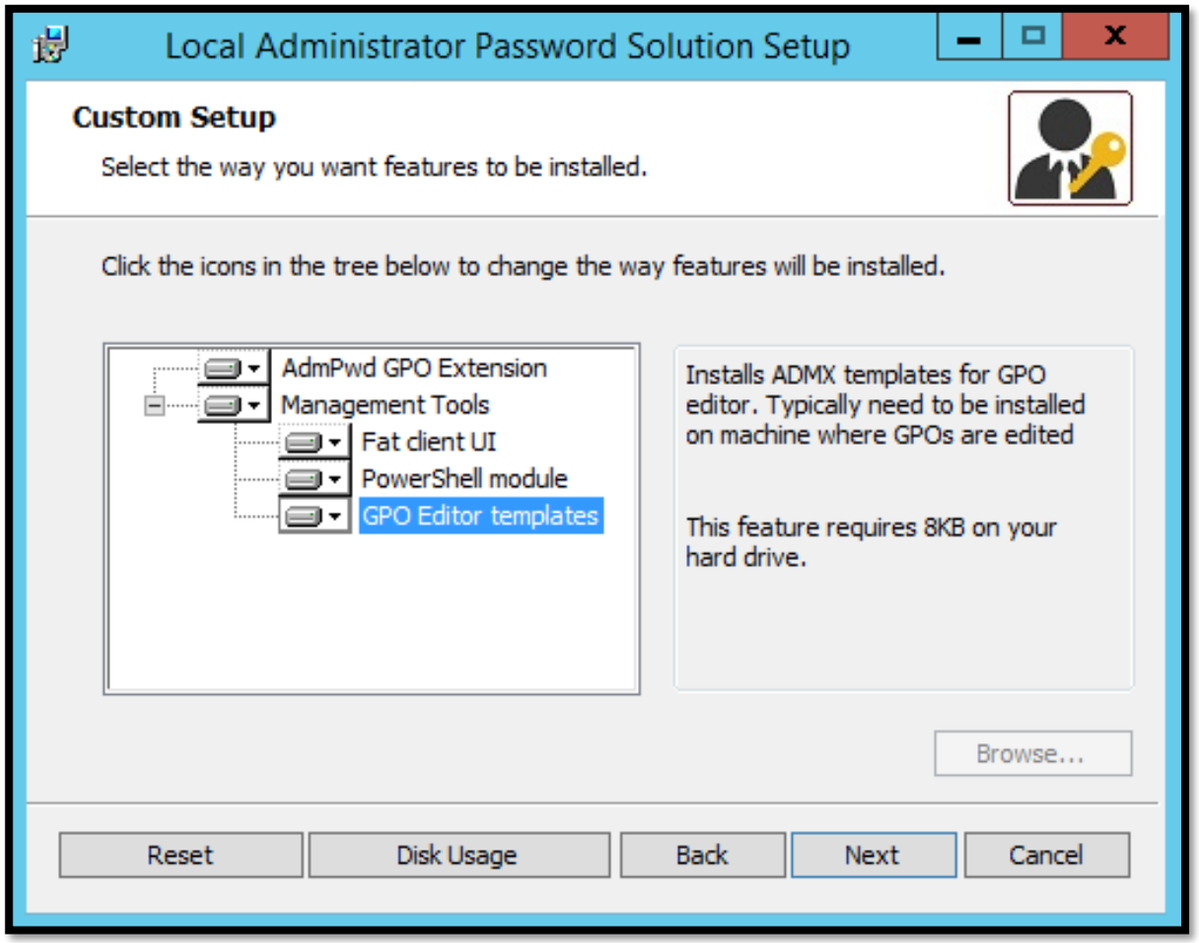
LAPS - Requirements

- Any domain member computer *(server or client)*
- Domain Functional level 2003 or higher
- AD Schema must be extended to use LAPS
- LAPS client on managed computers
- .NET Framework 4.0
- Windows PowerShell 2.0 or later

LAPS - Configuring and managing

- Install LAPS on management server
- Extend schema by PowerShell command
  - *msMcsAdmPwd and msMcsAdmPwdExpirationTime*
- Configure permissions for LAPS client computers
- Install LAPS client on desired computers *(manually or GPO)*
- Configure LAPS with GPO
  - *Enabling LAPS*
  - *Password complexity, length, expiration*

LAPS - Screenshots



LAPS - Screenshots

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.
```

```
PS C:\Windows\system32> Import-Module AdmPwd.PS
PS C:\Windows\system32> Update-AdmPwdADSchema

Operation           DistinguishedName                                              Status
---------           -----------------                                              ------
AddSchemaAttribute  cn=ms-Mcs-AdmPwdExpirationTime,CN=Schema,CN=Configuration,DC=t... Success
AddSchemaAttribute  cn=ms-Mcs-AdmPwd,CN=Schema,CN=Configuration,DC=tech-trainer,DC... Success
ModifySchemaClass   cn=computer,CN=Schema,CN=Configuration,DC=tech-trainer,DC=info   Success
```

```
PS C:\Windows\system32> Set-AdmPwdComputerSelfPermission -Identity Servers

Name                DistinguishedName                                              Status
----                -----------------                                              ------
Servers             OU=Servers,OU=TechTrainer,DC=tech-trainer,DC=info              Delegated
```

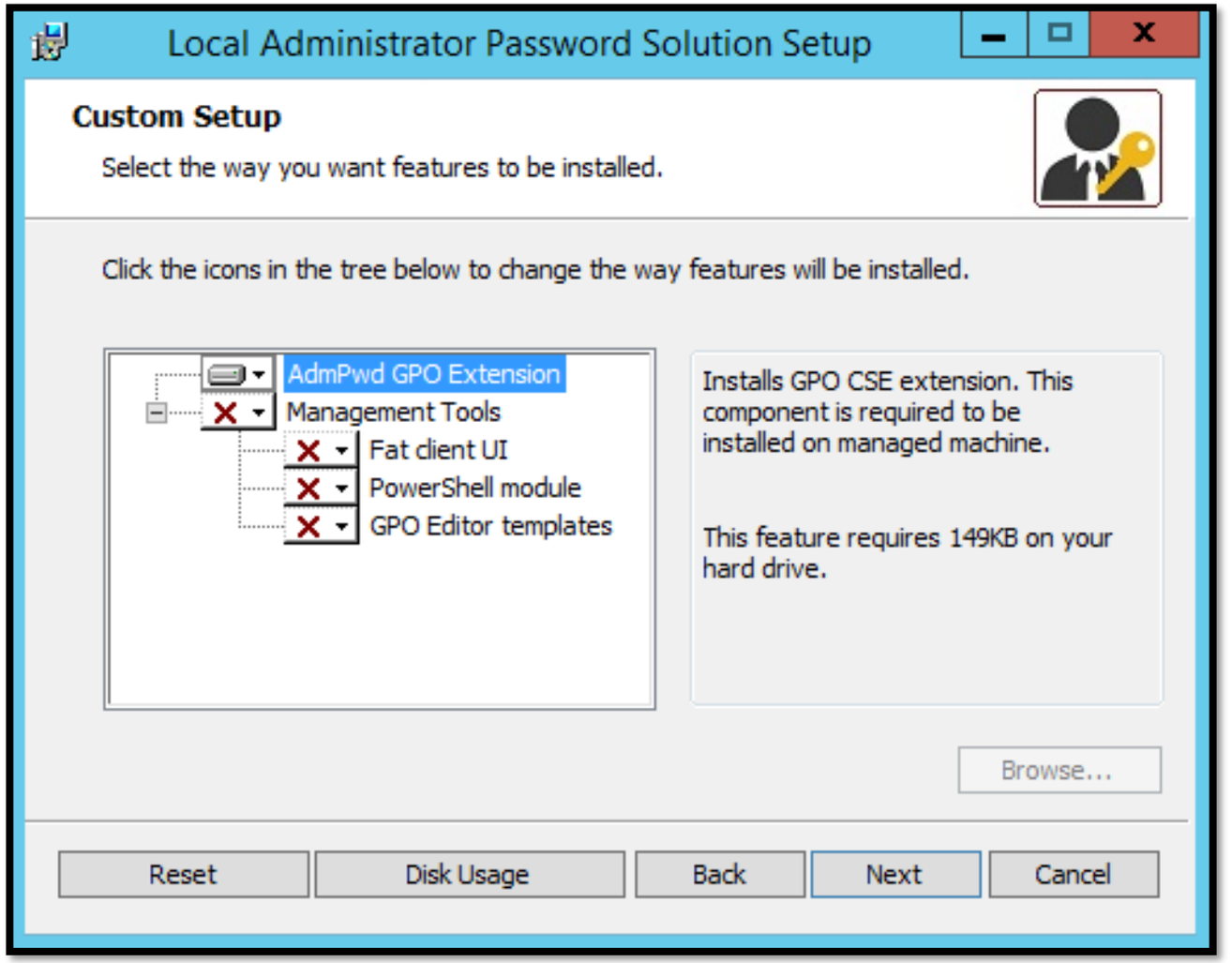
```
PS C:\Windows\system32> Set-AdmPwdReadPasswordPermission -OrgUnit Servers -AllowedPrincipals "Domain-Admins"

Name                DistinguishedName                                              Status
----                -----------------                                              ------
Servers             OU=Servers,OU=TechTrainer,DC=tech-trainer,DC=info              Delegated
```

```
PS C:\Windows\system32> Set-AdmPwdResetPasswordPermission -OrgUnit Servers -AllowedPrincipals "Domain-Admins"

Name                DistinguishedName                                              Status
----                -----------------                                              ------
Servers             OU=Servers,OU=TechTrainer,DC=tech-trainer,DC=info              Delegated
```

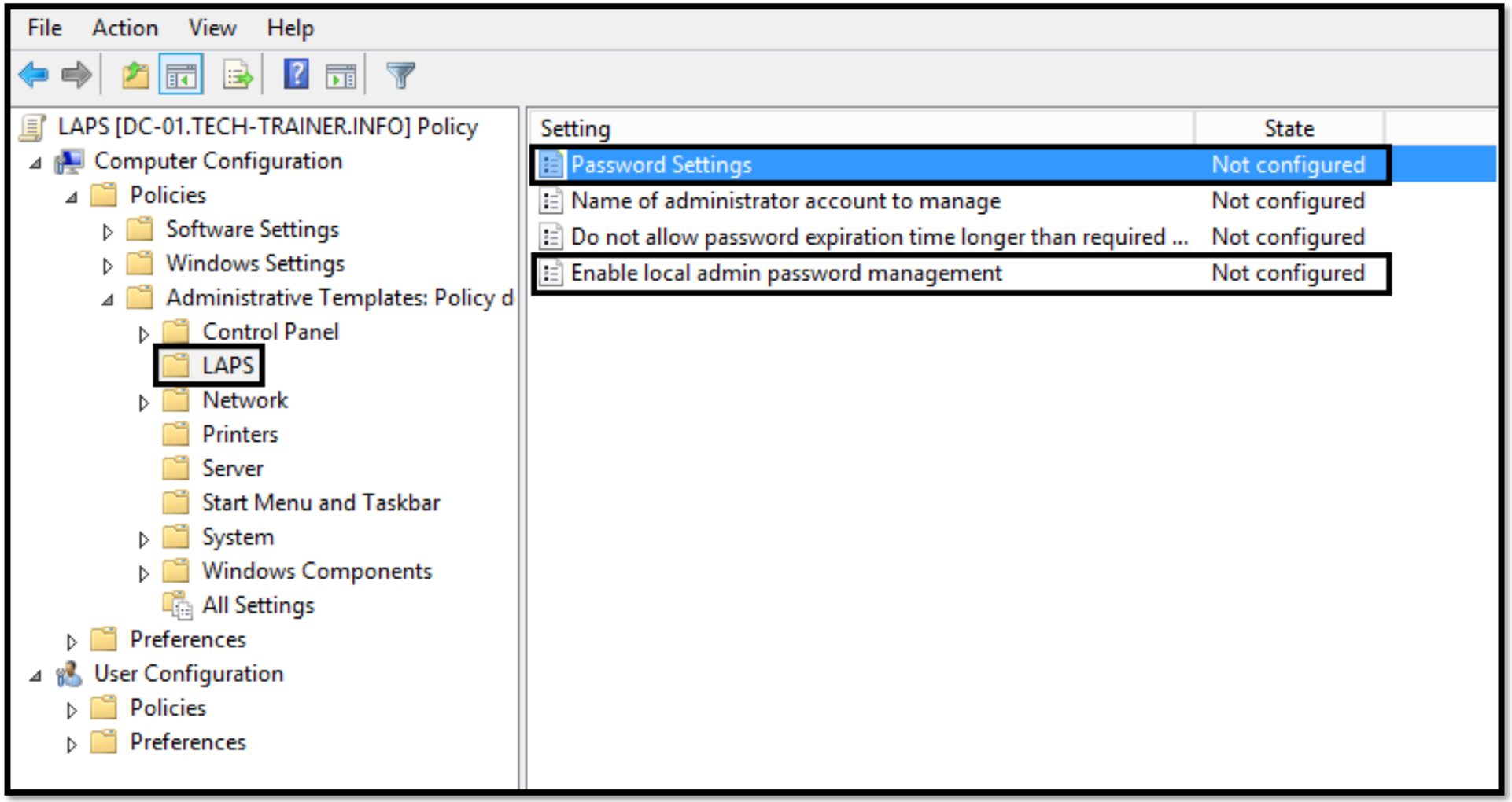
```
PS C:\Windows\system32>
```

Windays 18

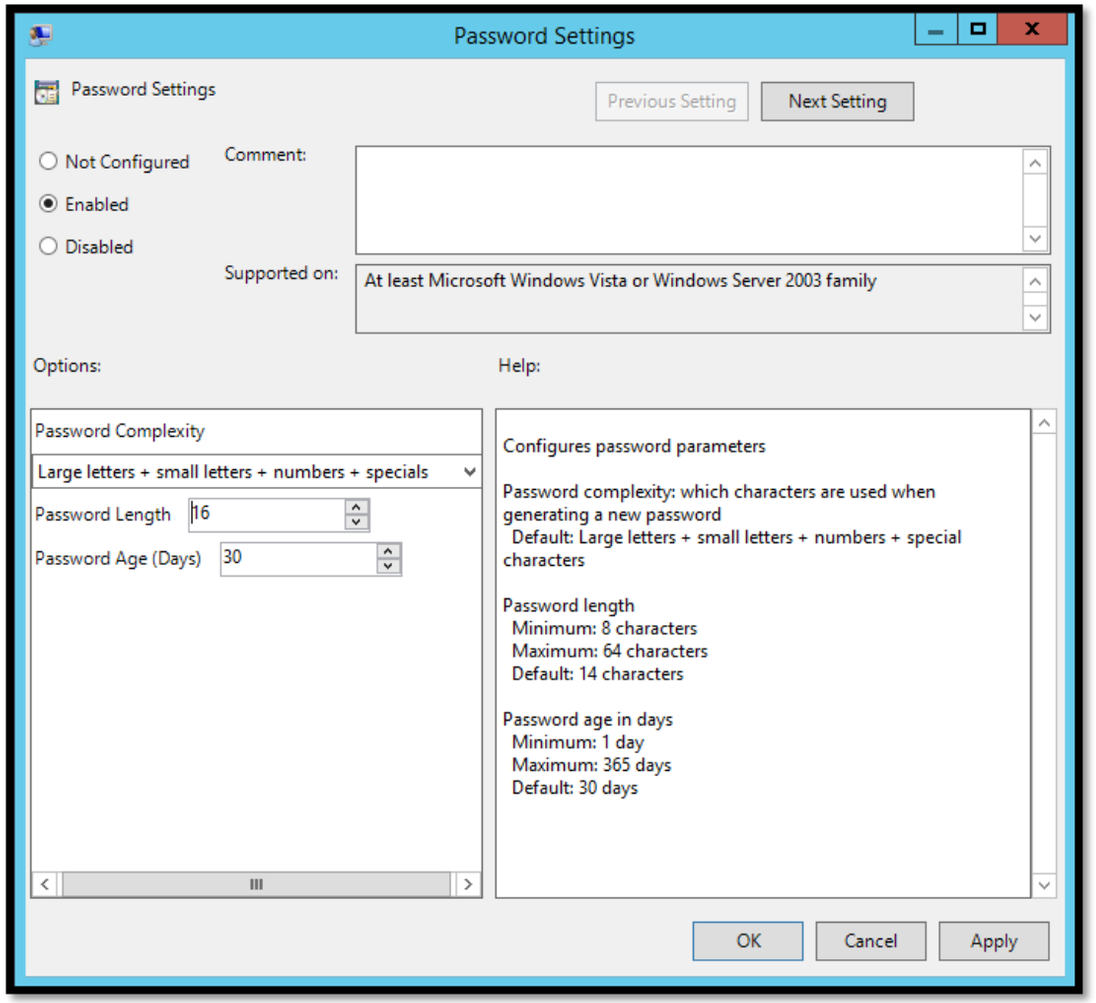
LAPS - Screenshots

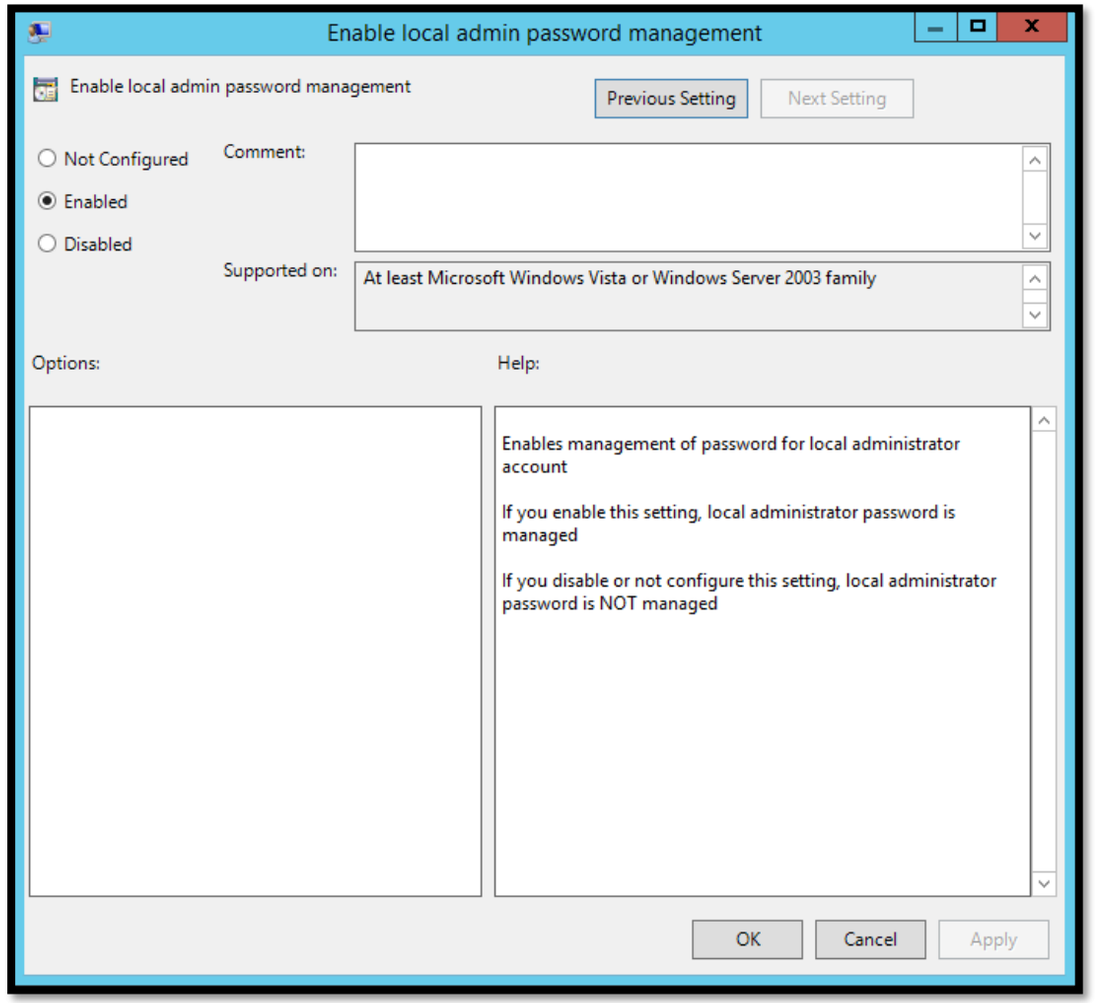


LAPS - Screenshots



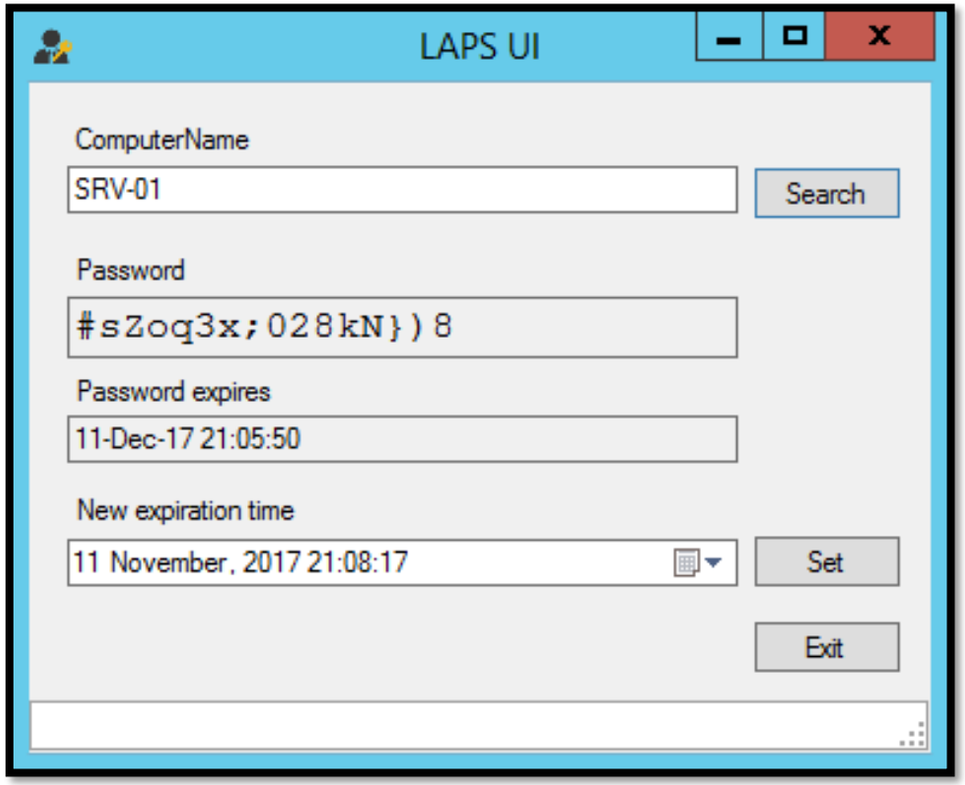
LAPS - Screenshots





LAPS - Screenshots

```
PS C:\Windows\system32> Get-AdmPwdPassword -ComputerName SRV-01 | Format-Table

ComputerName          DistinguishedName                                Password          ExpirationTimestamp
------------          -----------------                                --------          -------------------
SRV-01                CN=SRV-01,OU=Servers,OU=TechTrainer,DC=tec... #sZoq3x;028kN})8   25-Nov-17 21:09:08


PS C:\Windows\system32>
```



JEA – Just Enough Administration

- JEA provides RBAC on Windows PowerShell remoting
- The endpoint limits the user to use predefined PowerShell cmdlets, parameters, and parameter values
- Actions are performed by using a special machine local virtual account
- Native support in Windows Server 2016 and Windows 10
- Supported on other operating systems with installed WMF 5.0

JEA – Disadvantages

- Not suitable for troubleshooting tasks
- Setup requires understanding precisely which cmdlets, parameters, aliases, and values are needed to perform specific tasks
- JEA works only with Windows PowerShell sessions
- User must be familiar with PowerShell

JEA - Configuring

- Create role-capability file(s)
  - *Configure visible cmdlets*
  - *Configure visible functions*
  - *Configure visible external commands*
- Create session-configuration file(s)
  - *Configure role defitinions*
- Creating JEA endpoint / Register session-configuration file(s)
- Connect to JEA endpoint
  - *Enter-PSSession -ComputerName $ -ConfigurationName $*

JEA - Screenshots

```powershell
# Set location for creating modules and create appropriate folder
Set-Location 'C:\Program Files\WindowsPowerShell\Modules'
New-Item -Name HelpDeskJEA -ItemType Directory
Set-Location .\HelpDeskJEA

# Creating new module manifest
New-ModuleManifest .\HelpDeskJEA.psd1

# Create folder and new empty role capability file
New-Item -Name RoleCapabilities -ItemType Directory
Set-Location .\RoleCapabilities
New-PSRoleCapabilityFile -Path .\HelpDeskJEA.psrc

# Edit Role Capability file
ISE HelpDeskJEA.psrc

# Create session configuration file
New-PSSessionConfigurationFile -Path .\HelpDeskJEA.pssc -Full

# Edit session configuration file
ISE HelpDeskJEA.pssc

# Create JEA endpoint
Register-PSSessionConfiguration -Name HelpDeskJEA -Path .\HelpDeskJEA.pssc
Restart-Service WinRM

# Check PS Session Configuration
Get-PSSessionConfiguration
```

JEA - Screenshots

- Edit role-capability file

```
VisibleCmdlets = 'Restart-Computer', 'Get-NetIPAddress'

VisibleCmdlets = @{ Name = 'Restart-Computer'; Parameters = @{ Name = 'Name' }}

VisibleCmdlets = @{ Name = 'Restart-Service'; Parameters = @{ Name = 'Name'; ValidateSet = 'Dns', 'Spooler' }},
                 @{ Name = 'Start-Website'; Parameters = @{ Name = 'Name'; ValidatePattern = 'HR_*' }}

VisibleExternalCommands = 'C:\Windows\System32\whoami.exe'
```

- Edit session-configuration file

```
SessionType = 'RestrictedRemoteServer'

RunAsVirtualAccount = $true

RoleDefinitions = @{ 'Tech-Trainer\Help Desk' = @{ RoleCapabilities = 'HelpDeskJEA' };}
```

JEA - Screenshots

```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Enter-PSSession -ComputerName DC-01
[DC-01]: PS C:\Users\vladimir\Documents> Whoami
tech-trainer\vladimir
[DC-01]: PS C:\Users\vladimir\Documents> (Get-Command).count
1735
[DC-01]: PS C:\Users\vladimir\Documents> _
```

JEA - Screenshots

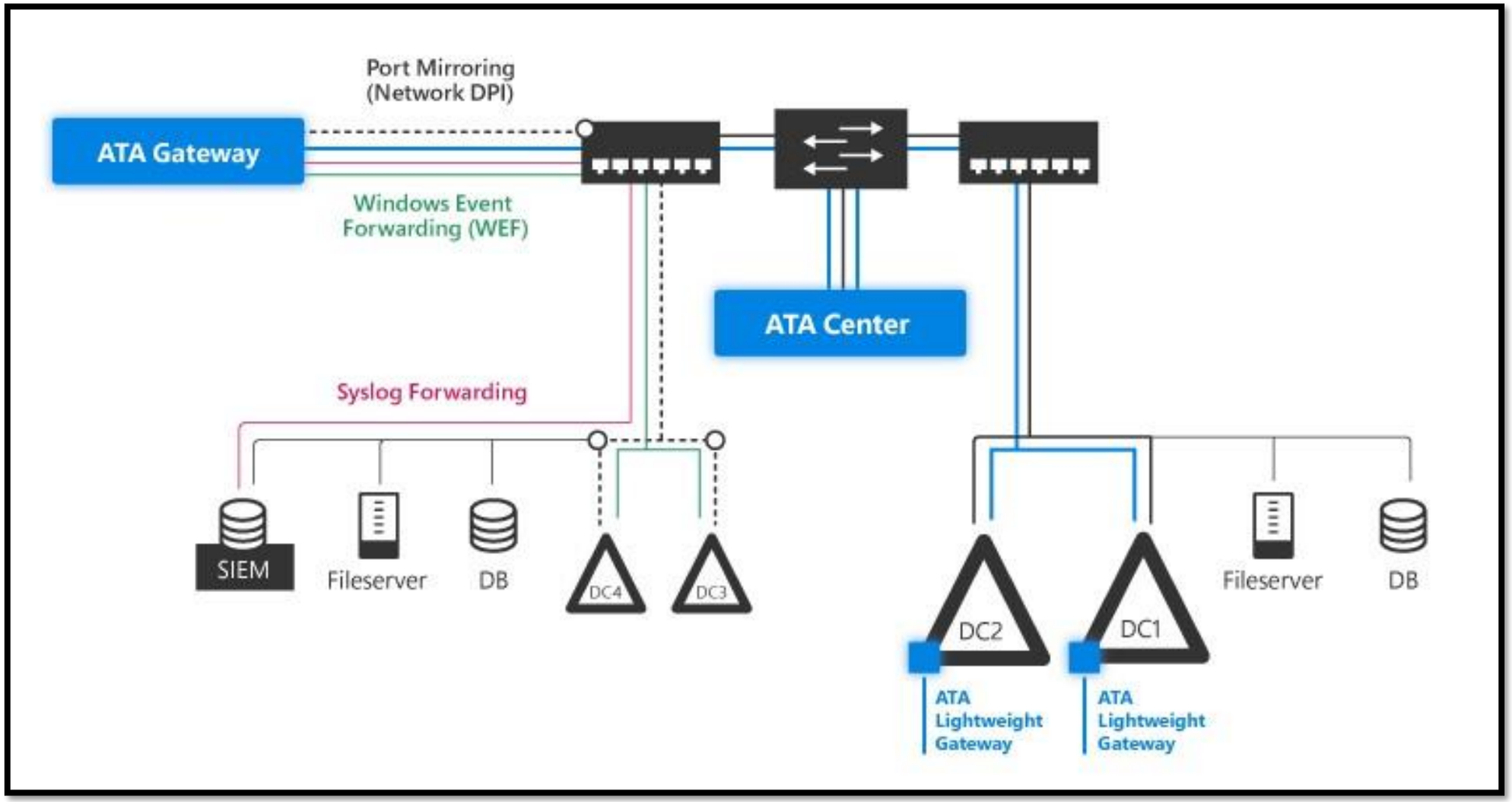
```
Windows PowerShell
Copyright (C) 2014 Microsoft Corporation. All rights reserved.

PS C:\Users\helpdesk> Enter-PSSession -ComputerName DC-01
Enter-PSSession : Connecting to remote server DC-01 failed with the following error message : Access is denied. For
more information, see the about_Remote_Troubleshooting Help topic.
At line:1 char:1
+ Enter-PSSession -ComputerName DC-01
+ ~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
    + CategoryInfo          : InvalidArgument: (DC-01:String) [Enter-PSSession], PSRemotingTransportException
    + FullyQualifiedErrorId : CreateRemoteRunspaceFailed

PS C:\Users\helpdesk> Enter-PSSession -ComputerName DC-01 -ConfigurationName HelpDeskJEA
[DC-01]: PS>whoami
winrm virtual users\winrm va_2_tech-trainer_helpdesk
[DC-01]: PS>(Get-Command).count
10
[DC-01]: PS>Get-Command

CommandType     Name                                               Version    Source
-----------     ----                                               -------    ------
Function        Clear-Host
Function        Exit-PSSession
Function        Get-Command
Function        Get-FormatData
Function        Get-Help
Function        Get-NetIPAddress                                   1.0.0.0    NetTCPIP
Function        Measure-Object
Function        Out-Default
Function        Select-Object
Cmdlet          Restart-Computer                                   3.0.0.0    Microsoft.PowerShell.Management


[DC-01]: PS>
```

Other techniques and solutions

ATA - Advanced Threat Analitycs

- Analyze ➔ Learns ➔ Detect ➔ Alert
- ATA is an Network Intrusion Detection System
- Prevents all known signature-based attacks
- Perform behavior-based detection and learn user behavior
- Provides recommendations for investigation for each identified suspicious activity or known attack

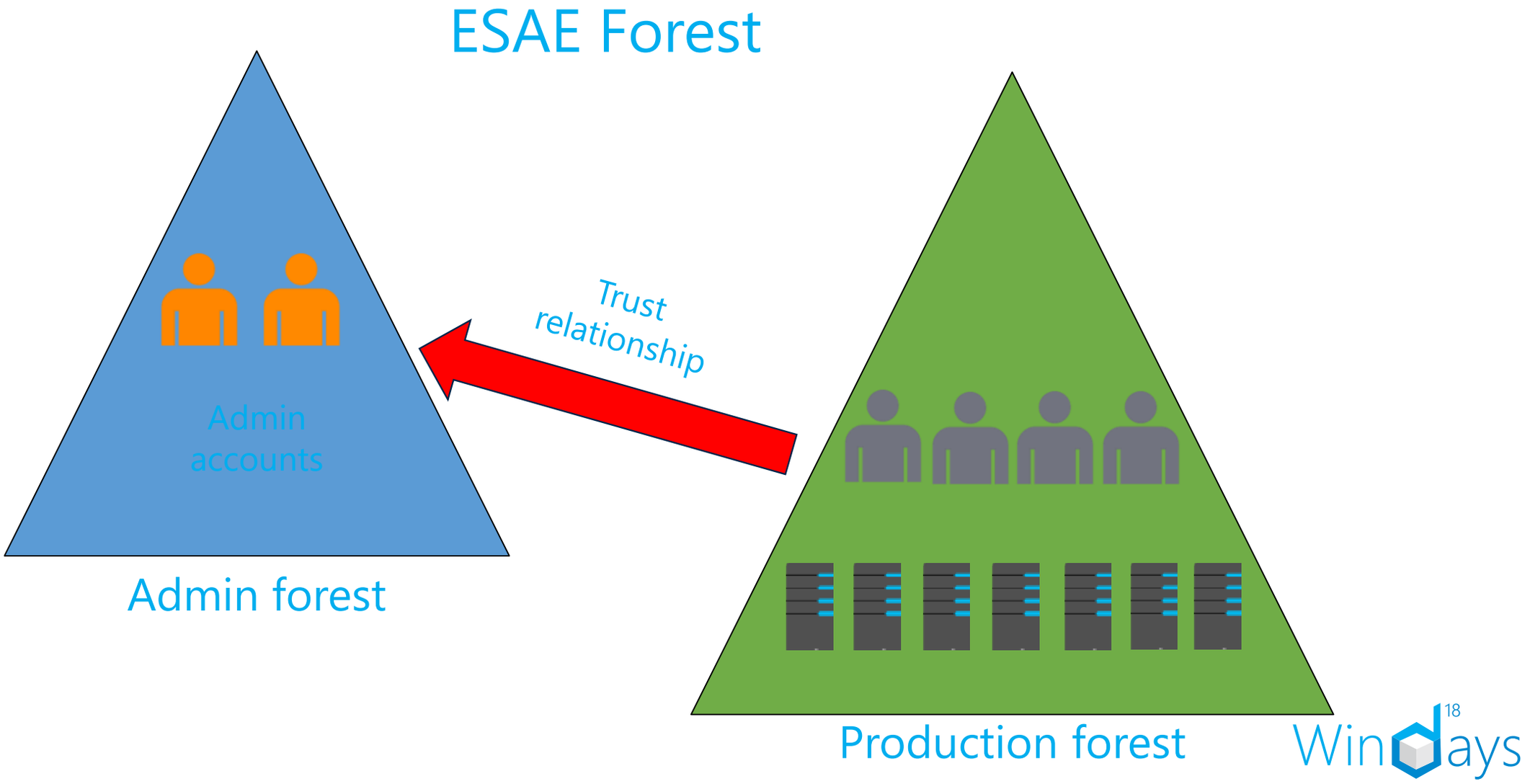
ATA - Advanced Threat Analitycs



Enhanced Security Admin Environment

- The ESAE forest should be a single-domain AD forest
- ESAE forest **should** contain only admin accounts for the production forest
- Applications or additional resources **should't** be deployed in the ESAE forest
- One way forest trust **must** exists - Production forest trusts the ESAE forest

Enhanced Security Admin Environment



Other techniques and solutions

- Enhanced Mitigation Experience Toolkit
- Just In Time and Privileged Access Management
- Shielded VMs
- App Locker
- . . .

We must not forget
a.k.a. Oldie Goldie principles

Oldie goldie

- System patching (manually, WSUS, SCCM)
- Backup (online, onsite, offline)
- Backup testing
- Least privilege
- Separated administrator account
- Password & Kerberos policy
- Disable SMBv1 *(be careful, sensitive task)*
- Disable NTLM *(be careful)*

Q & A

Thank you for your attention

Windays 18

Technology

Microsoft