# Table of content

Table of content 1

1. General Information - Forest Summary 4

a. General Information - Forest Sites 5

b. General Information - Subnets 5

c. General Information - Site Links 5

2. General Information - Domain ad.evotec.pl 6

a. General Information - Domain Summary 6

b. General Information - Domain Well Known Folders 6

c. General Information - Domain Controllers 6

d. General Information - Password Policies 6

e. General Information - Fine-grained Password Policies 7

f. General Information - Group Policies 7

g. General Information - Group Policies Details 7

h. General Information - DNS A/SRV Records 8

i. General Information - Trusts 8

j. General Information - Organizational Units 8

k. General Information - Priviliged Groups 9

l. General Information - Domain Users in ad.evotec.pl 10

i. General Information - Users Count 10

ii. General Information - Domain Administrators 11

iii. General Information - Enterprise Administrators 11

m. General Information - Computer Objects in ad.evotec.pl 11

i. General Information - Computers 11

ii. General Information - Servers 11

iii. General Information - Unknown Computers 12

n. Domain Password Quality 12

i. Password Quality - Passwords with Reversible Encryption 13

ii. Password Quality - Passwords with LM Hash 13

iii. Password Quality - Empty Passwords 13

iv. Password Quality - Known passwords 13

v. Password Quality - Default Computer Password 13

vi. Password Quality - Password Not Required 13

vii. Password Quality - Non expiring passwords 13

viii. Password Quality - AES Keys Missing 13

ix. Password Quality - Kerberos Pre-Auth Not Required 13

x. Password Quality - Only DES Encryption Allowed 13

xi. Password Quality - Delegatable to Service 13

xii. Password Quality - Groups of Users With Same Password 14

xiii. Password Quality - Leaked Passwords 14

xiv. Password Quality - Statistics 14

3. General Information - Domain ad.evotec.xyz 16

a. General Information - Domain Summary 16

b. General Information - Domain Well Known Folders 16

c. General Information - Domain Controllers 16

d. General Information - Password Policies 16

e. General Information - Fine-grained Password Policies 17

f. General Information - Group Policies 17

g. General Information - Group Policies Details 19

h. General Information - DNS A/SRV Records 22

i. General Information - Trusts 23

j. General Information - Organizational Units 23

k. General Information - Priviliged Groups 24

l. General Information - Domain Users in ad.evotec.xyz 25

i. General Information - Users Count 25

ii. General Information - Domain Administrators 26

iii. General Information - Enterprise Administrators 26

m. General Information - Computer Objects in ad.evotec.xyz 27

i. General Information - Computers 27

ii. General Information - Servers 27

iii. General Information - Unknown Computers 28

n. Domain Password Quality 28

i. Password Quality - Passwords with Reversible Encryption 29

ii. Password Quality - Passwords with LM Hash 29

iii. Password Quality - Empty Passwords 29

iv. Password Quality - Known passwords 30

v. Password Quality - Default Computer Password 30

vi. Password Quality - Password Not Required 30

vii. Password Quality - Non expiring passwords 30

viii. Password Quality - AES Keys Missing 34

ix. Password Quality - Kerberos Pre-Auth Not Required 34

x. Password Quality - Only DES Encryption Allowed 34

xi. Password Quality - Delegatable to Service 34

xii. Password Quality - Groups of Users With Same Password 35

xiii. Password Quality - Leaked Passwords 35

xiv. Password Quality - Statistics 35

This document provides low-level documentation of Active Directory infrastructure in Evotec organization. This document contains general data that has been exported from Active Directory and provides an overview of the whole environment.

# General Information - Forest Summary

Active Directory at Evotec has a forest name ad.evotec.xyz. Following table contains forest summary with important information:

|  |  |
| --- | --- |
| Forest Summary | |
| Name | ad.evotec.xyz |
| Root Domain | ad.evotec.xyz |
| Forest Distingushed Name | DC=ad,DC=evotec,DC=xyz |
| Forest Functional Level | Windows2012R2Forest |
| Domains Count | 2 |
| Sites Count | 2 |
| Domains | ad.evotec.xyz, ad.evotec.pl |
| Sites | KATOWICE-1, KATOWICE-2 |

Following table contains FSMO servers:

|  |  |
| --- | --- |
| FSMO Roles | |
| Domain Naming Master | AD1.ad.evotec.xyz |
| Schema Master | AD1.ad.evotec.xyz |

Following table contains optional forest features:

|  |  |
| --- | --- |
| Optional Features | |
| Recycle Bin Enabled | True |
| Privileged Access Management Feature Enabled | False |
| Laps Enabled | True |

Following UPN suffixes were created in this forest:

|  |  |
| --- | --- |
| UPN Suffixes | |
| ad.evotec.xyz | Primary / Default UPN |
| myneva.eu | Secondary |
| single.evotec.xyz | Secondary |
| newUPN@com | Secondary |
| evotec.xyz | Secondary |
| evotec.pl | Secondary |

No SPN suffixes were created in this forest.

# General Information - Forest Sites

Forest Sites list can be found below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Protected | SubnetsCount | DomainControllersCount |
| KATOWICE-1 | Main location |  | 3 | 0 |
| KATOWICE-2 |  |  | 2 | 5 |

Forest Sites list can be found below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| TopologyCleanupEnabled | TopologyDetectStaleEnabled | TopologyMinimumHopsEnabled | UniversalGroupCachingEnabled | UniversalGroupCachingRefreshSite |
|  |  |  |  |  |
|  |  |  |  |  |

# General Information - Subnets

Table below contains information regarding relation between Subnets and sites

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Protected | Modified | Created |
| 192.168.240.0/24 |  | True | 01/07/2021 13:18:17 | 07/29/2018 20:40:45 |
| 192.168.241.0/24 |  | False | 07/29/2018 20:40:57 | 07/29/2018 20:40:57 |
| 192.168.239.0/24 | This is my site | False | 07/30/2018 15:27:43 | 07/29/2018 23:13:33 |
| 10.0.20.32/32 |  | False | 02/25/2021 11:06:41 | 02/25/2021 11:06:41 |
| 10.0.0.0/8 |  | False | 02/25/2021 11:07:16 | 02/25/2021 11:07:16 |
| 10.0.20.34/32 |  | False | 02/25/2021 12:12:32 | 02/25/2021 12:12:32 |

Table below contains information regarding relation between Subnets and sites

|  |  |
| --- | --- |
| Name | Site |
| 192.168.240.0/24 | CN=KATOWICE-2,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 192.168.241.0/24 |  |
| 192.168.239.0/24 | CN=KATOWICE-1,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 10.0.20.32/32 | CN=KATOWICE-1,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 10.0.0.0/8 | CN=KATOWICE-2,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 10.0.20.34/32 | CN=KATOWICE-1,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |

# General Information - Site Links

Forest Site Links information is available in table below

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Cost | ReplicationFrequencyInMinutes | ReplInterval | ReplicationSchedule |
| DEFAULTIPSITELINK | 100 | 15 | 15 |  |
| ForeignLink | 100 | 15 | 15 |  |

# General Information - Domain ad.evotec.pl

# General Information - Domain Summary

Following domain exists within forest :

* + Domain DC=ad,DC=evotec,DC=pl
    - Name for fully qualified domain name (FQDN): ad.evotec.pl
    - Name for NetBIOS: EVOTECPL

# General Information - Domain Well Known Folders

Following table has defined well known folders:

|  |  |
| --- | --- |
| Well known folders | |
| UsersContainer | CN=Users,DC=ad,DC=evotec,DC=pl |
| ComputersContainer | CN=Computers,DC=ad,DC=evotec,DC=pl |
| DomainControllersContainer | OU=Domain Controllers,DC=ad,DC=evotec,DC=pl |
| DeletedObjectsContainer | CN=Deleted Objects,DC=ad,DC=evotec,DC=pl |
| SystemsContainer | CN=System,DC=ad,DC=evotec,DC=pl |
| LostAndFoundContainer | CN=LostAndFound,DC=ad,DC=evotec,DC=pl |
| QuotasContainer | CN=NTDS Quotas,DC=ad,DC=evotec,DC=pl |
| ForeignSecurityPrincipalsContainer | CN=ForeignSecurityPrincipals,DC=ad,DC=evotec,DC=pl |

# General Information - Domain Controllers

Following table contains domain controllers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Host Name | Operating System | Site | Ipv4 |
| DC1 | DC1.ad.evotec.pl | Windows Server 2019 Standard Evaluation | KATOWICE-2 | 192.168.240.238 |
| ADRODC | ADRODC.ad.evotec.pl | Windows Server 2016 Standard | KATOWICE-2 | 192.168.240.253 |

Following table contains FSMO servers with roles for domain ad.evotec.pl

|  |  |
| --- | --- |
| FSMO Roles for ad.evotec.pl | |
| PDC Emulator | DC1.ad.evotec.pl |
| RID Master | DC1.ad.evotec.pl |
| Infrastructure Master | DC1.ad.evotec.pl |

# General Information - Password Policies

Following table contains password policies for all users within ad.evotec.pl

|  |  |
| --- | --- |
| Default Password Policy for ad.evotec.pl | |
| Complexity Enabled | True |
| Lockout Duration | 30 |
| Lockout Observation Window | 30 |
| Lockout Threshold | 0 |
| Max Password Age | 180 |
| Min Password Length | 10 |
| Min Password Age | 0 |
| Password History Count | 10 |
| Reversible Encryption Enabled | False |
| Distinguished Name | DC=ad,DC=evotec,DC=pl |

# General Information - Fine-grained Password Policies

Following table contains Fine-grained password policies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Complexity Enabled | Lockout Duration | Lockout Observation Window | Lockout Threshold |
| Fine Policy Test | False | 00:30:00 | 00:30:00 | 0 |

# General Information - Group Policies

Following table contains group policies for ad.evotec.pl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Gpo Status | Creation Time | Modification Time | Description |
| DC | Configure Time PDC | UserSettingsDisabled | 09/13/2019 14:39:56 | 12/05/2020 23:44:30 |  |
| Default Domain Policy | UserSettingsDisabled | 07/26/2018 12:59:51 | 12/05/2020 23:44:38 |  |
| Default Domain Controllers Policy | UserSettingsDisabled | 07/26/2018 12:59:51 | 12/05/2020 23:47:46 |  |
| DC | PowerShell Logging | UserSettingsDisabled | 09/13/2019 10:54:24 | 12/05/2020 23:47:50 |  |
| TEST | Empty GPO - AD.EVOTEC.PL CrossDomain GPO | AllSettingsEnabled | 06/17/2020 08:18:36 | 12/04/2020 23:37:32 |  |

# General Information - Group Policies Details

Following table contains group policies for ad.evotec.pl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Links | Has Computer Settings | Has User Settings | User Enabled |
| DC | Configure Time PDC | ad.evotec.pl/Domain Controllers | True | False | false |
| Default Domain Policy | ad.evotec.pl | True | False | false |
| Default Domain Controllers Policy | ad.evotec.pl/Domain Controllers | True | False | false |
| DC | PowerShell Logging | ad.evotec.pl/Domain Controllers | True | False | false |
| TEST | Empty GPO - AD.EVOTEC.PL CrossDomain GPO |  | False | False | true |

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Target | NameTarget | Priority | Weight | Port |
| dc1.ad.evotec.pl | dc1.ad.evotec.pl | 0 | 100 | 88 |
| dc1.ad.evotec.pl | dc1.ad.evotec.pl | 0 | 100 | 389 |

Following table contains A records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Address | IPAddress | IP4Address | Name | Type |
| 192.168.240.238 | 192.168.240.238 | 192.168.240.238 | dc1.ad.evotec.pl | A |
| 192.168.240.238 | 192.168.240.238 | 192.168.240.238 | dc1.ad.evotec.pl | A |

# General Information - Trusts

Following table contains trusts established with domains...

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Trust Source | Trust Target | Trust Direction | Trust Attributes | Trust Status |
| ad.evotec.pl | ad.evotec.xyz | BiDirectional | Within Forest | OK |

# General Information - Organizational Units

Following table contains all OU's created in ad.evotec.pl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Canonical Name | Managed | Manager Email | Protected | Description |
| ad.evotec.pl/Development |  |  | True |  |
| ad.evotec.pl/Domain Controllers |  |  | False | Default container for domain controllers |
| ad.evotec.pl/Production |  |  | False |  |
| ad.evotec.pl/Production/Accounts |  |  | True |  |
| ad.evotec.pl/Production/Accounts/Contacts |  |  | True |  |
| ad.evotec.pl/Production/Accounts/Service |  |  | True |  |
| ad.evotec.pl/Production/Accounts/ServiceAzure |  |  | True |  |
| ad.evotec.pl/Production/Accounts/Special |  |  | True |  |
| ad.evotec.pl/Production/Accounts/SpecialAzure |  |  | True |  |
| ad.evotec.pl/Production/Accounts/Users |  |  | True |  |
| ad.evotec.pl/Production/Accounts/UsersNoSync |  |  | True |  |
| ad.evotec.pl/Production/Devices |  |  | True |  |
| ad.evotec.pl/Production/Devices/Computers |  |  | True |  |
| ad.evotec.pl/Production/Devices/Servers |  |  | True |  |
| ad.evotec.pl/Production/Devices/Servers.Hosts |  |  | True |  |
| ad.evotec.pl/Production/Groups |  |  | True |  |
| ad.evotec.pl/Production/Groups/Delegation |  |  | True |  |
| ad.evotec.pl/Production/Groups/Distibution |  |  | True |  |
| ad.evotec.pl/Production/Groups/O365 |  |  | True |  |
| ad.evotec.pl/Production/Groups/O365/Licenses |  |  | True |  |
| ad.evotec.pl/Production/Groups/O365/WriteBack |  |  | True |  |
| ad.evotec.pl/Production/Groups/Security |  |  | True |  |
| ad.evotec.pl/Production/Groups/Security/NetworkAdministration |  |  | True |  |
| ad.evotec.pl/Production/Groups/Security/NetworkVPNAdmin |  |  | True |  |
| ad.evotec.pl/Production/Groups/Security/NetworkVPNUsers |  |  | True |  |
| ad.evotec.pl/Production/Users |  |  | False |  |

# General Information - Priviliged Groups

Following table contains list of priviliged groups and count of the members in it.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group Name | Group Category | Group Scope | Group SID | High Privileged Group |
| Administrators | Security | DomainLocal | S-1-5-32-544 | True |
| Network Configuration Operators | Security | DomainLocal | S-1-5-32-556 | False |
| Event Log Readers | Security | DomainLocal | S-1-5-32-573 | False |
| Hyper-V Administrators | Security | DomainLocal | S-1-5-32-578 | False |
| Remote Management Users | Security | DomainLocal | S-1-5-32-580 | False |
| Domain Admins | Security | Global | S-1-5-21-3661168273-3802070955-2987026695-512 | True |
| Group Policy Creator Owners | Security | Global | S-1-5-21-3661168273-3802070955-2987026695-520 | False |
| Backup Operators | Security | DomainLocal | S-1-5-32-551 | True |
| Print Operators | Security | DomainLocal | S-1-5-32-550 | True |
| Replicator | Security | DomainLocal | S-1-5-32-552 | True |
| Account Operators | Security | DomainLocal | S-1-5-32-548 | True |
| Server Operators | Security | DomainLocal | S-1-5-32-549 | True |

# General Information - Domain Users in ad.evotec.pl

## General Information - Users Count

Following table and chart shows number of users in its categories

|  |  |
| --- | --- |
| Users Count | |
| Users Count Incl. System | 10 |
| Users Count | 8 |
| Users Expired | 5 |
| Users Expired Incl. Disabled | 7 |
| Users Never Expiring | 1 |
| Users Never Expiring Incl. Disabled | 1 |
| Users System Accounts | 2 |

## General Information - Domain Administrators

Following users have highest priviliges and are able to control a lot of Windows resources.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Name | User Principal Name | Sam Account Name | Email Address |
|  | Administrator |  | Administrator |  |

## General Information - Enterprise Administrators

No Enterprise Administrators users were defined for this domain.

# General Information - Computer Objects in ad.evotec.pl

## General Information - Computers

Following table and chart shows number of computers and their versions

## General Information - Servers

Following table and chart shows number of servers and their versions

|  |  |
| --- | --- |
| Servers Count | |
| Windows Server 2019 Standard | 1 |
| Windows Server 2019 Standard Evaluation | 1 |
| Windows Server 2016 Standard | 1 |

## General Information - Unknown Computers

Following table and chart shows number of unknown object computers in domain.

|  |  |
| --- | --- |
| Unknown Computers Count | |
| Unknown | 1 |

# Domain Password Quality

This section provides overview about password quality used in ad.evotec.pl. One should review if all those potentially dangerous approaches to password quality should be left as is or addressed in one way or another.

## Password Quality - Passwords with Reversible Encryption

There are no accounts that have passwords stored using reversible encryption.

## Password Quality - Passwords with LM Hash

LM-hashes is the oldest password storage used by Windows, dating back to OS/2 system. There were no accounts found that use LM Hashes.

## Password Quality - Empty Passwords

Following accounts have no password set:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Guest |  | Guest |  |  |

## Password Quality - Known passwords

Domain was tested for the use of known passwords from the list below:

* + P@ssw0rd!

There were no accounts found that match given dictionary.

## Password Quality - Default Computer Password

There were no accounts found that match default computer password criteria.

## Password Quality - Password Not Required

These accounts are not required to have a password. For some accounts it may be perfectly acceptable but for some it may not. Those accounts should be reviewed and accepted or changed to proper security.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| EVOTEC$ |  | EVOTEC$ |  |  |
| Guest |  | Guest |  |  |
| test7 |  | TEST7$ |  |  |

## Password Quality - Non expiring passwords

Following account have do not expire password policy set on them. Those accounts should be reviewed whether allowing them to never expire is good idea and accepted risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Administrator |  | Administrator |  |  |
| Guest |  | Guest |  |  |

## Password Quality - AES Keys Missing

There are no accounts that hvae their Kerberos AES keys missing.

## Password Quality - Kerberos Pre-Auth Not Required

There were no accounts found that do not require pre-authentication.

## Password Quality - Only DES Encryption Allowed

There are no account that require only DES encryption.

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Administrator |  | Administrator |  |  |
| krbtgt |  | krbtgt |  |  |

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Testing 1 ADM Account | adm\_testing1@ad.evotec.pl | adm\_testing1 | Testing 1 ADM Account | Testing 1 |
| MyUser Testing 2 ADM | adm\_testing2@ad.evotec.pl | adm\_testing2 | MyUser Testing 2 ADM | MyUser |

## Password Quality - Leaked Passwords

There were no passwords found that match in given dictionary.

## Password Quality - Statistics

Following table and chart shows password statistics

|  |  |
| --- | --- |
| Password Quality - Statistics | |
| Clear Text Passwords | 0 |
| LM Hashes | 0 |
| Empty Passwords | 1 |
| Weak Passwords | 0 |
| Weak Passwords Enabled | 0 |
| Weak Passwords Disabled | 0 |
| Weak Passwords (HASH) | 0 |
| Weak Passwords (HASH) Enabled | 0 |
| Weak Passwords (HASH) Disabled | 0 |
| Default Computer Passwords | 0 |
| Password Not Required | 3 |
| Password Never Expires | 2 |
| AES Keys Missing | 0 |
| PreAuth Not Required | 0 |
| DES Encryption Only | 0 |
| Delegatable Admins | 2 |
| Duplicate Password Users | 2 |
| Duplicate Password Grouped | 1 |

# General Information - Domain ad.evotec.xyz

# General Information - Domain Summary

Following domain exists within forest :

* + Domain DC=ad,DC=evotec,DC=xyz
    - Name for fully qualified domain name (FQDN): ad.evotec.xyz
    - Name for NetBIOS: EVOTEC

# General Information - Domain Well Known Folders

Following table has defined well known folders:

|  |  |
| --- | --- |
| Well known folders | |
| UsersContainer | CN=Users,DC=ad,DC=evotec,DC=xyz |
| ComputersContainer | CN=Computers,DC=ad,DC=evotec,DC=xyz |
| DomainControllersContainer | OU=Domain Controllers,DC=ad,DC=evotec,DC=xyz |
| DeletedObjectsContainer | CN=Deleted Objects,DC=ad,DC=evotec,DC=xyz |
| SystemsContainer | CN=System,DC=ad,DC=evotec,DC=xyz |
| LostAndFoundContainer | CN=LostAndFound,DC=ad,DC=evotec,DC=xyz |
| QuotasContainer | CN=NTDS Quotas,DC=ad,DC=evotec,DC=xyz |
| ForeignSecurityPrincipalsContainer | CN=ForeignSecurityPrincipals,DC=ad,DC=evotec,DC=xyz |

# General Information - Domain Controllers

Following table contains domain controllers

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Host Name | Operating System | Site | Ipv4 |
| AD1 | AD1.ad.evotec.xyz | Windows Server 2016 Standard | KATOWICE-2 | 192.168.240.189 |
| AD2 | AD2.ad.evotec.xyz | Windows Server 2016 Standard | KATOWICE-2 | 192.168.240.192 |
| AD3 | AD3.ad.evotec.xyz | Windows Server 2019 Standard Evaluation | KATOWICE-2 | 192.168.240.236 |

Following table contains FSMO servers with roles for domain ad.evotec.xyz

|  |  |
| --- | --- |
| FSMO Roles for ad.evotec.xyz | |
| PDC Emulator | AD1.ad.evotec.xyz |
| RID Master | AD1.ad.evotec.xyz |
| Infrastructure Master | AD1.ad.evotec.xyz |

# General Information - Password Policies

Following table contains password policies for all users within ad.evotec.xyz

|  |  |
| --- | --- |
| Default Password Policy for ad.evotec.xyz | |
| Complexity Enabled | True |
| Lockout Duration | 35 |
| Lockout Observation Window | 35 |
| Lockout Threshold | 5 |
| Max Password Age | 42 |
| Min Password Length | 7 |
| Min Password Age | 1 |
| Password History Count | 24 |
| Reversible Encryption Enabled | False |
| Distinguished Name | DC=ad,DC=evotec,DC=xyz |

# General Information - Fine-grained Password Policies

Following table contains Fine-grained password policies

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Complexity Enabled | Lockout Duration | Lockout Observation Window | Lockout Threshold |
| 15 days policy | True | 00:30:00 | 00:30:00 | 0 |
| 10 days policy | True | 00:30:00 | 00:30:00 | 0 |

# General Information - Group Policies

Following table contains group policies for ad.evotec.xyz

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Gpo Status | Creation Time | Modification Time | Description |
| TEST | Registry GPOs | AllSettingsDisabled | 07/15/2020 08:28:29 | 11/08/2020 10:44:58 |  |
| TEST | Time Settings | AllSettingsEnabled | 01/25/2021 21:13:07 | 01/25/2021 21:14:16 |  |
| ALL | Enable RDP | AllSettingsEnabled | 08/07/2018 12:47:44 | 12/06/2020 10:19:20 |  |
| COMPUTERS | Add Administrator | AllSettingsEnabled | 06/26/2020 13:03:16 | 06/26/2020 14:42:08 |  |
| TEST | Password Filter | AllSettingsEnabled | 07/31/2020 14:42:42 | 07/31/2020 21:13:34 |  |
| TEST | Local Users and Groups | UserSettingsDisabled | 06/17/2020 13:23:22 | 11/07/2020 21:45:00 |  |
| ALL | Allow use of biometrics | UserSettingsDisabled | 05/20/2018 23:50:07 | 11/26/2020 10:24:02 | Test description |
| TEST | Bitlocker Settings | AllSettingsEnabled | 07/31/2020 22:13:25 | 07/31/2020 21:15:00 |  |
| TEST | GPOZaurr Permissions Testing | AllSettingsEnabled | 11/11/2020 21:29:24 | 12/22/2020 23:51:56 |  |
| TEST | Empty GPO Block Admin | AllSettingsEnabled | 05/06/2020 15:47:17 | 07/15/2020 07:26:40 |  |
| TEST | Empty 1 | AllSettingsEnabled | 11/11/2020 10:17:49 | 02/09/2021 16:54:00 |  |
| TEST | Event Log Audit Rules | AllSettingsEnabled | 07/30/2020 22:29:10 | 07/30/2020 23:18:02 |  |
| ALL | Certificates | AllSettingsEnabled | 06/06/2020 20:03:36 | 08/17/2020 07:32:28 |  |
| Default Domain Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 10/05/2020 18:31:34 | Test |
| TEST | Empty 4 | AllSettingsEnabled | 12/21/2020 13:50:32 | 02/09/2021 16:54:24 |  |
| ALL | Trusted Websites | AllSettingsEnabled | 05/09/2020 10:03:32 | 05/09/2020 09:16:10 |  |
| Copy of ALL | Trusted Websites | AllSettingsEnabled | 08/05/2020 12:21:20 | 08/05/2020 11:25:32 |  |
| ALL | Bitlocker Settings | AllSettingsEnabled | 08/07/2018 12:22:23 | 05/13/2020 19:23:48 |  |
| TEST | Folder Redirection | AllSettingsEnabled | 02/10/2021 18:27:14 | 02/10/2021 18:58:02 |  |
| TEST | Something Registry | AllSettingsEnabled | 02/09/2021 13:28:15 | 02/09/2021 16:55:44 |  |
| DC | Event Log Settings | AllSettingsEnabled | 05/20/2018 10:13:53 | 03/20/2021 15:12:34 |  |
| TEST | Windows Firewall | AllSettingsEnabled | 02/10/2021 18:29:35 | 02/11/2021 11:18:00 |  |
| DC | Event Log Audit Rules | AllSettingsEnabled | 05/20/2018 10:14:09 | 06/10/2020 23:19:48 |  |
| TEST | Empty 2 | AllSettingsEnabled | 10/19/2020 10:00:37 | 02/09/2021 16:54:08 |  |
| ALL | Firewall Settings | AllSettingsEnabled | 08/07/2018 16:42:25 | 11/11/2020 13:28:48 |  |
| COMPUTERS | Enable Sets | AllSettingsDisabled | 06/11/2018 13:06:51 | 12/01/2020 19:24:44 |  |
| TEST | IE Testing | AllSettingsEnabled | 07/21/2020 15:17:38 | 07/21/2020 14:18:20 |  |
| TEST | Empty 8 | AllSettingsEnabled | 07/21/2020 14:37:20 | 02/09/2021 16:55:06 |  |
| Default Domain Controllers Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 06/02/2020 10:42:32 |  |
| TEST | Empty 3 | AllSettingsEnabled | 12/21/2020 13:50:45 | 02/09/2021 16:54:18 |  |
| TEST | LAPS | AllSettingsEnabled | 07/31/2020 09:20:18 | 11/12/2020 09:47:58 |  |
| TEST | Empty 7 | AllSettingsEnabled | 02/02/2021 10:42:16 | 02/09/2021 16:55:00 |  |
| TEST | Task | AllSettingsEnabled | 08/24/2020 13:15:58 | 11/22/2020 14:36:22 |  |
| DC | Password Filter | AllSettingsEnabled | 05/23/2020 11:23:28 | 07/31/2020 12:15:40 |  |
| ALL | Windows PowerShell | AllSettingsEnabled | 08/27/2020 11:48:19 | 08/27/2020 10:49:28 |  |
| TEST | Empty 11 | AllSettingsEnabled | 01/14/2021 11:21:19 | 02/09/2021 16:56:08 |  |
| COMPUTERS | LAPS | AllSettingsEnabled | 12/16/2019 21:25:32 | 05/30/2020 18:12:58 |  |
| TEST | Empty 6 | AllSettingsEnabled | 12/09/2020 20:33:36 | 02/09/2021 16:54:54 |  |
| TEST | Empty 5 - CrossLink | AllSettingsEnabled | 12/24/2020 08:45:23 | 02/09/2021 16:54:44 |  |
| TEST | Printers | AllSettingsEnabled | 07/17/2020 09:09:18 | 08/01/2020 21:44:02 |  |
| TEST | Empty O365 GPO | AllSettingsEnabled | 05/28/2020 11:04:12 | 07/15/2020 07:26:16 |  |
| Copy of ALL | Certificates | AllSettingsEnabled | 08/13/2020 11:25:08 | 08/13/2020 10:52:42 |  |
| TEST | Empty GPO | AllSettingsEnabled | 07/09/2020 11:05:59 | 07/15/2020 07:26:04 |  |
| TEST | Office Configuration | AllSettingsEnabled | 07/17/2020 11:16:13 | 07/31/2020 21:47:38 |  |
| TEST | Windows Defender | AllSettingsEnabled | 08/19/2020 10:09:59 | 08/19/2020 09:20:46 |  |
| TEST | Services Testing | AllSettingsEnabled | 07/15/2020 23:11:14 | 07/15/2020 22:14:06 |  |
| TEST | IE Settings | AllSettingsEnabled | 08/25/2020 11:06:38 | 08/25/2020 10:10:00 |  |
| TEST | Empty 10 | AllSettingsEnabled | 07/31/2020 00:18:12 | 02/09/2021 16:55:32 |  |
| TEST | Testing SCRIPTS | AllSettingsEnabled | 07/14/2020 22:34:33 | 07/15/2020 07:26:28 |  |
| TEST | Empty 9 | AllSettingsEnabled | 07/24/2020 11:02:55 | 02/09/2021 16:55:20 |  |
| TEST | Task Scheduler | AllSettingsEnabled | 07/17/2020 11:09:27 | 07/17/2020 10:13:58 |  |

# General Information - Group Policies Details

Following table contains group policies for ad.evotec.xyz

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Links | Has Computer Settings | Has User Settings | User Enabled |
| TEST | Registry GPOs |  | True | False | false |
| TEST | Time Settings |  | True | False | true |
| ALL | Enable RDP | ad.evotec.xyz/ITR01;ad.evotec.xyz/ITR02;ad.evotec.xyz | True | False | true |
| COMPUTERS | Add Administrator |  | True | False | true |
| TEST | Password Filter |  | True | False | true |
| TEST | Local Users and Groups |  | True | True | false |
| ALL | Allow use of biometrics | ad.evotec.xyz/Domain Controllers;ad.evotec.xyz | True | False | false |
| TEST | Bitlocker Settings |  | True | False | true |
| TEST | GPOZaurr Permissions Testing | ad.evotec.xyz | False | True | true |
| TEST | Empty GPO Block Admin |  | False | False | true |
| TEST | Empty 1 |  | False | False | true |
| TEST | Event Log Audit Rules |  | True | False | true |
| ALL | Certificates | ad.evotec.xyz | True | False | true |
| Default Domain Policy | ad.evotec.xyz | True | False | true |
| TEST | Empty 4 |  | False | False | true |
| ALL | Trusted Websites | ad.evotec.xyz | False | True | true |
| Copy of ALL | Trusted Websites |  | False | True | true |
| ALL | Bitlocker Settings | ad.evotec.xyz | True | False | true |
| TEST | Folder Redirection |  | False | True | true |
| TEST | Something Registry |  | False | True | true |
| DC | Event Log Settings | ad.evotec.xyz/Domain Controllers | True | False | true |
| TEST | Windows Firewall |  | True | False | true |
| DC | Event Log Audit Rules | ad.evotec.xyz/Domain Controllers | True | False | true |
| TEST | Empty 2 |  | False | False | true |
| ALL | Firewall Settings | ad.evotec.xyz | True | False | true |
| COMPUTERS | Enable Sets | ad.evotec.xyz/ITR01/SE;ad.evotec.xyz/ITR02/Test;ad.evotec.xyz | True | False | false |
| TEST | IE Testing |  | False | True | true |
| TEST | Empty 8 |  | False | False | true |
| Default Domain Controllers Policy | ad.evotec.xyz/Domain Controllers | True | False | true |
| TEST | Empty 3 |  | False | False | true |
| TEST | LAPS |  | True | False | true |
| TEST | Empty 7 |  | False | False | true |
| TEST | Task |  | False | False | true |
| DC | Password Filter | ad.evotec.xyz/Domain Controllers | True | False | true |
| ALL | Windows PowerShell | ad.evotec.xyz | True | False | true |
| TEST | Empty 11 |  | False | False | true |
| COMPUTERS | LAPS | ad.evotec.xyz/ITR02/Computers;ad.evotec.xyz/ITR01/SE;ad.evotec.xyz/ITR01/SE/SE2 | True | False | true |
| TEST | Empty 6 |  | False | False | true |
| TEST | Empty 5 - CrossLink |  | False | False | true |
| TEST | Printers |  | True | True | true |
| TEST | Empty O365 GPO |  | False | False | true |
| Copy of ALL | Certificates |  | True | False | true |
| TEST | Empty GPO | ad.evotec.xyz | False | False | true |
| TEST | Office Configuration |  | False | True | true |
| TEST | Windows Defender |  | True | False | true |
| TEST | Services Testing |  | True | False | true |
| TEST | IE Settings |  | False | True | true |
| TEST | Empty 10 |  | False | False | true |
| TEST | Testing SCRIPTS |  | True | False | true |
| TEST | Empty 9 |  | True | False | true |
| TEST | Task Scheduler |  | True | False | true |

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Target | NameTarget | Priority | Weight | Port |
| ad3.ad.evotec.xyz | ad3.ad.evotec.xyz | 0 | 100 | 88 |
| ad2.ad.evotec.xyz | ad2.ad.evotec.xyz | 0 | 100 | 88 |
| ad1.ad.evotec.xyz | ad1.ad.evotec.xyz | 0 | 100 | 88 |
| ad3.ad.evotec.xyz | ad3.ad.evotec.xyz | 0 | 100 | 389 |
| ad2.ad.evotec.xyz | ad2.ad.evotec.xyz | 0 | 100 | 389 |
| ad1.ad.evotec.xyz | ad1.ad.evotec.xyz | 0 | 100 | 389 |

Following table contains A records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Address | IPAddress | IP4Address | Name | Type |
| 192.168.240.236 | 192.168.240.236 | 192.168.240.236 | ad3.ad.evotec.xyz | A |
| 192.168.240.192 | 192.168.240.192 | 192.168.240.192 | ad2.ad.evotec.xyz | A |
| 192.168.240.189 | 192.168.240.189 | 192.168.240.189 | ad1.ad.evotec.xyz | A |
| 192.168.240.236 | 192.168.240.236 | 192.168.240.236 | ad3.ad.evotec.xyz | A |
| 192.168.240.192 | 192.168.240.192 | 192.168.240.192 | ad2.ad.evotec.xyz | A |
| 192.168.240.189 | 192.168.240.189 | 192.168.240.189 | ad1.ad.evotec.xyz | A |

# General Information - Trusts

Following table contains trusts established with domains...

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Trust Source | Trust Target | Trust Direction | Trust Attributes | Trust Status |
| ad.evotec.xyz | ad.evotec.pl | BiDirectional | Within Forest | OK |
| ad.evotec.xyz | test.evotec.pl | BiDirectional | Forest Transitive | OK |

# General Information - Organizational Units

Following table contains all OU's created in ad.evotec.xyz

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Canonical Name | Managed | Manager Email | Protected | Description |
| ad.evotec.xyz/Domain Controllers |  |  | False | Default container for domain controllers |
| ad.evotec.xyz/ITR01 |  |  | False |  |
| ad.evotec.xyz/ITR01/SE |  |  | False |  |
| ad.evotec.xyz/ITR01/SE/SE1 |  |  | False |  |
| ad.evotec.xyz/ITR01/SE/SE1/User |  |  | True |  |
| ad.evotec.xyz/ITR01/SE/SE1/User/Users |  |  | True |  |
| ad.evotec.xyz/ITR01/SE/SE2 |  |  | True |  |
| ad.evotec.xyz/ITR01/US |  |  | True |  |
| ad.evotec.xyz/ITR02 |  |  | False |  |
| ad.evotec.xyz/ITR02/Computers |  |  | False |  |
| ad.evotec.xyz/ITR02/Test |  |  | False |  |
| ad.evotec.xyz/Microsoft Exchange Security Groups |  |  | False |  |
| ad.evotec.xyz/Production |  |  | True |  |
| ad.evotec.xyz/Production/Accounts |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/Contacts |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/Service |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/ServiceAzure |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/Special |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/SpecialAzure |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/Users |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/UsersNoSync |  |  | True |  |
| ad.evotec.xyz/Production/Accounts/UsersNoSync/IQM |  |  | False |  |
| ad.evotec.xyz/Production/Accounts/UsersNoSync/MyNeva |  |  | False |  |
| ad.evotec.xyz/Production/Accounts/UsersNoSync/Regas |  |  | False |  |
| ad.evotec.xyz/Production/Devices |  |  | True |  |
| ad.evotec.xyz/Production/Devices/Computers |  |  | True |  |
| ad.evotec.xyz/Production/Devices/Servers |  |  | True |  |
| ad.evotec.xyz/Production/Devices/Servers.Hosts |  |  | True |  |
| ad.evotec.xyz/Production/Groups |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Delegation |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Distibution |  |  | True |  |
| ad.evotec.xyz/Production/Groups/O365 |  |  | True |  |
| ad.evotec.xyz/Production/Groups/O365/Licenses |  |  | True |  |
| ad.evotec.xyz/Production/Groups/O365/WriteBack |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Security |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Security/NetworkAdministration |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Security/NetworkVPNAdmin |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Security/NetworkVPNUsers |  |  | True |  |
| ad.evotec.xyz/Production/Groups/Security/Test : Test |  |  | True |  |

# General Information - Priviliged Groups

Following table contains list of priviliged groups and count of the members in it.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Group Name | Group Category | Group Scope | Group SID | High Privileged Group |
| Administrators | Security | DomainLocal | S-1-5-32-544 | True |
| Print Operators | Security | DomainLocal | S-1-5-32-550 | True |
| Backup Operators | Security | DomainLocal | S-1-5-32-551 | True |
| Replicator | Security | DomainLocal | S-1-5-32-552 | True |
| Network Configuration Operators | Security | DomainLocal | S-1-5-32-556 | False |
| Event Log Readers | Security | DomainLocal | S-1-5-32-573 | False |
| Hyper-V Administrators | Security | DomainLocal | S-1-5-32-578 | False |
| Remote Management Users | Security | DomainLocal | S-1-5-32-580 | False |
| Schema Admins | Security | Universal | S-1-5-21-853615985-2870445339-3163598659-518 | True |
| Enterprise Admins | Security | Universal | S-1-5-21-853615985-2870445339-3163598659-519 | True |
| Domain Admins | Security | Global | S-1-5-21-853615985-2870445339-3163598659-512 | True |
| Group Policy Creator Owners | Security | Global | S-1-5-21-853615985-2870445339-3163598659-520 | False |
| Server Operators | Security | DomainLocal | S-1-5-32-549 | True |
| Account Operators | Security | DomainLocal | S-1-5-32-548 | True |
| Incoming Forest Trust Builders | Security | DomainLocal | S-1-5-32-557 | False |

# General Information - Domain Users in ad.evotec.xyz

## General Information - Users Count

Following table and chart shows number of users in its categories

|  |  |
| --- | --- |
| Users Count | |
| Users Count Incl. System | 152 |
| Users Count | 147 |
| Users Expired | 14 |
| Users Expired Incl. Disabled | 116 |
| Users Never Expiring | 19 |
| Users Never Expiring Incl. Disabled | 31 |
| Users System Accounts | 5 |

## General Information - Domain Administrators

Following users have highest priviliges and are able to control a lot of Windows resources.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Name | User Principal Name | Sam Account Name | Email Address |
| Administrator | Administrator | Administrator@ad.evotec.xyz | Administrator | Administrator@ad.evotec.xyz |
| Administrator Przemysław Kłys | Administrator Przemysław Kłys | adm.pklys@ad.evotec.xyz | adm.pklys |  |
| Przemysław Kłys | Przemysław Kłys | przemyslaw.klys@evotec.pl | przemyslaw.klys | przemyslaw.klys@evotec.pl |
| ADM Testing 1 | ADM Testing 1 | adm\_testing1@ad.evotec.xyz | adm\_testing1 |  |
| Some Mailbox | Some Mailbox | some1@evotec.pl | some1 | SomeMailbox@ad.evotec.xyz |
| Service Task Scheduler | Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler |  |
| Temporary Admin | Temporary Admin 1 | TemporaryAdmin@ad.evotec.xyz | TemporaryAdmin |  |

## General Information - Enterprise Administrators

Following users have highest priviliges across Forest and are able to control a lot of Windows resources.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Name | User Principal Name | Sam Account Name | Email Address |
| Przemysław Kłys | Przemysław Kłys | przemyslaw.klys@evotec.pl | przemyslaw.klys | przemyslaw.klys@evotec.pl |
| Administrator | Administrator | Administrator@ad.evotec.xyz | Administrator | Administrator@ad.evotec.xyz |

# General Information - Computer Objects in ad.evotec.xyz

## General Information - Computers

Following table and chart shows number of computers and their versions

|  |  |
| --- | --- |
| Computers Count | |
| Windows 10 Enterprise | 3 |
| Windows 10 Pro | 2 |
| Windows 10 Pro N Insider Preview | 1 |

## General Information - Servers

Following table and chart shows number of servers and their versions

|  |  |
| --- | --- |
| Servers Count | |
| Windows Server 2016 Standard | 6 |
| Windows Server 2012 R2 Standard Evaluation | 1 |
| Windows Server 2019 Standard Evaluation | 7 |

## General Information - Unknown Computers

Following table and chart shows number of unknown object computers in domain.

|  |  |
| --- | --- |
| Unknown Computers Count | |
| Unknown | 6 |

# Domain Password Quality

This section provides overview about password quality used in ad.evotec.xyz. One should review if all those potentially dangerous approaches to password quality should be left as is or addressed in one way or another.

## Password Quality - Passwords with Reversible Encryption

Passwords of these accounts are stored using reversible encryption.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Expiration Date Test | expiration@evotec.xyz | expiration | Expiration Date Test | Expiration |
| Test Przemyslaw Klys | test.przemyslaw.klys@ad.evotec.xyz | test.przemyslaw.klys | Test Przemyslaw Klys | Test Przemyslaw |

## Password Quality - Passwords with LM Hash

LM-hashes is the oldest password storage used by Windows, dating back to OS/2 system. There were no accounts found that use LM Hashes.

## Password Quality - Empty Passwords

Following accounts have no password set:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Exchange Online-ApplicationAccount | Exchange\_Online-ApplicationAccount@ad.evotec.xyz | $E31000-VQ0GNFC5U2JU | (offboarded) |  |
| DefaultAccount |  | DefaultAccount | (offboarded) |  |
| Guest |  | Guest | Guest |  |
| SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9} | SystemMailbox{e0dc1c29-89c3-4034-b678-e6c29d823ed9}@ad.evotec.xyz | SM\_2501271fcd0143199 | Microsoft Exchange (offboarded) |  |
| Microsoft Exchange Federation Mailbox | FederatedEmail.4c1f4d8b-8179-4148-93bf-00a95fa1e042@ad.evotec.xyz | SM\_541db8fc4c894be19 | Microsoft Exchange Federation Mailbox |  |
| Microsoft Exchange Approval Assistant | SystemMailbox{1f05a927-d2bf-4ddc-92db-28bdc645a9a6}@ad.evotec.xyz | SM\_6152b2ecbc6b4d8fb | Microsoft Exchange Approval Assistant |  |
| Microsoft Exchange Migration | Migration.8f3e7716-2011-43e4-96b1-aba62d229136@ad.evotec.xyz | SM\_8fcde8d3dfd241bfb | Microsoft Exchange Migration |  |
| Microsoft Exchange (offboarded) | SystemMailbox{bb558c35-97f1-4cb9-8ff7-d53741dc928c}@ad.evotec.xyz | SM\_c383d4fac8c34f62a | Microsoft Exchange (offboarded) |  |
| Discovery Search Mailbox | DiscoverySearchMailbox {D919BA05-46A6-415f-80AD-7E09334BB852}@ad.evotec.xyz | SM\_e6e481ec2d2f4f938 | Discovery Search Mailbox |  |

## Password Quality - Known passwords

Domain was tested for the use of known passwords from the list below:

* + P@ssw0rd!

There were no accounts found that match given dictionary.

## Password Quality - Default Computer Password

There were no accounts found that match default computer password criteria.

## Password Quality - Password Not Required

These accounts are not required to have a password. For some accounts it may be perfectly acceptable but for some it may not. Those accounts should be reviewed and accepted or changed to proper security.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Exchange Online-ApplicationAccount | Exchange\_Online-ApplicationAccount@ad.evotec.xyz | $E31000-VQ0GNFC5U2JU | (offboarded) |  |
| DefaultAccount |  | DefaultAccount | (offboarded) |  |
| EVOTECPL$ |  | EVOTECPL$ | (offboarded) |  |
| Guest |  | Guest | Guest |  |
| TEST$ |  | TEST$ |  |  |
| Test1 |  | TEST1$ |  |  |
| Test2 |  | TEST2$ |  |  |
| Test4 |  | TEST4$ |  |  |
| Test6 |  | TEST6$ |  |  |
| TestingDSInstall |  | TESTINGDSINSTAL$ |  |  |

## Password Quality - Non expiring passwords

Following account have do not expire password policy set on them. Those accounts should be reviewed whether allowing them to never expire is good idea and accepted risk.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Administrator Przemysław Kłys | adm.pklys@ad.evotec.xyz | adm.pklys | Administrator Przemysław Kłys | Administrator Przemysław |
| Administrator | Administrator@ad.evotec.xyz | Administrator | Administrator |  |
| AZUREADSSOACC |  | AZUREADSSOACC$ |  |  |
| DefaultAccount |  | DefaultAccount | (offboarded) |  |
| Guest |  | Guest | Guest |  |
| HealthMailbox-EX2013X3-001 (offboarded) | HealthMailbox14193432ba1143fda716adf2892e98c6@ad.evotec.xyz | HealthMailbox1419343 | HealthMailbox-EX2013X3-001 (offboarded) |  |
| HealthMailbox2d50e3005c484d25a609113593de2c33 | HealthMailbox2d50e3005c484d25a609113593de2c33@ad.evotec.xyz | HealthMailbox2d50e30 | HealthMailbox-EX2013X3-005 |  |
| HealthMailbox49c425434f14404789901106b55279ad | HealthMailbox49c425434f14404789901106b55279ad@ad.evotec.xyz | HealthMailbox49c4254 | HealthMailbox-EX2013X3-004 |  |
| HealthMailbox4bbdf1b0c959451bbabc05a9e40713d5 | HealthMailbox4bbdf1b0c959451bbabc05a9e40713d5@ad.evotec.xyz | HealthMailbox4bbdf1b | HealthMailbox-EX2013X3-002 |  |
| HealthMailbox5c21e4f881c0456cadd937c9f64a61da | HealthMailbox5c21e4f881c0456cadd937c9f64a61da@ad.evotec.xyz | HealthMailbox5c21e4f | HealthMailbox-EX2013X3-003 |  |
| HealthMailbox-EX2013X3-003 (offboarded) | HealthMailbox60155b13835f4e669b2fabf5b95dfd74@ad.evotec.xyz | HealthMailbox60155b1 | HealthMailbox-EX2013X3-003 (offboarded) |  |
| HealthMailbox-EX2013X3-010 (offboarded) | HealthMailbox603739f5e90b43539922000fece40c6b@ad.evotec.xyz | HealthMailbox603739f | HealthMailbox-EX2013X3-010 (offboarded) |  |
| HealthMailbox-EX2013X3-005 (offboarded) | HealthMailbox61f9b982483640bf8ce51c097113cc94@ad.evotec.xyz | HealthMailbox61f9b98 | HealthMailbox-EX2013X3-005 (offboarded) |  |
| HealthMailbox-EX2013X3-008 (offboarded) | HealthMailbox751984c8c5c54b849143e72fccb98a27@ad.evotec.xyz | HealthMailbox751984c | HealthMailbox-EX2013X3-008 (offboarded) |  |
| HealthMailbox8d5e4ebac4be48c1957878877a544d1a | HealthMailbox8d5e4ebac4be48c1957878877a544d1a@ad.evotec.xyz | HealthMailbox8d5e4eb | HealthMailbox-EX2013X3-007 |  |
| HealthMailbox9bf79ab078f34b8da31862a98411a3f2 | HealthMailbox9bf79ab078f34b8da31862a98411a3f2@ad.evotec.xyz | HealthMailbox9bf79ab | HealthMailbox-EX2013X3-008 |  |
| HealthMailboxb1a64c238bb847ceaafd3f7eadc15ef4 | HealthMailboxb1a64c238bb847ceaafd3f7eadc15ef4@ad.evotec.xyz | HealthMailboxb1a64c2 | HealthMailbox-EX2013X3-006 |  |
| HealthMailboxb3289545c3e744818c6aeece7ab43c2a | HealthMailboxb3289545c3e744818c6aeece7ab43c2a@ad.evotec.xyz | HealthMailboxb328954 | HealthMailbox-EX2013X3-Mailbox-Database-1527735546 |  |
| HealthMailbox-EX2013X3-002 (offboarded) | HealthMailboxbb779b7f61384f1abd85a4cc2e793321@ad.evotec.xyz | HealthMailboxbb779b7 | HealthMailbox-EX2013X3-002 (offboarded) |  |
| HealthMailbox-EX2013X3-006 (offboarded) | HealthMailboxc57ed73ae291405da8589c3f2d9a94da@ad.evotec.xyz | HealthMailboxc57ed73 | HealthMailbox-EX2013X3-006 (offboarded) |  |
| HealthMailboxcd3fe85ae75442aeb5487fd56b8b2cd8 | HealthMailboxcd3fe85ae75442aeb5487fd56b8b2cd8@ad.evotec.xyz | HealthMailboxcd3fe85 | HealthMailbox-EX2013X3-001 |  |
| HealthMailbox-EX2013X3-Mailbox-Database-1527735546 (offboarded) | HealthMailboxceaf9714b5e8497aabe5d8c7d390c762@ad.evotec.xyz | HealthMailboxceaf971 | HealthMailbox-EX2013X3-Mailbox-Database-1527735546 (offboarded) |  |
| HealthMailbox-EX2013X3-009 (offboarded) | HealthMailboxd9af2950e74d411cb88eed998353ae6e@ad.evotec.xyz | HealthMailboxd9af295 | HealthMailbox-EX2013X3-009 (offboarded) |  |
| HealthMailboxdcb7fda57f054f458ddc4592d90a209c | HealthMailboxdcb7fda57f054f458ddc4592d90a209c@ad.evotec.xyz | HealthMailboxdcb7fda | HealthMailbox-EX2013X3-009 |  |
| HealthMailbox-EX2013X3-004 (offboarded) | HealthMailboxe03c754075c6456cac3e996649243352@ad.evotec.xyz | HealthMailboxe03c754 | HealthMailbox-EX2013X3-004 (offboarded) |  |
| HealthMailboxf7e9bcb0f2e14c60896a7c2b5bc3fef8 | HealthMailboxf7e9bcb0f2e14c60896a7c2b5bc3fef8@ad.evotec.xyz | HealthMailboxf7e9bcb | HealthMailbox-EX2013X3-010 |  |
| HealthMailbox-EX2013X3-007 (offboarded) | HealthMailboxfcd7e01b1f1246449c76ee183185ee32@ad.evotec.xyz | HealthMailboxfcd7e01 | HealthMailbox-EX2013X3-007 (offboarded) |  |
| MSOL\_6f0d1d4965ec |  | MSOL\_6f0d1d4965ec |  |  |
| My User | myuserPrincipal@evotec.pl | myuser | My User | My |
| Weird Name, with $,. | myweirdtest@ad.evotec.xyz | myweirdtest | Weird Name, with $,. | Weird |
| Przemysław Kłys | przemyslaw.klys@evotec.pl | przemyslaw.klys | Przemysław Kłys | Przemysław |
| SA Azure ATP | sa-azureatp@ad.evotec.xyz | sa-azureatp | SA Azure ATP | SA Azure |
| Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler | Service Task Scheduler | Service Task |
| Test AD | TestingAD@ad.evotec.xyz | TestingAD | Test AD | Test AD |

## Password Quality - AES Keys Missing

There are no accounts that hvae their Kerberos AES keys missing.

## Password Quality - Kerberos Pre-Auth Not Required

There were no accounts found that do not require pre-authentication.

## Password Quality - Only DES Encryption Allowed

There are no account that require only DES encryption.

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| Administrator Przemysław Kłys | adm.pklys@ad.evotec.xyz | adm.pklys | Administrator Przemysław Kłys | Administrator Przemysław |
| ADM Testing 1 | adm\_testing1@ad.evotec.xyz | adm\_testing1 | ADM Testing 1 | Testing 1 |
| Administrator | Administrator@ad.evotec.xyz | Administrator | Administrator |  |
| Expiration Date Test | expiration@evotec.xyz | expiration | Expiration Date Test | Expiration |
| krbtgt |  | krbtgt | (offboarded) |  |
| Przemysław Kłys | przemyslaw.klys@evotec.pl | przemyslaw.klys | Przemysław Kłys | Przemysław |
| SADM Testing 2 | sadm\_testing2@ad.evotec.xyz | sadm\_testing2 | SADM Testing 2 | SADM |
| Some Mailbox | some1@evotec.pl | some1 | Some Mailbox | Some |
| Special Test User | SpecialTestUser@ad.evotec.xyz | SpecialTestUser | Special Test User | Special |
| Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler | Service Task Scheduler | Service Task |
| Temporary Admin 1 | TemporaryAdmin@ad.evotec.xyz | TemporaryAdmin | Temporary Admin | Temporary |
| Test User Test | test@ad.evotec.xyz | test | Test User Test | Test User |
| Test Przemyslaw Klys | test.przemyslaw.klys@ad.evotec.xyz | test.przemyslaw.klys | Test Przemyslaw Klys | Test Przemyslaw |

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | UserPrincipalName | SamAccountName | DisplayName | GivenName |
| LAPS Test | lapstest@ad.evotec.xyz | lapstest | LAPS Test | LAPS |
| Test IntetOrgUser | TestIntetOrgUser@ad.evotec.xyz | TestIntetOrgUser | Test IntetOrgUser | Test IntetOrgUser |
| ADM Testing 1 | adm\_testing1@ad.evotec.xyz | adm\_testing1 | ADM Testing 1 | Testing 1 |
| ADM Testing 2 | adm\_testing2@ad.evotec.xyz | adm\_testing2 | ADM Testing 2 | Testing account 1 |
| Weird Name, with $,. | myweirdtest@ad.evotec.xyz | myweirdtest | Weird Name, with $,. | Weird |
| SADM Testing 2 | sadm\_testing2@ad.evotec.xyz | sadm\_testing2 | SADM Testing 2 | SADM |
| Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler | Service Task Scheduler | Service Task |
| Temporary Admin 1 | TemporaryAdmin@ad.evotec.xyz | TemporaryAdmin | Temporary Admin | Temporary |
| Test User Test | test@ad.evotec.xyz | test | Test User Test | Test User |
| Test Przemyslaw Klys | test.przemyslaw.klys@ad.evotec.xyz | test.przemyslaw.klys | Test Przemyslaw Klys | Test Przemyslaw |
| Testing 1 | testing1@ad.evotec.xyz | testing1 | Testing 1 | Testing 1 |
| Test AD | TestingAD@ad.evotec.xyz | TestingAD | Test AD | Test AD |
| Test My, User | testmyuser@ad.evotec.xyz | testmyuser | Test My, User | Test |

## Password Quality - Leaked Passwords

There were no passwords found that match in given dictionary.

## Password Quality - Statistics

Following table and chart shows password statistics

|  |  |
| --- | --- |
| Password Quality - Statistics | |
| Clear Text Passwords | 2 |
| LM Hashes | 0 |
| Empty Passwords | 9 |
| Weak Passwords | 0 |
| Weak Passwords Enabled | 0 |
| Weak Passwords Disabled | 0 |
| Weak Passwords (HASH) | 0 |
| Weak Passwords (HASH) Enabled | 0 |
| Weak Passwords (HASH) Disabled | 0 |
| Default Computer Passwords | 0 |
| Password Not Required | 10 |
| Password Never Expires | 34 |
| AES Keys Missing | 0 |
| PreAuth Not Required | 0 |
| DES Encryption Only | 0 |
| Delegatable Admins | 13 |
| Duplicate Password Users | 13 |
| Duplicate Password Grouped | 2 |