# 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.xyz 6

a. General Information - Domain Summary 6

b. General Information - Domain Controllers 6

c. General Information - Password Policies 6

d. General Information - Fine Grained Password Policies 6

e. General Information - Group Policies 6

f. General Information - Group Policies Details 7

g. General Information - DNS A/SRV Records 8

h. General Information - Trusts 8

i. General Information - Organizational Units 8

j. General Information - Priviliged Groups 9

k. General Information - Domain Users in ad.evotec.xyz 9

i. General Information - Users Count 9

ii. General Information - Domain Administrators 10

iii. General Information - Enterprise Administrators 10

l. General Information - Computer Objects in ad.evotec.xyz 10

i. General Information - Computers 10

ii. General Information - Servers 10

iii. General Information - Unknown Computers 11

m. Domain Password Quality 11

i. Password Quality - Passwords with Reversible Encryption 11

ii. Password Quality - Passwords with LM Hash 11

iii. Password Quality - Empty Passwords 11

iv. Password Quality - Known passwords 11

v. Password Quality - Default Computer Password 11

vi. Password Quality - Password Not Required 11

vii. Password Quality - Non expiring passwords 11

viii. Password Quality - AES Keys Missing 11

ix. Password Quality - Kerberos Pre-Auth Not Required 11

x. Password Quality - Only DES Encryption Allowed 12

xi. Password Quality - Delegatable to Service 12

xii. Password Quality - Groups of Users With Same Password 12

xiii. Password Quality - Leaked Passwords 12

xiv. Password Quality - Statistics 12

3. General Information - Domain ad.evotec.pl 13

a. General Information - Domain Summary 13

b. General Information - Domain Controllers 13

c. General Information - Password Policies 13

d. General Information - Fine Grained Password Policies 13

e. General Information - Group Policies 13

f. General Information - Group Policies Details 14

g. General Information - DNS A/SRV Records 15

h. General Information - Trusts 15

i. General Information - Organizational Units 15

j. General Information - Priviliged Groups 16

k. General Information - Domain Users in ad.evotec.pl 16

i. General Information - Users Count 16

ii. General Information - Domain Administrators 17

iii. General Information - Enterprise Administrators 17

l. General Information - Computer Objects in ad.evotec.pl 17

i. General Information - Computers 17

ii. General Information - Servers 17

iii. General Information - Unknown Computers 18

m. Domain Password Quality 18

i. Password Quality - Passwords with Reversible Encryption 18

ii. Password Quality - Passwords with LM Hash 18

iii. Password Quality - Empty Passwords 18

iv. Password Quality - Known passwords 18

v. Password Quality - Default Computer Password 18

vi. Password Quality - Password Not Required 18

vii. Password Quality - Non expiring passwords 18

viii. Password Quality - AES Keys Missing 18

ix. Password Quality - Kerberos Pre-Auth Not Required 18

x. Password Quality - Only DES Encryption Allowed 19

xi. Password Quality - Delegatable to Service 19

xii. Password Quality - Groups of Users With Same Password 19

xiii. Password Quality - Leaked Passwords 19

xiv. Password Quality - Statistics 19

This document provides a low-level design of roles and permissions for the IT infrastructure team at Evotec organization. This document utilizes knowledge from AD General Concept document that should be delivered with this document. Having all the information described in attached document one can start designing Active Directory with those principles in mind. It's important to know while best practices that were described are important in decision making they should not be treated as final and only solution. Most important aspect is to make sure company has full usability of Active Directory and is happy with how it works. Making things harder just for the sake of implementation of best practices isn't always the best way to go.

# 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 Functional Level | Windows2012R2Forest |
| Domains Count | 2 |
| Sites Count | 4 |
| Domains | ad.evotec.xyz, ad.evotec.pl |
| Sites | KATOWICE-1, GLIWICE, KATOWICE-2, MIKOLOW |

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 | False |
| Privileged Access Management Feature Enabled | False |

Following UPN suffixes were created in this forest:

|  |  |
| --- | --- |
| UPN Suffixes | |
| ad.evotec.xyz | Primary / Default UPN |
| 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 | Modified | Created |
| KATOWICE-1 | Main location | False | 07/30/2018 15:45:00 | 05/20/2018 09:55:23 |
| GLIWICE | Some description | False | 07/30/2018 15:44:24 | 07/21/2018 19:41:01 |
| KATOWICE-2 |  | False | 07/21/2018 19:41:38 | 07/21/2018 19:41:14 |
| MIKOLOW |  | False | 07/21/2018 19:41:21 | 07/21/2018 19:41:21 |

Forest Sites list can be found below:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Topology Cleanup Enabled | Topology Detect Stale Enabled | Topology Minimum Hops Enabled | Universal Group Caching Enabled |
| KATOWICE-1 |  |  |  |  |
| GLIWICE |  |  |  |  |
| KATOWICE-2 |  |  |  |  |
| MIKOLOW |  |  |  |  |

# General Information - Subnets

Table below contains information regarding relation between Subnets and sites

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Description | Protected | Modified | Created |
| 192.168.240.0/24 |  | True | 07/30/2018 15:28:02 | 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 |

Table below contains information regarding relation between Subnets and sites

|  |  |
| --- | --- |
| Name | Site |
| 192.168.240.0/24 | CN=KATOWICE-1,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 192.168.241.0/24 | CN=MIKOLOW,CN=Sites,CN=Configuration,DC=ad,DC=evotec,DC=xyz |
| 192.168.239.0/24 | 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 | 180 | 180 |  |

# General Information - Domain ad.evotec.xyz

# General Information - Domain Summary

Following domain exists within forest ad.evotec.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-1 | 192.168.240.189 |
| AD2 | AD2.ad.evotec.xyz | Windows Server 2016 Standard | KATOWICE-1 | 192.168.240.192 |

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 | 00:30:00 |
| Lockout Observation Window | 00:30:00 |
| Lockout Threshold | 0 |
| Max Password Age | 42.00:00:00 |
| Min Password Length | 7 |
| Min Password Age | 1.00:00:00 |
| Password History Count | 24 |
| Reversible Encryption Enabled | False |
| Distinguished Name | DC=ad,DC=evotec,DC=xyz |

# General Information - Fine Grained Password Policies

Following section should cover fine grained password policies. There were no fine grained password polices defined in ad.evotec.xyz. There was no formal requirement to have them set up.

# General Information - Group Policies

Following table contains group policies for ad.evotec.xyz

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Gpo Status | Creation Time | Modification Time | Description |
| ALL | Enable RDP | AllSettingsEnabled | 08/07/2018 12:47:44 | 08/07/2018 12:47:44 |  |
| ALL | PowerShell Settings | AllSettingsEnabled | 06/16/2018 12:19:39 | 06/16/2018 12:21:08 |  |
| COMPUTERS | Allow use of biometrics | AllSettingsEnabled | 05/20/2018 23:50:07 | 05/20/2018 23:51:22 |  |
| Default Domain Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 05/20/2018 09:59:46 |  |
| ALL | Bitlocker Settings | AllSettingsEnabled | 08/07/2018 12:22:23 | 08/07/2018 12:24:04 |  |
| DC | Event Log Settings | AllSettingsEnabled | 05/20/2018 10:13:53 | 12/29/2018 19:31:32 |  |
| DC | Event Log Audit Rules | AllSettingsEnabled | 05/20/2018 10:14:09 | 04/29/2019 13:40:06 |  |
| ALL | Firewall Settings | AllSettingsEnabled | 08/07/2018 16:42:25 | 08/07/2018 16:46:16 |  |
| COMPUTERS | Enable Sets | AllSettingsEnabled | 06/11/2018 13:06:51 | 06/11/2018 13:07:16 |  |
| Default Domain Controllers Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 08/05/2018 09:55:08 |  |
| Users | Synced Office 365 Users | AllSettingsEnabled | 11/19/2018 22:54:44 | 11/19/2018 23:54:44 | My comment |
| Test | AllSettingsEnabled | 12/27/2018 00:17:38 | 12/27/2018 01:17:38 |  |

# General Information - Group Policies Details

Following table contains group policies for ad.evotec.xyz

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Links | Has Computer Settings | Has User Settings | User Enabled |
| ALL | Enable RDP | ad.evotec.xyz | True | False | true |
| ALL | PowerShell Settings | ad.evotec.xyz | True | True | true |
| COMPUTERS | Allow use of biometrics |  | True | False | true |
| Default Domain Policy | ad.evotec.xyz | True | False | true |
| ALL | Bitlocker Settings | ad.evotec.xyz/Production/Computers ad.evotec.xyz/Production/Servers ad.evotec.xyz | True | False | true |
| DC | Event Log Settings | ad.evotec.xyz/Domain Controllers | True | False | true |
| DC | Event Log Audit Rules | ad.evotec.xyz/Domain Controllers | True | False | true |
| ALL | Firewall Settings | ad.evotec.xyz | True | False | true |
| COMPUTERS | Enable Sets | ad.evotec.xyz/Production/Computers ad.evotec.xyz | True | False | true |
| Default Domain Controllers Policy | ad.evotec.xyz/Domain Controllers | True | False | true |
| Users | Synced Office 365 Users | ad.evotec.xyz/Production/Users-O365 | False | False | true |
| Test |  | False | False | true |

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Target | NameTarget | Priority | Weight | Port |
| AD1.ad.evotec.xyz | AD1.ad.evotec.xyz | 0 | 100 | 88 |
| AD2.ad.evotec.xyz | AD2.ad.evotec.xyz | 0 | 100 | 88 |
| 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 |
| 192.168.240.189 | 192.168.240.189 | 192.168.240.189 | AD1.ad.evotec.xyz | A |
| 192.168.240.192 | 192.168.240.192 | 192.168.240.192 | AD2.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 |

# General Information - Organizational Units

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Canonical Name | Managed By | Manager Email | Protected | Description |
| ad.evotec.xyz/Domain Controllers |  |  | False | Default container for domain controllers |
| ad.evotec.xyz/Microsoft Exchange Security Groups |  |  | False |  |
| ad.evotec.xyz/Production |  |  | True |  |
| ad.evotec.xyz/Production/Computers |  |  | False |  |
| ad.evotec.xyz/Production/Contacts |  |  | True |  |
| ad.evotec.xyz/Production/Groups |  |  | True |  |
| ad.evotec.xyz/Production/Groups/SecurityGroups |  |  | True |  |
| ad.evotec.xyz/Production/Servers |  |  | True |  |
| ad.evotec.xyz/Production/Users |  |  | True |  |
| ad.evotec.xyz/Production/Users-O365 |  |  | True | OU for Synchronization of Users to Office 365 |
| ad.evotec.xyz/Production/Users-Offboarded |  |  | 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 |
| 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 | 49 |
| Users Count | 45 |
| Users Expired | 4 |
| Users Expired Incl. Disabled | 15 |
| Users Never Expiring | 15 |
| Users Never Expiring Incl. Disabled | 28 |
| Users System Accounts | 4 |

# 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 |
| Temporary Admin | Temporary Admin | TemporaryAdmin@ad.evotec.xyz | TemporaryAdmin |  |
| Service Task Scheduler | Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler |  |

# 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 | 2 |
| Windows 10 Pro | 1 |
| 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 | 1 |

# General Information - Unknown Computers

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

|  |  |
| --- | --- |
| Unknown Computers Count | |
| Unknown | 4 |

# 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.

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. Due to the limited charset allowed, they are fairly easy to crack. Following accounts are affected:

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:

There are no accounts in ad.evotec.xyz that have no password set.

## Password Quality - Known passwords

Passwords of these accounts have been found in given dictionary. It's highely recommended to notify those users and ask them to change their passwords asap!

There were no passwords found that match given dictionary.

## Password Quality - Default Computer Password

These computer objects have their password set to default:

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.

There were no accounts found that does not require password.

## 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.

There are no accounts in ad.evotec.xyz that never expire.

## Password Quality - AES Keys Missing

Following accounts have their Kerberos AES keys missing

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

## Password Quality - Kerberos Pre-Auth Not Required

Kerberos pre-authentication is not required for these accounts

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

## Password Quality - Only DES Encryption Allowed

Only DES encryption is allowed to be used with these accounts

There are no account that require only DES encryption.

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

No accounts were found that are allowed to be delegated to a service.

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

There are no 2 passwords that are the same in ad.evotec.xyz.

## Password Quality - Leaked Passwords

Passwords of these accounts have been found in given HASH dictionary (https://haveibeenpwned.com/). It's highely recommended to notify those users and ask them to change their passwords asap!

There were no passwords found that match in given dictionary.

## Password Quality - Statistics

Following table and chart shows password statistics

|  |  |
| --- | --- |
| Name | Value |
| Clear Text Passwords | 0 |
| LM Hashes | 0 |
| Empty Passwords | 0 |
| 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 | 0 |
| Password Never Expires | 0 |
| AES Keys Missing | 0 |
| PreAuth Not Required | 0 |
| DES Encryption Only | 0 |
| Delegatable Admins | 0 |
| Duplicate Password Users | 0 |
| Duplicate Password Grouped | 0 |

# General Information - Domain ad.evotec.pl

# General Information - Domain Summary

Following domain exists within forest ad.evotec.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-1 | 192.168.240.189 |
| AD2 | AD2.ad.evotec.xyz | Windows Server 2016 Standard | KATOWICE-1 | 192.168.240.192 |

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

|  |  |
| --- | --- |
| FSMO Roles for ad.evotec.pl | |
| 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.pl

|  |  |
| --- | --- |
| Default Password Policy for ad.evotec.pl | |
| Complexity Enabled | True |
| Lockout Duration | 00:30:00 |
| Lockout Observation Window | 00:30:00 |
| Lockout Threshold | 0 |
| Max Password Age | 42.00:00:00 |
| Min Password Length | 7 |
| Min Password Age | 1.00:00:00 |
| Password History Count | 24 |
| Reversible Encryption Enabled | False |
| Distinguished Name | DC=ad,DC=evotec,DC=xyz |

# General Information - Fine Grained Password Policies

Following section should cover fine grained password policies. There were no fine grained password polices defined in ad.evotec.pl. There was no formal requirement to have them set up.

# General Information - Group Policies

Following table contains group policies for ad.evotec.pl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Display Name | Gpo Status | Creation Time | Modification Time | Description |
| ALL | Enable RDP | AllSettingsEnabled | 08/07/2018 12:47:44 | 08/07/2018 12:47:44 |  |
| ALL | PowerShell Settings | AllSettingsEnabled | 06/16/2018 12:19:39 | 06/16/2018 12:21:08 |  |
| COMPUTERS | Allow use of biometrics | AllSettingsEnabled | 05/20/2018 23:50:07 | 05/20/2018 23:51:22 |  |
| Default Domain Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 05/20/2018 09:59:46 |  |
| ALL | Bitlocker Settings | AllSettingsEnabled | 08/07/2018 12:22:23 | 08/07/2018 12:24:04 |  |
| DC | Event Log Settings | AllSettingsEnabled | 05/20/2018 10:13:53 | 12/29/2018 19:31:32 |  |
| DC | Event Log Audit Rules | AllSettingsEnabled | 05/20/2018 10:14:09 | 04/29/2019 13:40:06 |  |
| ALL | Firewall Settings | AllSettingsEnabled | 08/07/2018 16:42:25 | 08/07/2018 16:46:16 |  |
| COMPUTERS | Enable Sets | AllSettingsEnabled | 06/11/2018 13:06:51 | 06/11/2018 13:07:16 |  |
| Default Domain Controllers Policy | AllSettingsEnabled | 05/20/2018 09:55:29 | 08/05/2018 09:55:08 |  |
| Users | Synced Office 365 Users | AllSettingsEnabled | 11/19/2018 22:54:44 | 11/19/2018 23:54:44 | My comment |
| Test | AllSettingsEnabled | 12/27/2018 00:17:38 | 12/27/2018 01:17:38 |  |

# General Information - Group Policies Details

Following table contains group policies for ad.evotec.pl

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Name | Links | Has Computer Settings | Has User Settings | User Enabled |
| ALL | Enable RDP | ad.evotec.xyz | True | False | true |
| ALL | PowerShell Settings | ad.evotec.xyz | True | True | true |
| COMPUTERS | Allow use of biometrics |  | True | False | true |
| Default Domain Policy | ad.evotec.xyz | True | False | true |
| ALL | Bitlocker Settings | ad.evotec.xyz/Production/Computers ad.evotec.xyz/Production/Servers ad.evotec.xyz | True | False | true |
| DC | Event Log Settings | ad.evotec.xyz/Domain Controllers | True | False | true |
| DC | Event Log Audit Rules | ad.evotec.xyz/Domain Controllers | True | False | true |
| ALL | Firewall Settings | ad.evotec.xyz | True | False | true |
| COMPUTERS | Enable Sets | ad.evotec.xyz/Production/Computers ad.evotec.xyz | True | False | true |
| Default Domain Controllers Policy | ad.evotec.xyz/Domain Controllers | True | False | true |
| Users | Synced Office 365 Users | ad.evotec.xyz/Production/Users-O365 | False | False | true |
| Test |  | False | False | true |

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Target | NameTarget | Priority | Weight | Port |
| AD1.ad.evotec.xyz | AD1.ad.evotec.xyz | 0 | 100 | 88 |
| AD2.ad.evotec.xyz | AD2.ad.evotec.xyz | 0 | 100 | 88 |
| 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 |
| 192.168.240.189 | 192.168.240.189 | 192.168.240.189 | AD1.ad.evotec.xyz | A |
| 192.168.240.192 | 192.168.240.192 | 192.168.240.192 | AD2.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 |

# General Information - Organizational Units

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

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Canonical Name | Managed By | Manager Email | Protected | Description |
| ad.evotec.xyz/Domain Controllers |  |  | False | Default container for domain controllers |
| ad.evotec.xyz/Microsoft Exchange Security Groups |  |  | False |  |
| ad.evotec.xyz/Production |  |  | True |  |
| ad.evotec.xyz/Production/Computers |  |  | False |  |
| ad.evotec.xyz/Production/Contacts |  |  | True |  |
| ad.evotec.xyz/Production/Groups |  |  | True |  |
| ad.evotec.xyz/Production/Groups/SecurityGroups |  |  | True |  |
| ad.evotec.xyz/Production/Servers |  |  | True |  |
| ad.evotec.xyz/Production/Users |  |  | True |  |
| ad.evotec.xyz/Production/Users-O365 |  |  | True | OU for Synchronization of Users to Office 365 |
| ad.evotec.xyz/Production/Users-Offboarded |  |  | 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 |
| 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.pl

# General Information - Users Count

Following table and chart shows number of users in its categories

|  |  |
| --- | --- |
| Users Count | |
| Users Count Incl. System | 49 |
| Users Count | 45 |
| Users Expired | 4 |
| Users Expired Incl. Disabled | 15 |
| Users Never Expiring | 15 |
| Users Never Expiring Incl. Disabled | 28 |
| Users System Accounts | 4 |

# 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 |
| Temporary Admin | Temporary Admin | TemporaryAdmin@ad.evotec.xyz | TemporaryAdmin |  |
| Service Task Scheduler | Service Task Scheduler | svcTaskScheduler@ad.evotec.xyz | svcTaskScheduler |  |

# 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.pl

# General Information - Computers

Following table and chart shows number of computers and their versions

|  |  |
| --- | --- |
| Computers Count | |
| Windows 10 Enterprise | 2 |
| Windows 10 Pro | 1 |
| 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 | 1 |

# General Information - Unknown Computers

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

|  |  |
| --- | --- |
| Unknown Computers Count | |
| Unknown | 4 |

# 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

Passwords of these accounts are stored using 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. Due to the limited charset allowed, they are fairly easy to crack. Following accounts are affected:

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:

There are no accounts in ad.evotec.pl that have no password set.

## Password Quality - Known passwords

Passwords of these accounts have been found in given dictionary. It's highely recommended to notify those users and ask them to change their passwords asap!

There were no passwords found that match given dictionary.

## Password Quality - Default Computer Password

These computer objects have their password set to default:

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.

There were no accounts found that does not require password.

## 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.

There are no accounts in ad.evotec.pl that never expire.

## Password Quality - AES Keys Missing

Following accounts have their Kerberos AES keys missing

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

## Password Quality - Kerberos Pre-Auth Not Required

Kerberos pre-authentication is not required for these accounts

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

## Password Quality - Only DES Encryption Allowed

Only DES encryption is allowed to be used with these accounts

There are no account that require only DES encryption.

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

No accounts were found that are allowed to be delegated to a service.

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

There are no 2 passwords that are the same in ad.evotec.pl.

## Password Quality - Leaked Passwords

Passwords of these accounts have been found in given HASH dictionary (https://haveibeenpwned.com/). It's highely recommended to notify those users and ask them to change their passwords asap!

There were no passwords found that match in given dictionary.

## Password Quality - Statistics

Following table and chart shows password statistics

|  |  |
| --- | --- |
| Name | Value |
| Clear Text Passwords | 0 |
| LM Hashes | 0 |
| Empty Passwords | 0 |
| 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 | 0 |
| Password Never Expires | 0 |
| AES Keys Missing | 0 |
| PreAuth Not Required | 0 |
| DES Encryption Only | 0 |
| Delegatable Admins | 0 |
| Duplicate Password Users | 0 |
| Duplicate Password Grouped | 0 |