# 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 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 6

g. General Information - DNS A/SRV Records 6

h. General Information - Trusts 6

i. General Information - Organizational Units 6

j. General Information - Priviliged Groups 6

k. General Information - Domain Users in 7

i. General Information - Users Count 7

ii. General Information - Domain Administrators 7

iii. General Information - Enterprise Administrators 7

l. General Information - Computer Objects in 7

i. General Information - Computers 7

ii. General Information - Servers 7

iii. General Information - Unknown Computers 7

m. Domain Password Quality 7

i. Password Quality - Passwords with Reversible Encryption 7

ii. Password Quality - Passwords with LM Hash 7

iii. Password Quality - Empty Passwords 7

iv. Password Quality - Known passwords 7

v. Password Quality - Default Computer Password 7

vi. Password Quality - Password Not Required 7

vii. Password Quality - Non expiring passwords 7

viii. Password Quality - AES Keys Missing 8

ix. Password Quality - Kerberos Pre-Auth Not Required 8

x. Password Quality - Only DES Encryption Allowed 8

xi. Password Quality - Delegatable to Service 8

xii. Password Quality - Groups of Users With Same Password 8

xiii. Password Quality - Leaked Passwords 8

xiv. Password Quality - Statistics 8

3. General Information - Domain ad.evotec.xyz 9

a. General Information - Domain Summary 9

b. General Information - Domain Controllers 9

c. General Information - Password Policies 9

d. General Information - Fine-grained Password Policies 9

e. General Information - Group Policies 9

f. General Information - Group Policies Details 9

g. General Information - DNS A/SRV Records 9

h. General Information - Trusts 9

i. General Information - Organizational Units 9

j. General Information - Priviliged Groups 9

k. General Information - Domain Users in 10

i. General Information - Users Count 10

ii. General Information - Domain Administrators 10

iii. General Information - Enterprise Administrators 10

l. General Information - Computer Objects in 10

i. General Information - Computers 10

ii. General Information - Servers 10

iii. General Information - Unknown Computers 10

m. Domain Password Quality 10

i. Password Quality - Passwords with Reversible Encryption 10

ii. Password Quality - Passwords with LM Hash 10

iii. Password Quality - Empty Passwords 10

iv. Password Quality - Known passwords 10

v. Password Quality - Default Computer Password 10

vi. Password Quality - Password Not Required 10

vii. Password Quality - Non expiring passwords 10

viii. Password Quality - AES Keys Missing 11

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

x. Password Quality - Only DES Encryption Allowed 11

xi. Password Quality - Delegatable to Service 11

xii. Password Quality - Groups of Users With Same Password 11

xiii. Password Quality - Leaked Passwords 11

xiv. Password Quality - Statistics 11

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 . 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 | 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 15:45:06 | 05/20/2018 09:55:23 |
| GLIWICE | Some description | False | 07/30/2018 15:44:34 | 07/21/2018 19:41:01 |
| KATOWICE-2 |  | False | 07/21/2018 19:41:53 | 07/21/2018 19:41:14 |
| MIKOLOW |  | False | 07/21/2018 19:41:36 | 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 15:28:11 | 07/29/2018 20:40:45 |
| 192.168.241.0/24 |  | False | 07/29/2018 20:41:00 | 07/29/2018 20:40:57 |
| 192.168.239.0/24 | This is my site | False | 07/30/2018 15:27:49 | 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.pl

# General Information - Domain Summary

Following domain exists within forest :

* Domain
  + Name for fully qualified domain name (FQDN):
  + Name for NetBIOS:

# General Information - Domain Controllers

Following table contains domain controllers

Following table contains FSMO servers with roles for domain

# General Information - Password Policies

Following table contains password policies for all users within

# General Information - Fine-grained Password Policies

# General Information - Group Policies

Following table contains group policies for

# General Information - Group Policies Details

Following table contains group policies for

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

Following table contains A records for Kerberos and LDAP

# General Information - Trusts

Following table contains trusts established with domains...

# General Information - Organizational Units

Following table contains all OU's created in

# General Information - Priviliged Groups

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

# General Information - Domain Users in

## General Information - Users Count

Following table and chart shows number of users in its categories

## General Information - Domain Administrators

## General Information - Enterprise Administrators

# General Information - Computer Objects in

## 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

## General Information - Unknown Computers

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

# Domain Password Quality

This section provides overview about password quality used in . 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.

## 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:

## Password Quality - Empty Passwords

Following accounts have no password set:

## Password Quality - Known passwords

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

## Password Quality - Default Computer Password

These computer objects have their password set to default:

## 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.

## 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.

## Password Quality - AES Keys Missing

Following accounts have their Kerberos AES keys missing

## Password Quality - Kerberos Pre-Auth Not Required

Kerberos pre-authentication is not required for these accounts

## Password Quality - Only DES Encryption Allowed

Only DES encryption is allowed to be used with these accounts

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

## Password Quality - Leaked Passwords

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

## Password Quality - Statistics

Following table and chart shows password statistics

# General Information - Domain ad.evotec.xyz

# General Information - Domain Summary

Following domain exists within forest :

* Domain
  + Name for fully qualified domain name (FQDN):
  + Name for NetBIOS:

# General Information - Domain Controllers

Following table contains domain controllers

Following table contains FSMO servers with roles for domain

# General Information - Password Policies

Following table contains password policies for all users within

# General Information - Fine-grained Password Policies

# General Information - Group Policies

Following table contains group policies for

# General Information - Group Policies Details

Following table contains group policies for

# General Information - DNS A/SRV Records

Following table contains SRV records for Kerberos and LDAP

Following table contains A records for Kerberos and LDAP

# General Information - Trusts

Following table contains trusts established with domains...

# General Information - Organizational Units

Following table contains all OU's created in

# General Information - Priviliged Groups

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

# General Information - Domain Users in

## General Information - Users Count

Following table and chart shows number of users in its categories

## General Information - Domain Administrators

## General Information - Enterprise Administrators

# General Information - Computer Objects in

## 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

## General Information - Unknown Computers

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

# Domain Password Quality

This section provides overview about password quality used in . 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.

## 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:

## Password Quality - Empty Passwords

Following accounts have no password set:

## Password Quality - Known passwords

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

## Password Quality - Default Computer Password

These computer objects have their password set to default:

## 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.

## 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.

## Password Quality - AES Keys Missing

Following accounts have their Kerberos AES keys missing

## Password Quality - Kerberos Pre-Auth Not Required

Kerberos pre-authentication is not required for these accounts

## Password Quality - Only DES Encryption Allowed

Only DES encryption is allowed to be used with these accounts

## Password Quality - Delegatable to Service

These accounts are allowed to be delegated to a service:

## Password Quality - Groups of Users With Same Password

Following groups of users have same passwords:

## Password Quality - Leaked Passwords

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

## Password Quality - Statistics

Following table and chart shows password statistics