KRBTGT account password reset

alitajran.com/krbtgt-password-reset

September 9, 2021

When was the last time you changed the KRBTGT account password? If you don’t know the answer, it most likely means it’s a bad sign. Did you know that Microsoft recommends resetting the KRBTGT account password at least every 180 days? In this article, we will look at the KRBTGT account and how to reset the password with a PowerShell script.

KRBTGT account

The KRBTGT account is a local default account that acts as a service account for the Key Distribution Center (KDC) service. This account cannot be deleted, and the account name cannot be changed. The KRBTGT account cannot be enabled in Active Directory.

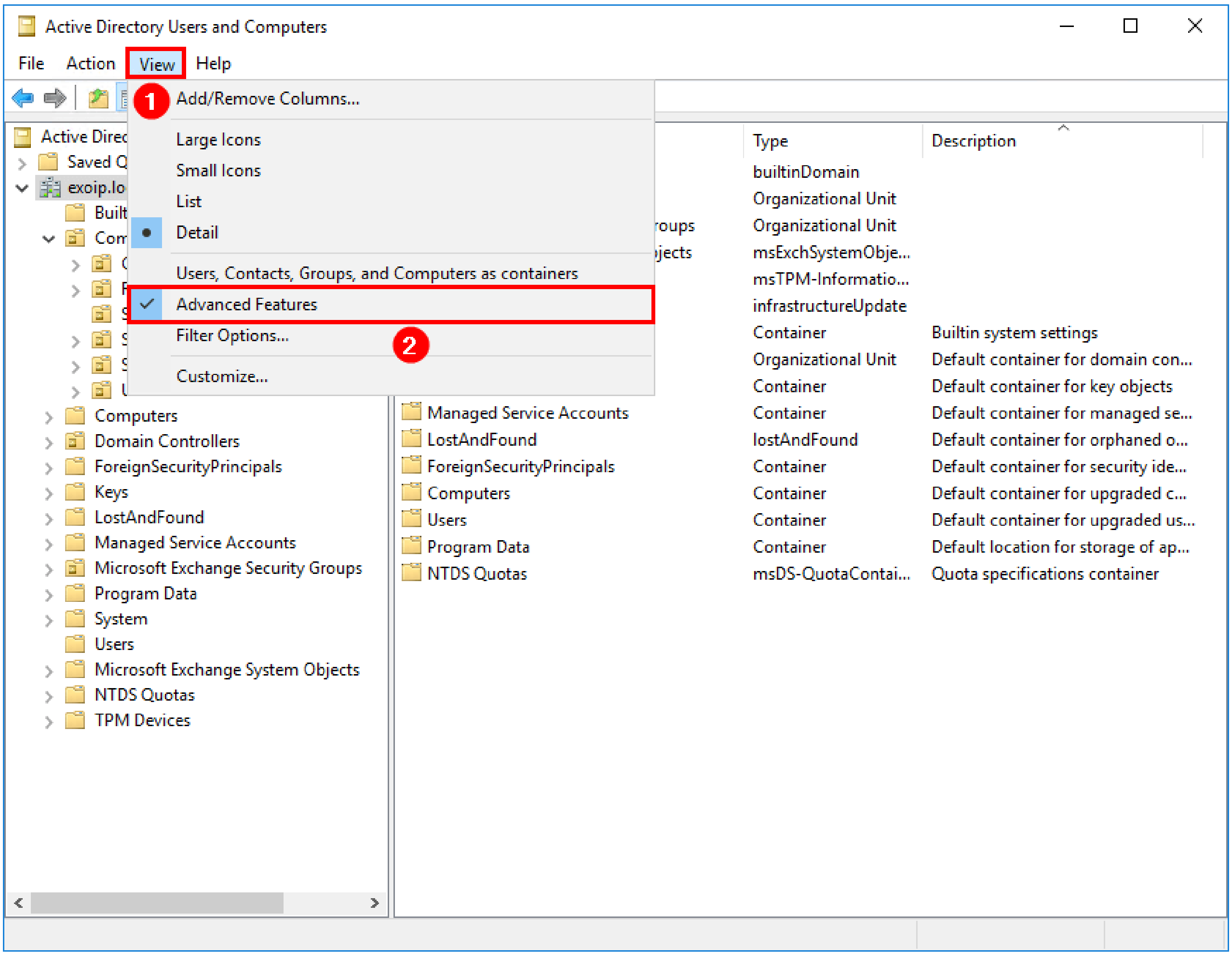
KRBTGT is also the security principal name used by the KDC for a Windows Server domain, as specified by RFC 4120. The KRBTGT account is the entity for the KRBTGT security principal, and it is created automatically when a new domain is created.

Note: You must reset the password for the KRBTGT account on a domain at least every 180 days.

Read the official Microsoft article about KRBTGT Account Password Reset Scripts now available for customers.

Check KRBTGT account password last set

Start Active Directory Users and Computers (ADUC). Click in the menu bar on **View** and enable **Advanced Features**.

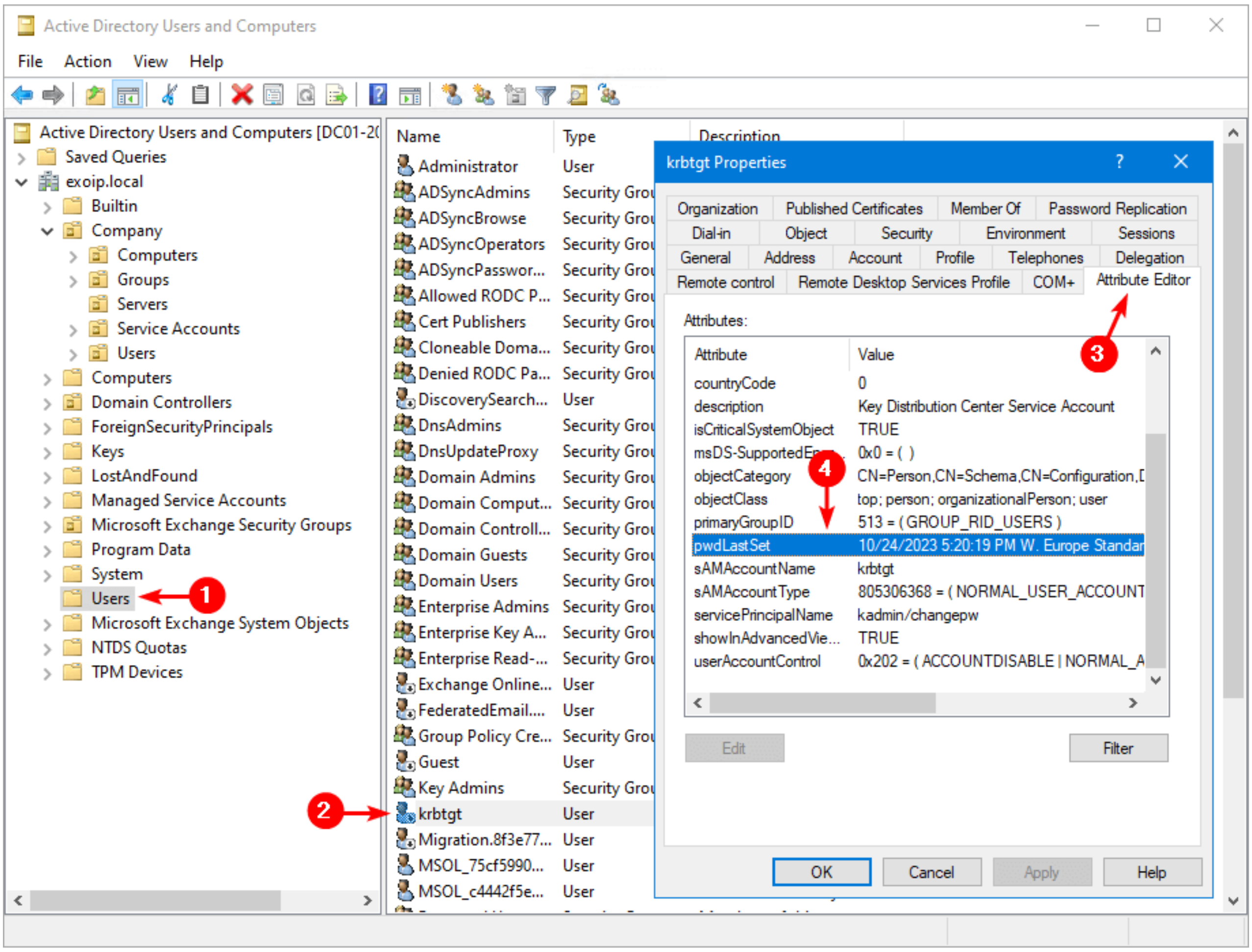


	Type	Description
	builtinDomain	
	Organizational Unit	
roups	Organizational Unit	
jects	msExchSystemObje...	
	msTPM-Informatio...	
	infrastructureUpdate	
	Container	Builtin system settings
	Organizational Unit	Default container for domain con...
	Container	Default container for key objects
Managed Service Accounts	Container	Default container for managed se...
LostAndFound	lostAndFound	Default container for orphaned o...
ForeignSecurityPrincipals	Container	Default container for security ide...
Computers	Container	Default container for upgraded c...
Users	Container	Default container for upgraded us...
Program Data	Container	Default location for storage of ap...
NTDS Quotas	msDS-QuotaContai...	Quota specifications container

Find the user object **krbtgt** and **double-click** on it to open the properties. Click the tab **Attribute Editor**. Find the attribute **pwdLastSet**.

Note: The SID for the KRBTGT account is *S-1-5-<domain>-502* and lives in the *Users OU* in the domain by default. Microsoft does not recommend moving this account to another OU.

In our example, the KRBTGT account was last set on 24 October 2023.



Attribute	Value
countryCode	0
description	Key Distribution Center Service Account
isCriticalSystemObject	TRUE
msDS-SupportedE...	0x0 = ( )
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	10/24/2023 5:20:19 PM W. Europe Standar
sAMAccountName	krbtgt
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	kadmin/changepw
showInAdvancedVie...	TRUE
userAccountControl	0x202 = (ACCOUNTDISABLE | NORMAL_A

Another way to check the KRBTGT account **password last set** time is to run Get-ADUser cmdlet in PowerShell.

```
Get-ADUser "krbtgt" -Property Created, PasswordLastSet
```

The output below appears with the details.

```
Created           : 5/1/2023 12:31:55 PM
DistinguishedName : CN=krbtgt,CN=Users,DC=exoip,DC=local
Enabled           : False
GivenName         :
Name              : krbtgt
ObjectClass       : user
ObjectGUID        : d99a5ba6-f2ea-4a14-9b52-57bd425786a1
PasswordLastSet   : 10/24/2023 05:20:19 PM
SamAccountName    : krbtgt
SID               : S-1-5-21-1083891243-2317051905-4228426097-502
Surname           :
UserPrincipalName :
```

KRBTGT account password reset change frequency

How often do you need to reset the KRBTGT account password? Reset the password for the KRBTGT account a least every 180 days. The password must be changed twice to remove the password history effectively. Changing once, waiting for replication to complete, and changing again reduces the risk of issues. Changing twice in rapid succession forces clients to re-authenticate (including application services) but is desired if a compromise is suspected.

Important: We do not recommend scheduling the PowerShell script as an automated task as things can go wrong for multiple environmental reasons.

KRBTGT account password reset PowerShell script

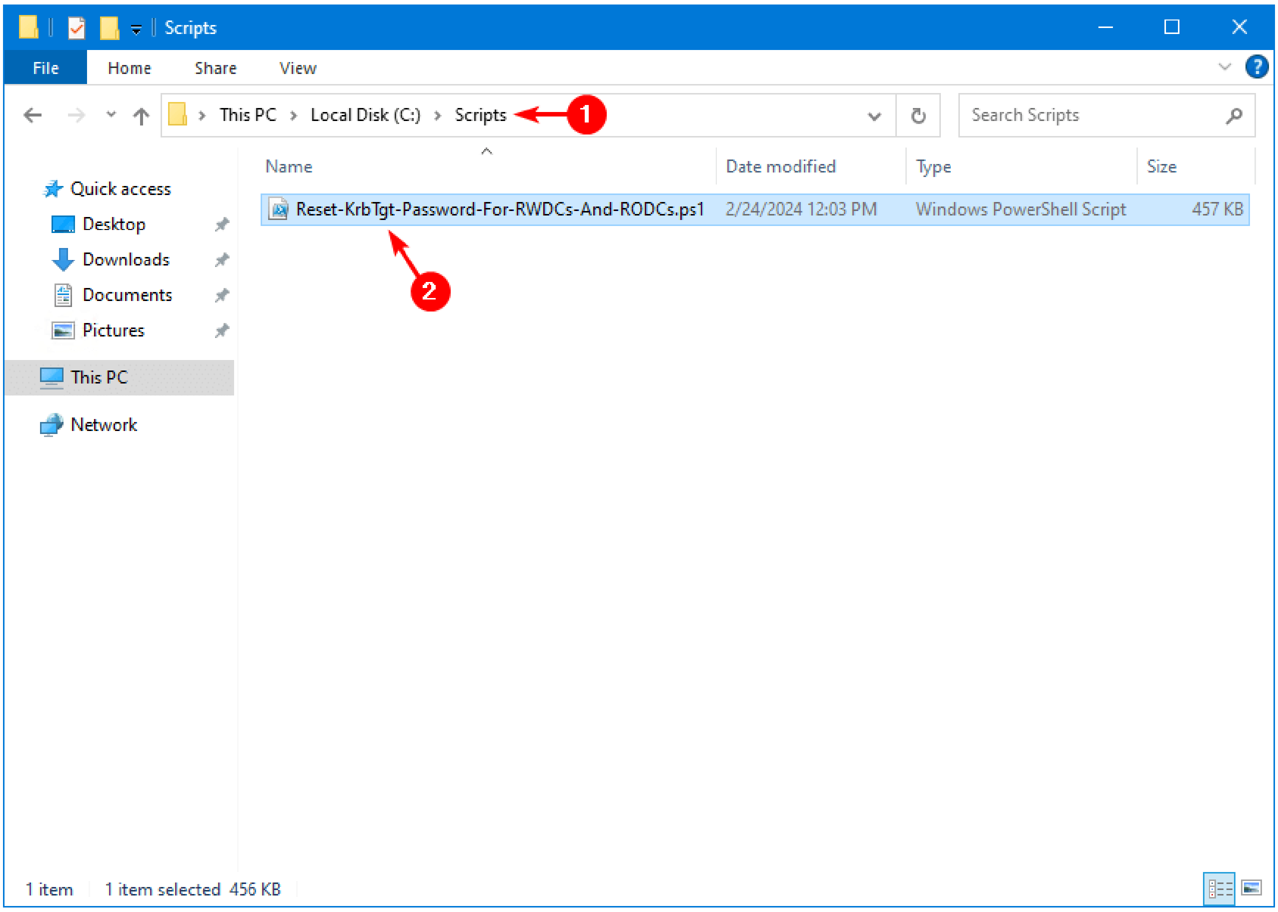
Sign in to the Doman Controller or Management Server.

Download the KRBTGT password reset script from GitHub or direct. The official script name is *Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1*. At the moment of writing, it's on **version 3.4**.

Ensure the file is unblocked to prevent errors when running the script. Read more in the article Not digitally signed error when running PowerShell script.

Note: Version 1 was written by Jared Poeppelman (Microsoft). After that, Jorge de Almeida Pintore rewrote the script, added tons of features, and that's how the new version was born. We recommend using version 3.

Place the script in the **C:\Scripts** folder. Create a **Scripts** folder if you don't have one.



This PC > Local Disk (C:) > Scripts

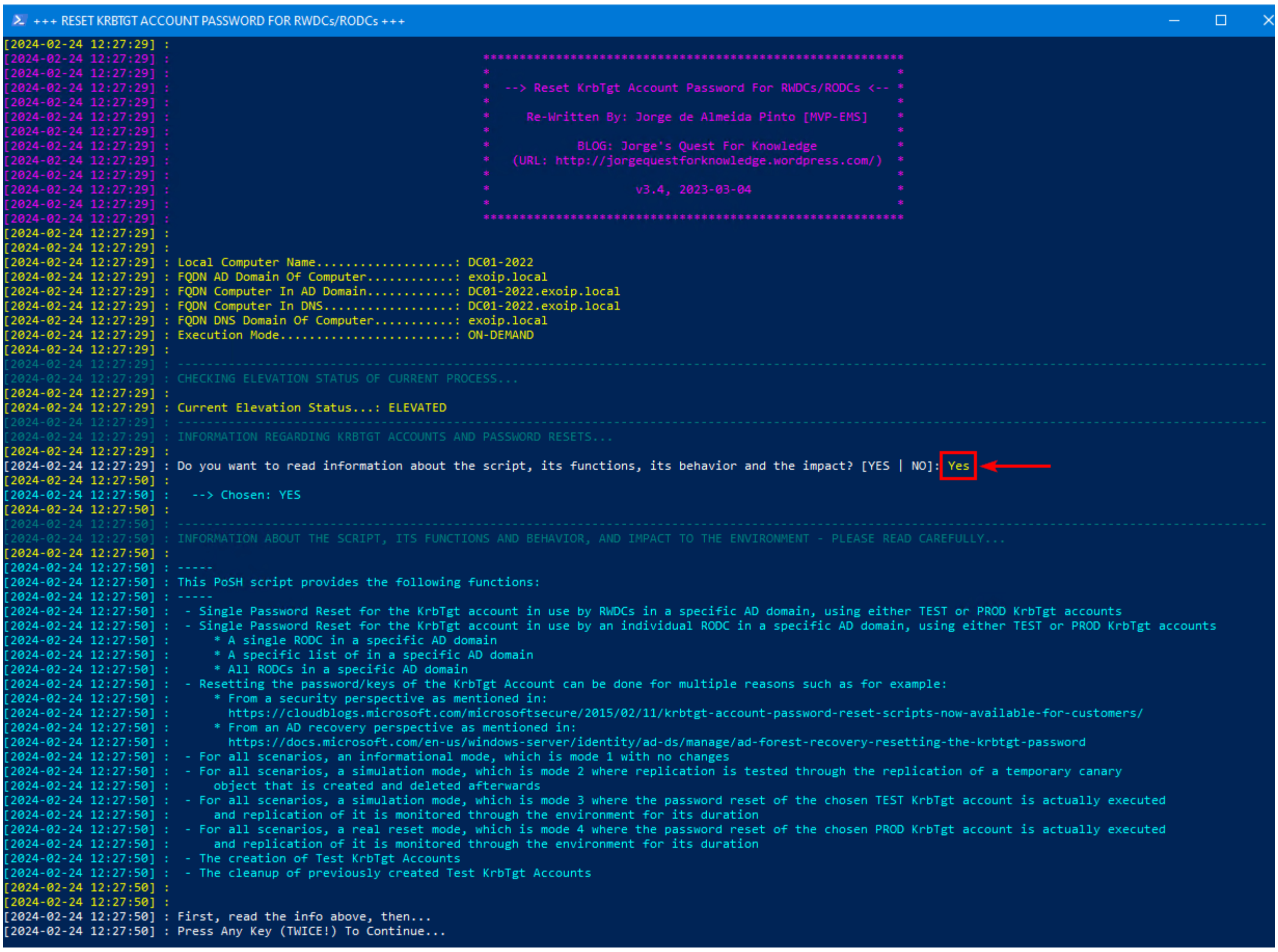
Name	Date modified	Type	Size
Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1	2/24/2024 12:03 PM	Windows PowerShell Script	457 KB

1 item 1 item selected 456 KB

Run Windows PowerShell as administrator and run the script.

```
C:\scripts\.\Reset-KrbTgt-Password-For-RWDCs-And-RODCs.ps1
```

The KRBTGT password reset script will present if you want to read the script's information, functions, behavior, and impact. Click **Yes** and go through the information.

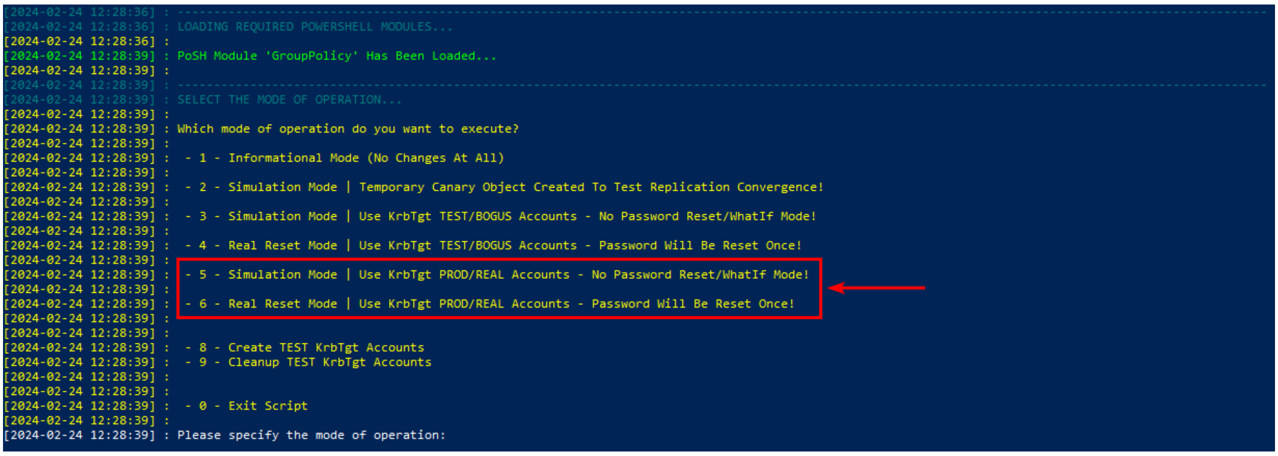


```
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] :                                          **********************************************************
[2024-02-24 12:27:29] :                                          *                                                        *
[2024-02-24 12:27:29] :                                          *  --> Reset KrbTgt Account Password For RWDCs/RODCs <-- *
[2024-02-24 12:27:29] :                                          *                                                        *
[2024-02-24 12:27:29] :                                          *     Re-Written By: Jorge de Almeida Pinto [MVP-EMS]    *
[2024-02-24 12:27:29] :                                          *                                                        *
[2024-02-24 12:27:29] :                                          *            BLOG: Jorge's Quest For Knowledge           *
[2024-02-24 12:27:29] :                                          *   (URL: http://jorgequestforknowledge.wordpress.com/)  *
[2024-02-24 12:27:29] :                                          *                                                        *
[2024-02-24 12:27:29] :                                          *                    v3.4, 2023-03-04                    *
[2024-02-24 12:27:29] :                                          *                                                        *
[2024-02-24 12:27:29] :                                          **********************************************************
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] : Local Computer Name...................: DC01-2022
[2024-02-24 12:27:29] : FQDN AD Domain Of Computer............: exoip.local
[2024-02-24 12:27:29] : FQDN Computer In AD Domain............: DC01-2022.exoip.local
[2024-02-24 12:27:29] : FQDN Computer In DNS..................: DC01-2022.exoip.local
[2024-02-24 12:27:29] : FQDN DNS Domain Of Computer...........: exoip.local
[2024-02-24 12:27:29] : Execution Mode........................: ON-DEMAND
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:27:29] : CHECKING ELEVATION STATUS OF CURRENT PROCESS...
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] : Current Elevation Status...: ELEVATED
[2024-02-24 12:27:29] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:27:29] : INFORMATION REGARDING KRBTGT ACCOUNTS AND PASSWORD RESETS...
[2024-02-24 12:27:29] :
[2024-02-24 12:27:29] : Do you want to read information about the script, its functions, its behavior and the impact? [YES | NO]: Yes
[2024-02-24 12:27:50] :
[2024-02-24 12:27:50] :   --> Chosen: YES
[2024-02-24 12:27:50] :
[2024-02-24 12:27:50] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:27:50] : INFORMATION ABOUT THE SCRIPT, ITS FUNCTIONS AND BEHAVIOR, AND IMPACT TO THE ENVIRONMENT - PLEASE READ CAREFULLY...
[2024-02-24 12:27:50] :
[2024-02-24 12:27:50] : -----
[2024-02-24 12:27:50] : This PoSH script provides the following functions:
[2024-02-24 12:27:50] : -----
[2024-02-24 12:27:50] :  - Single Password Reset for the KrbTgt account in use by RWDCs in a specific AD domain, using either TEST or PROD KrbTgt accounts
[2024-02-24 12:27:50] :  - Single Password Reset for the KrbTgt account in use by an individual RODC in a specific AD domain, using either TEST or PROD KrbTgt accounts
[2024-02-24 12:27:50] :     * A single RODC in a specific AD domain
[2024-02-24 12:27:50] :     * A specific list of in a specific AD domain
[2024-02-24 12:27:50] :     * All RODCs in a specific AD domain
[2024-02-24 12:27:50] :  - Resetting the password/keys of the KrbTgt Account can be done for multiple reasons such as for example:
[2024-02-24 12:27:50] :     * From a security perspective as mentioned in:
[2024-02-24 12:27:50] :       https://cloudblogs.microsoft.com/microsoftsecure/2015/02/11/krbtgt-account-password-reset-scripts-now-available-for-customers/
[2024-02-24 12:27:50] :     * From an AD recovery perspective as mentioned in:
[2024-02-24 12:27:50] :       https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/manage/ad-forest-recovery-resetting-the-krbtgt-password
[2024-02-24 12:27:50] :  - For all scenarios, an informational mode, which is mode 1 with no changes
[2024-02-24 12:27:50] :  - For all scenarios, a simulation mode, which is mode 2 where replication is tested through the replication of a temporary canary
[2024-02-24 12:27:50] :     object that is created and deleted afterwards
[2024-02-24 12:27:50] :  - For all scenarios, a simulation mode, which is mode 3 where the password reset of the chosen TEST KrbTgt account is actually executed
[2024-02-24 12:27:50] :     and replication of it is monitored through the environment for its duration
[2024-02-24 12:27:50] :  - For all scenarios, a real reset mode, which is mode 4 where the password reset of the chosen PROD KrbTgt account is actually executed
[2024-02-24 12:27:50] :     and replication of it is monitored through the environment for its duration
[2024-02-24 12:27:50] :  - The creation of Test KrbTgt Accounts
[2024-02-24 12:27:50] :  - The cleanup of previously created Test KrbTgt Accounts
[2024-02-24 12:27:50] :
[2024-02-24 12:27:50] :
[2024-02-24 12:27:50] : First, read the info above, then...
[2024-02-24 12:27:50] : Press Any Key (TWICE!) To Continue...
```

When you finish reading through the information, you will see **9 options** to select.

The ones that we will use are:

- **5 – Simulation Mode** | Use KrbTgt PROD/REAL Accounts – No Password Reset/WhatIf Mode!
- **6 – Real Reset Mode** | Use KrbTgt PROD/REAL Accounts – Password Will Be Reset Once!



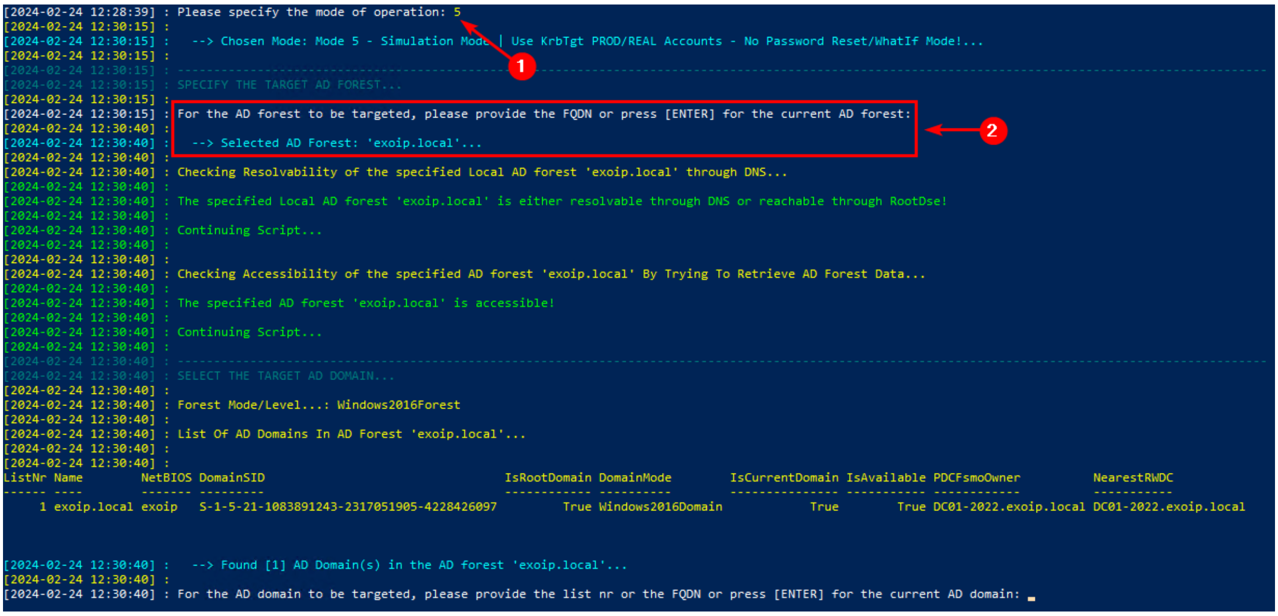
```
[2024-02-24 12:28:36] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:28:36] : LOADING REQUIRED POWERSHELL MODULES...
[2024-02-24 12:28:36] :
[2024-02-24 12:28:39] : PoSH Module 'GroupPolicy' Has Been Loaded...
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:28:39] : SELECT THE MODE OF OPERATION...
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] : Which mode of operation do you want to execute?
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 1 - Informational Mode (No Changes At All)
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 2 - Simulation Mode | Temporary Canary Object Created To Test Replication Convergence!
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 3 - Simulation Mode | Use KrbTgt TEST/BOGUS Accounts - No Password Reset/WhatIf Mode!
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 4 - Real Reset Mode | Use KrbTgt TEST/BOGUS Accounts - Password Will Be Reset Once!
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 5 - Simulation Mode | Use KrbTgt PROD/REAL Accounts - No Password Reset/WhatIf Mode!
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 6 - Real Reset Mode | Use KrbTgt PROD/REAL Accounts - Password Will Be Reset Once!
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 8 - Create TEST KrbTgt Accounts
[2024-02-24 12:28:39] :  - 9 - Cleanup TEST KrbTgt Accounts
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] :  - 0 - Exit Script
[2024-02-24 12:28:39] :
[2024-02-24 12:28:39] : Please specify the mode of operation:
```

Note: Option 5 will do nothing to the environment and will only show you all the details of what will happen. Option 6 will reset the KRBTGT password.

Simulation mode

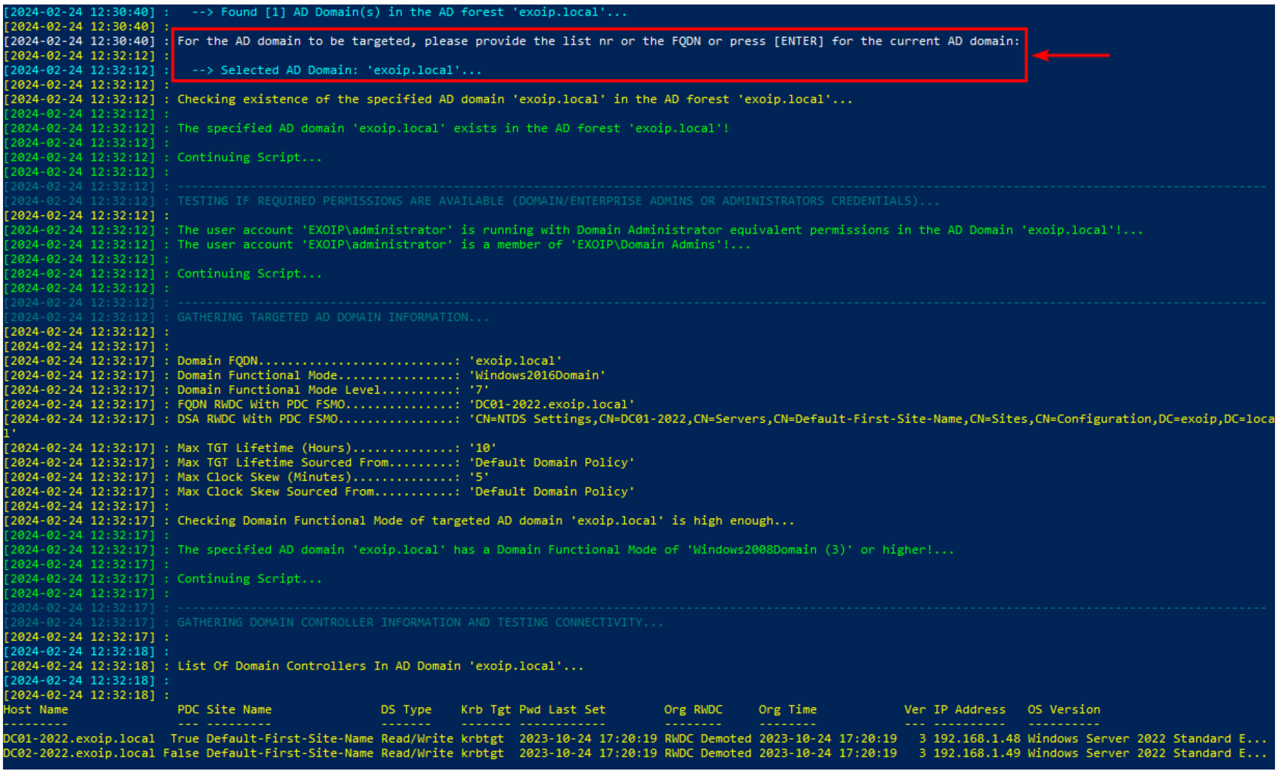
Press option **5**.

Fill in the AD forest FQDN that will be targeted, or press enter for the current AD forest. We like to target the forest *exoip.local*, which we are on now. After that, press **Enter**.



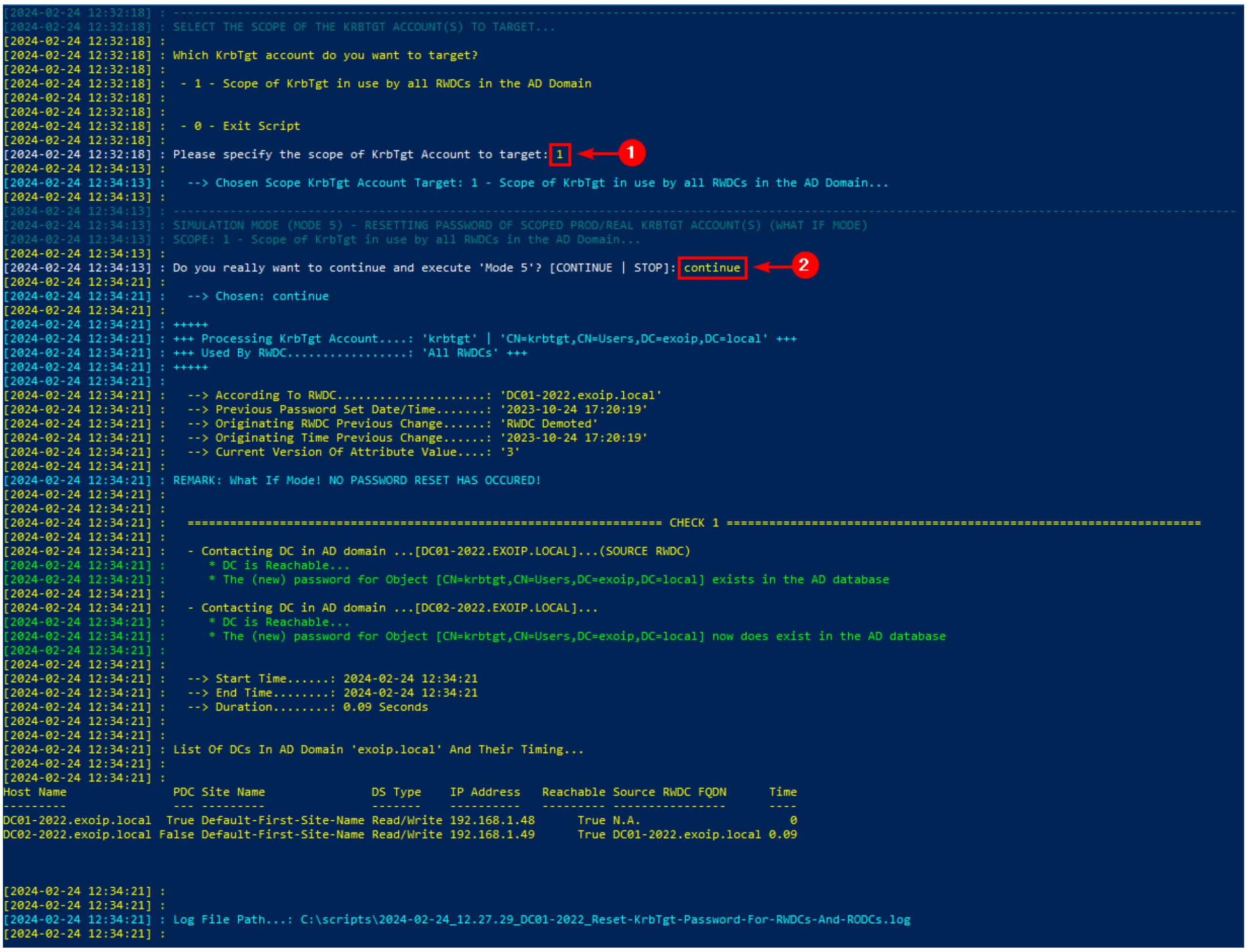
```
[2024-02-24 12:28:39] : Please specify the mode of operation: 5
[2024-02-24 12:30:15] :
[2024-02-24 12:30:15] :   --> Chosen Mode: Mode 5 - Simulation Mode | Use KrbTgt PROD/REAL Accounts - No Password Reset/WhatIf Mode!...
[2024-02-24 12:30:15] :
[2024-02-24 12:30:15] : ---------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:30:15] : SPECIFY THE TARGET AD FOREST...
[2024-02-24 12:30:15] :
[2024-02-24 12:30:15] : For the AD forest to be targeted, please provide the FQDN or press [ENTER] for the current AD forest:
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] :   --> Selected AD Forest: 'exoip.local'...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : Checking Resolvability of the specified Local AD forest 'exoip.local' through DNS...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : The specified Local AD forest 'exoip.local' is either resolvable through DNS or reachable through RootDse!
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : Continuing Script...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : Checking Accessibility of the specified AD forest 'exoip.local' By Trying To Retrieve AD Forest Data...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : The specified AD forest 'exoip.local' is accessible!
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : Continuing Script...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : ---------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:30:40] : SELECT THE TARGET AD DOMAIN...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : Forest Mode/Level...: Windows2016Forest
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : List Of AD Domains In AD Forest 'exoip.local'...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] :
ListNr Name        NetBIOS DomainSID                                IsRootDomain DomainMode       IsCurrentDomain IsAvailable PDCFsmoOwner         NearestRWDC
------ ----        ------- ---------                                ------------ ----------       --------------- ----------- ------------         -----------
     1 exoip.local exoip   S-1-5-21-1083891243-2317051905-4228426097         True Windows2016Domain            True        True DC01-2022.exoip.local DC01-2022.exoip.local


[2024-02-24 12:30:40] :   --> Found [1] AD Domain(s) in the AD forest 'exoip.local'...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : For the AD domain to be targeted, please provide the list nr or the FQDN or press [ENTER] for the current AD domain: _
```

Fill in the AD domain FQDN that will be targeted, or press enter for the current domain. We like to target the domain *exoip.local*, which we are on now. After that, press **Enter**.



```
[2024-02-24 12:30:40] :   --> Found [1] AD Domain(s) in the AD forest 'exoip.local'...
[2024-02-24 12:30:40] :
[2024-02-24 12:30:40] : For the AD domain to be targeted, please provide the list nr or the FQDN or press [ENTER] for the current AD domain:
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] :   --> Selected AD Domain: 'exoip.local'...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : Checking existence of the specified AD domain 'exoip.local' in the AD forest 'exoip.local'...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : The specified AD domain 'exoip.local' exists in the AD forest 'exoip.local'!
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : Continuing Script...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : ---------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:32:12] : TESTING IF REQUIRED PERMISSIONS ARE AVAILABLE (DOMAIN/ENTERPRISE ADMINS OR ADMINISTRATORS CREDENTIALS)...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : The user account 'EXOIP\administrator' is running with Domain Administrator equivalent permissions in the AD Domain 'exoip.local'!...
[2024-02-24 12:32:12] : The user account 'EXOIP\administrator' is a member of 'EXOIP\Domain Admins'!...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : Continuing Script...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:12] : ---------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:32:12] : GATHERING TARGETED AD DOMAIN INFORMATION...
[2024-02-24 12:32:12] :
[2024-02-24 12:32:17] :
[2024-02-24 12:32:17] : Domain FQDN..........................: 'exoip.local'
[2024-02-24 12:32:17] : Domain Functional Mode................: 'Windows2016Domain'
[2024-02-24 12:32:17] : Domain Functional Mode Level..........: '7'
[2024-02-24 12:32:17] : FQDN RWDC With PDC FSMO...............: 'DC01-2022.exoip.local'
[2024-02-24 12:32:17] : DSA RWDC With PDC FSMO................: 'CN=NTDS Settings,CN=DC01-2022,CN=Servers,CN=Default-First-Site-Name,CN=Sites,CN=Configuration,DC=exoip,DC=loca
l'
[2024-02-24 12:32:17] : Max TGT Lifetime (Hours)..............: '10'
[2024-02-24 12:32:17] : Max TGT Lifetime Sourced From.........: 'Default Domain Policy'
[2024-02-24 12:32:17] : Max Clock Skew (Minutes)..............: '5'
[2024-02-24 12:32:17] : Max Clock Skew Sourced From...........: 'Default Domain Policy'
[2024-02-24 12:32:17] :
[2024-02-24 12:32:17] : Checking Domain Functional Mode of targeted AD domain 'exoip.local' is high enough...
[2024-02-24 12:32:17] :
[2024-02-24 12:32:17] : The specified AD domain 'exoip.local' has a Domain Functional Mode of 'Windows2008Domain (3)' or higher!...
[2024-02-24 12:32:17] :
[2024-02-24 12:32:17] : Continuing Script...
[2024-02-24 12:32:17] :
[2024-02-24 12:32:17] : ---------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:32:17] : GATHERING DOMAIN CONTROLLER INFORMATION AND TESTING CONNECTIVITY...
[2024-02-24 12:32:17] :
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] : List Of Domain Controllers In AD Domain 'exoip.local'...
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] :
Host Name               PDC Site Name              DS Type    Krb Tgt Pwd Last Set        Org RWDC     Org Time            Ver IP Address   OS Version
---------               --- ---------              -------    ------- ------------        --------     --------            --- ----------   ----------
DC01-2022.exoip.local  True Default-First-Site-Name Read/Write krbtgt  2023-10-24 17:20:19 RWDC Demoted 2023-10-24 17:20:19   3 192.168.1.48 Windows Server 2022 Standard E...
DC02-2022.exoip.local False Default-First-Site-Name Read/Write krbtgt  2023-10-24 17:20:19 RWDC Demoted 2023-10-24 17:20:19   3 192.168.1.49 Windows Server 2022 Standard E...
```

Select which KRBTGT account you want to target. Select **1**. Type **Continue** and press **Enter**.



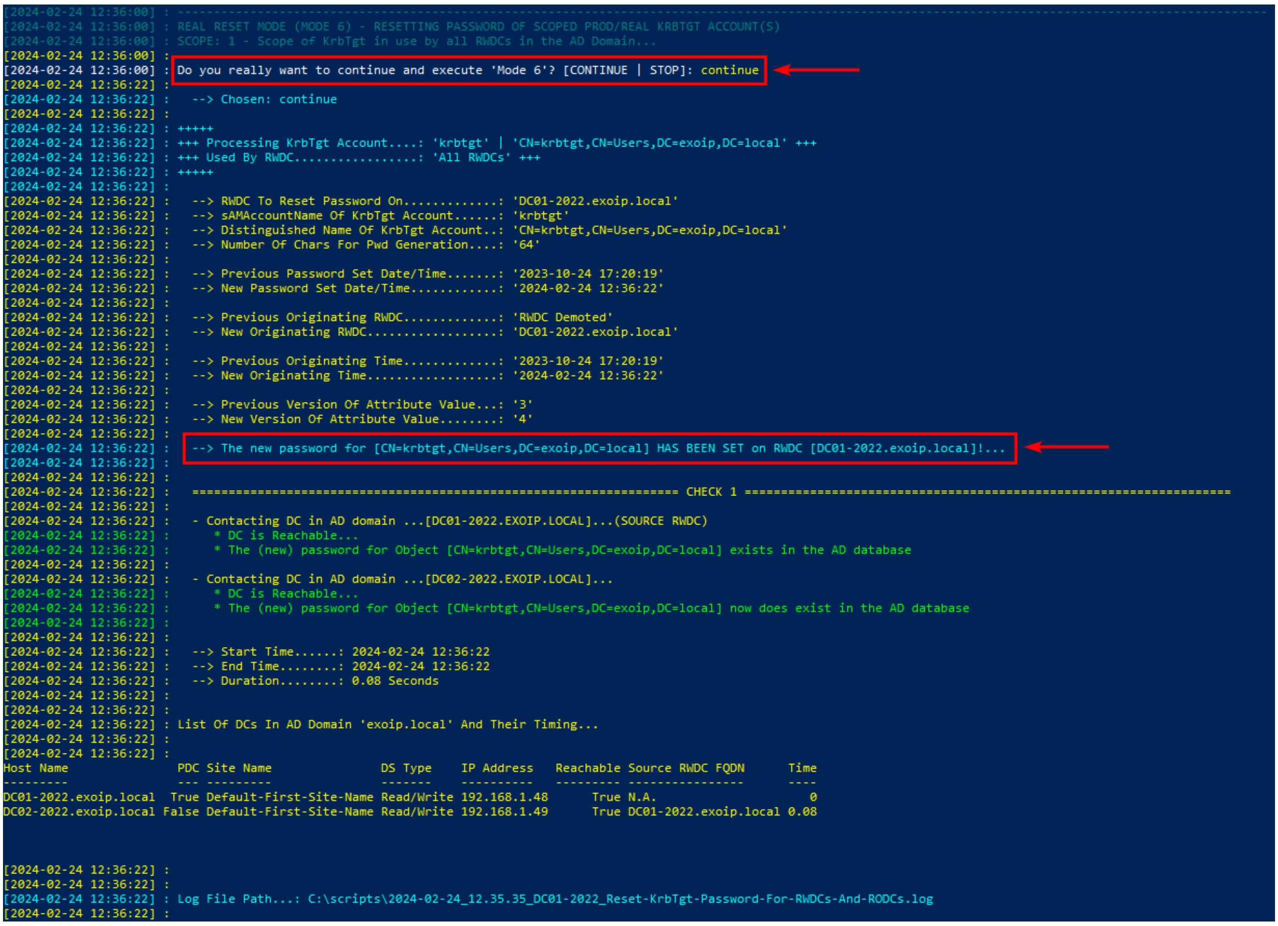
```
[2024-02-24 12:32:18] : ----------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:32:18] : SELECT THE SCOPE OF THE KRBTGT ACCOUNT(S) TO TARGET...
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] : Which KrbTgt account do you want to target?
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] :  - 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] :  - 0 - Exit Script
[2024-02-24 12:32:18] :
[2024-02-24 12:32:18] : Please specify the scope of KrbTgt Account to target: 1
[2024-02-24 12:34:13] :
[2024-02-24 12:34:13] :   --> Chosen Scope KrbTgt Account Target: 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain...
[2024-02-24 12:34:13] :
[2024-02-24 12:34:13] : ----------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:34:13] : SIMULATION MODE (MODE 5) - RESETTING PASSWORD OF SCOPED PROD/REAL KRBTGT ACCOUNT(S) (WHAT IF MODE)
[2024-02-24 12:34:13] : SCOPE: 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain...
[2024-02-24 12:34:13] :
[2024-02-24 12:34:13] : Do you really want to continue and execute 'Mode 5'? [CONTINUE | STOP]: continue
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   --> Chosen: continue
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] : +++++
[2024-02-24 12:34:21] : +++ Processing KrbTgt Account....: 'krbtgt' | 'CN=krbtgt,CN=Users,DC=exoip,DC=local' +++
[2024-02-24 12:34:21] : +++ Used By RWDC.................: 'All RWDCs' +++
[2024-02-24 12:34:21] : +++++
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   --> According To RWDC.....................: 'DC01-2022.exoip.local'
[2024-02-24 12:34:21] :   --> Previous Password Set Date/Time.......: '2023-10-24 17:20:19'
[2024-02-24 12:34:21] :   --> Originating RWDC Previous Change......: 'RWDC Demoted'
[2024-02-24 12:34:21] :   --> Originating Time Previous Change......: '2023-10-24 17:20:19'
[2024-02-24 12:34:21] :   --> Current Version Of Attribute Value....: '3'
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] : REMARK: What If Mode! NO PASSWORD RESET HAS OCCURED!
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   ================================================================== CHECK 1 ==================================================================
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   - Contacting DC in AD domain ...[DC01-2022.EXOIP.LOCAL]...(SOURCE RWDC)
[2024-02-24 12:34:21] :      * DC is Reachable...
[2024-02-24 12:34:21] :      * The (new) password for Object [CN=krbtgt,CN=Users,DC=exoip,DC=local] exists in the AD database
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   - Contacting DC in AD domain ...[DC02-2022.EXOIP.LOCAL]...
[2024-02-24 12:34:21] :      * DC is Reachable...
[2024-02-24 12:34:21] :      * The (new) password for Object [CN=krbtgt,CN=Users,DC=exoip,DC=local] now does exist in the AD database
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :   --> Start Time......: 2024-02-24 12:34:21
[2024-02-24 12:34:21] :   --> End Time........: 2024-02-24 12:34:21
[2024-02-24 12:34:21] :   --> Duration........: 0.09 Seconds
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] : List Of DCs In AD Domain 'exoip.local' And Their Timing...
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :
Host Name               PDC Site Name                DS Type    IP Address   Reachable Source RWDC FQDN      Time
---------               --- ---------                -------    ----------   --------- ----------------      ----
DC01-2022.exoip.local  True Default-First-Site-Name Read/Write 192.168.1.48      True N.A.                     0
DC02-2022.exoip.local False Default-First-Site-Name Read/Write 192.168.1.49      True DC01-2022.exoip.local 0.09



[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] :
[2024-02-24 12:34:21] : Log File Path...: C:\scripts\2024-02-24_12.27.29_DC01-2022_Reset-KrbTgt-Password-For-RWDCs-And-RODCs.log
[2024-02-24 12:34:21] :
```

If everything looks good, proceed to the next step.

Real reset mode

Do the same steps as above. But, this time, press option **6**.

The output will show that a new password is set for the account KRBTGT.



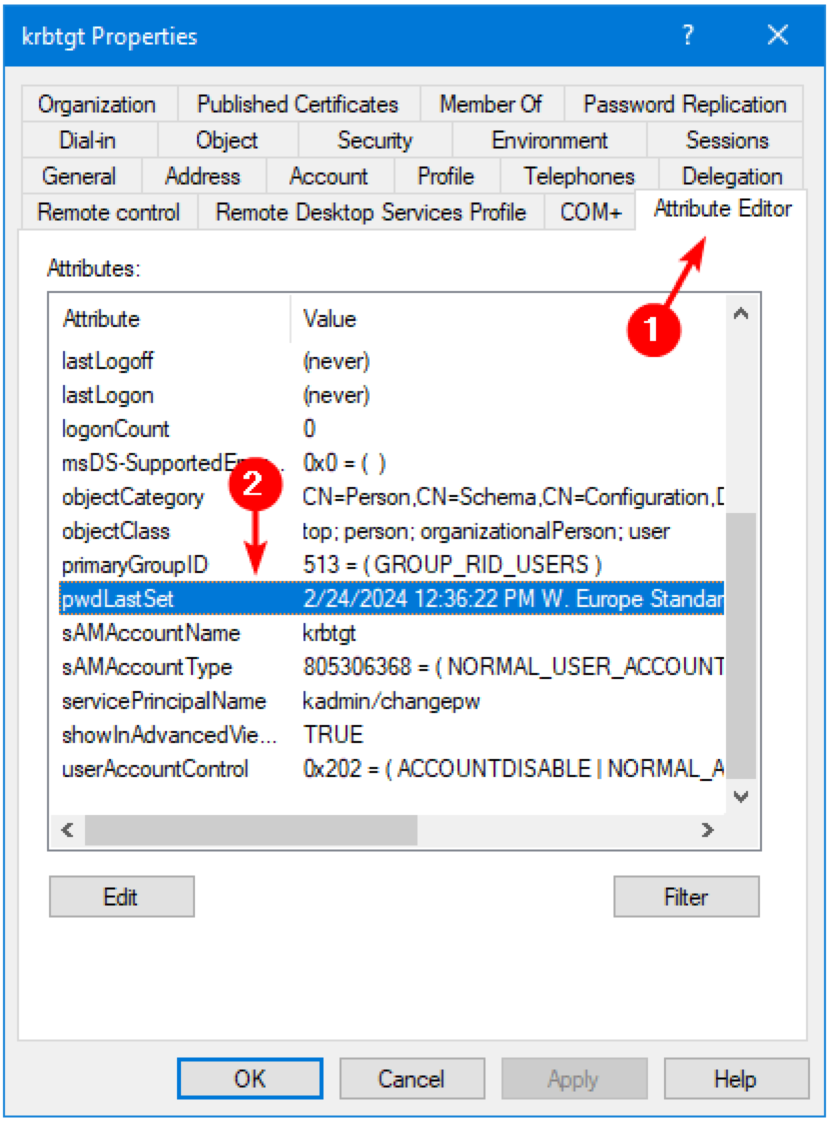
```
[2024-02-24 12:36:00] : ------------------------------------------------------------------------------------------------------------------------------------------------------
[2024-02-24 12:36:00] : REAL RESET MODE (MODE 6) - RESETTING PASSWORD OF SCOPED PROD/REAL KRBTGT ACCOUNT(S)
[2024-02-24 12:36:00] : SCOPE: 1 - Scope of KrbTgt in use by all RWDCs in the AD Domain...
[2024-02-24 12:36:00] :
[2024-02-24 12:36:00] : Do you really want to continue and execute 'Mode 6'? [CONTINUE | STOP]: continue
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Chosen: continue
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] : +++++
[2024-02-24 12:36:22] : +++ Processing KrbTgt Account....: 'krbtgt' | 'CN=krbtgt,CN=Users,DC=exoip,DC=local' +++
[2024-02-24 12:36:22] : +++ Used By RWDC.................: 'All RWDCs' +++
[2024-02-24 12:36:22] : +++++
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> RWDC To Reset Password On.............: 'DC01-2022.exoip.local'
[2024-02-24 12:36:22] :   --> sAMAccountName Of KrbTgt Account......: 'krbtgt'
[2024-02-24 12:36:22] :   --> Distinguished Name Of KrbTgt Account..: 'CN=krbtgt,CN=Users,DC=exoip,DC=local'
[2024-02-24 12:36:22] :   --> Number Of Chars For Pwd Generation....: '64'
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Previous Password Set Date/Time.......: '2023-10-24 17:20:19'
[2024-02-24 12:36:22] :   --> New Password Set Date/Time............: '2024-02-24 12:36:22'
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Previous Originating RWDC.............: 'RWDC Demoted'
[2024-02-24 12:36:22] :   --> New Originating RWDC..................: 'DC01-2022.exoip.local'
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Previous Originating Time.............: '2023-10-24 17:20:19'
[2024-02-24 12:36:22] :   --> New Originating Time..................: '2024-02-24 12:36:22'
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Previous Version Of Attribute Value...: '3'
[2024-02-24 12:36:22] :   --> New Version Of Attribute Value........: '4'
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> The new password for [CN=krbtgt,CN=Users,DC=exoip,DC=local] HAS BEEN SET on RWDC [DC01-2022.exoip.local]!...
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   =================================================================== CHECK 1 ===================================================================
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   - Contacting DC in AD domain ...[DC01-2022.EXOIP.LOCAL]...(SOURCE RWDC)
[2024-02-24 12:36:22] :      * DC is Reachable...
[2024-02-24 12:36:22] :      * The (new) password for Object [CN=krbtgt,CN=Users,DC=exoip,DC=local] exists in the AD database
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   - Contacting DC in AD domain ...[DC02-2022.EXOIP.LOCAL]...
[2024-02-24 12:36:22] :      * DC is Reachable...
[2024-02-24 12:36:22] :      * The (new) password for Object [CN=krbtgt,CN=Users,DC=exoip,DC=local] now does exist in the AD database
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :   --> Start Time......: 2024-02-24 12:36:22
[2024-02-24 12:36:22] :   --> End Time........: 2024-02-24 12:36:22
[2024-02-24 12:36:22] :   --> Duration........: 0.08 Seconds
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] : List Of DCs In AD Domain 'exoip.local' And Their Timing...
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :
Host Name               PDC Site Name               DS Type    IP Address   Reachable Source RWDC FQDN      Time
---------               --- ---------               -------    ----------   --------- ----------------      ----
DC01-2022.exoip.local  True Default-First-Site-Name Read/Write 192.168.1.48      True N.A.                     0
DC02-2022.exoip.local False Default-First-Site-Name Read/Write 192.168.1.49      True DC01-2022.exoip.local 0.08



[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] :
[2024-02-24 12:36:22] : Log File Path...: C:\scripts\2024-02-24_12.35.35_DC01-2022_Reset-KrbTgt-Password-For-RWDCs-And-RODCs.log
[2024-02-24 12:36:22] :
```

The KRBTGT account password reset script successfully set a new password for the KRBTGT account.

Verify KRBTGT account password has been set

Start Active Directory Users and Computers (ADUC). Find the user object **krbtgt** and **double-click** on it to open the properties. Click the tab **Attribute Editor**. Find the attribute **pwdLastSet**.

In our example, we can verify that the KRBTGT account was successfully reset on 24 February 2024 (today).

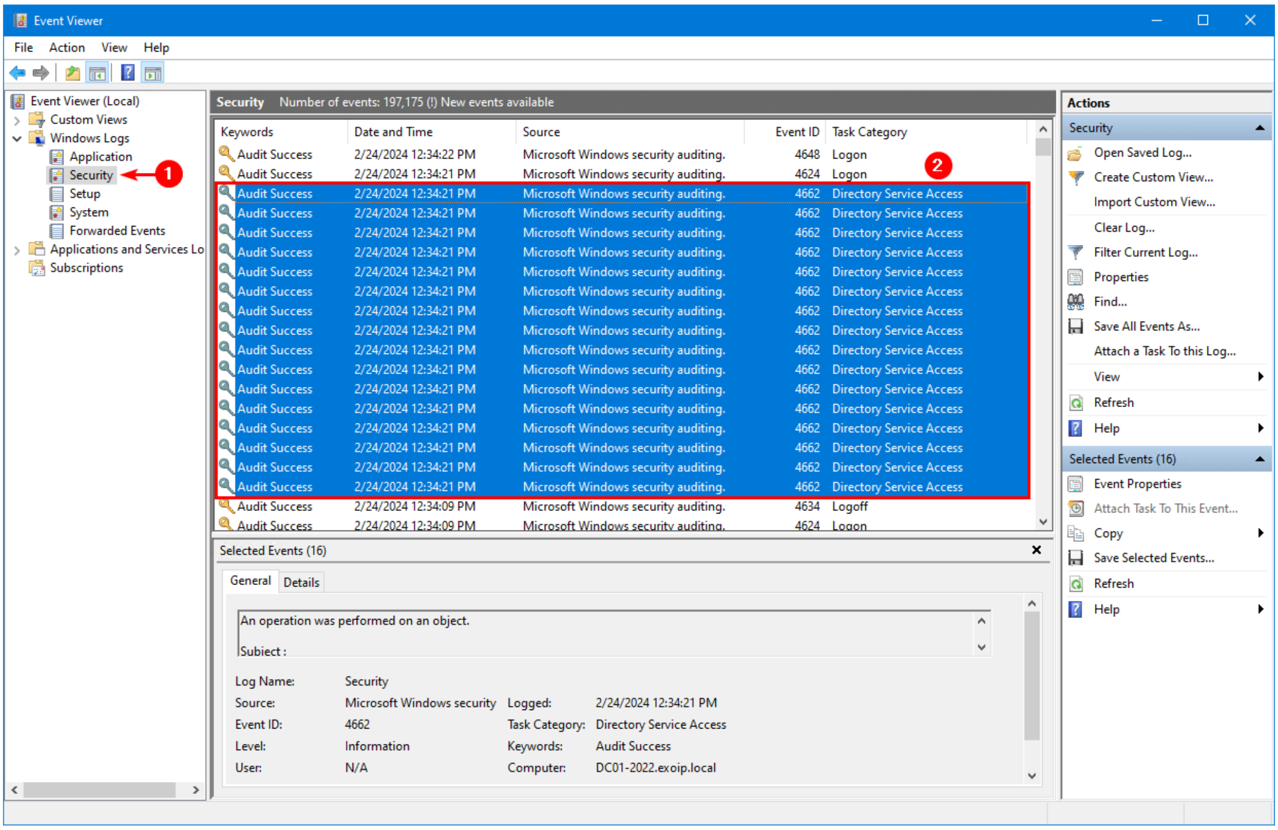


Attribute	Value
lastLogoff	(never)
lastLogon	(never)
logonCount	0
msDS-SupportedE...	0x0 = ( )
objectCategory	CN=Person,CN=Schema,CN=Configuration,D
objectClass	top; person; organizationalPerson; user
primaryGroupID	513 = (GROUP_RID_USERS)
pwdLastSet	2/24/2024 12:36:22 PM W. Europe Standar
sAMAccountName	krbtgt
sAMAccountType	805306368 = (NORMAL_USER_ACCOUNT
servicePrincipalName	kadmin/changepw
showInAdvancedVie...	TRUE
userAccountControl	0x202 = (ACCOUNTDISABLE | NORMAL_A

Check Windows Security event logs

After you run *Mode 5 – Simulation Mode*, the below events appear in the Security event logs:

Event **ID 4662**



Security Number of events: 197,175 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2024 12:34:22 PM	Microsoft Windows security auditing.	4648	Logon
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:21 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:34:09 PM	Microsoft Windows security auditing.	4634	Logoff
Audit Success	2/24/2024 12:34:09 PM	Microsoft Windows security auditing.	4624	Logon

Selected Events (16)

General Details

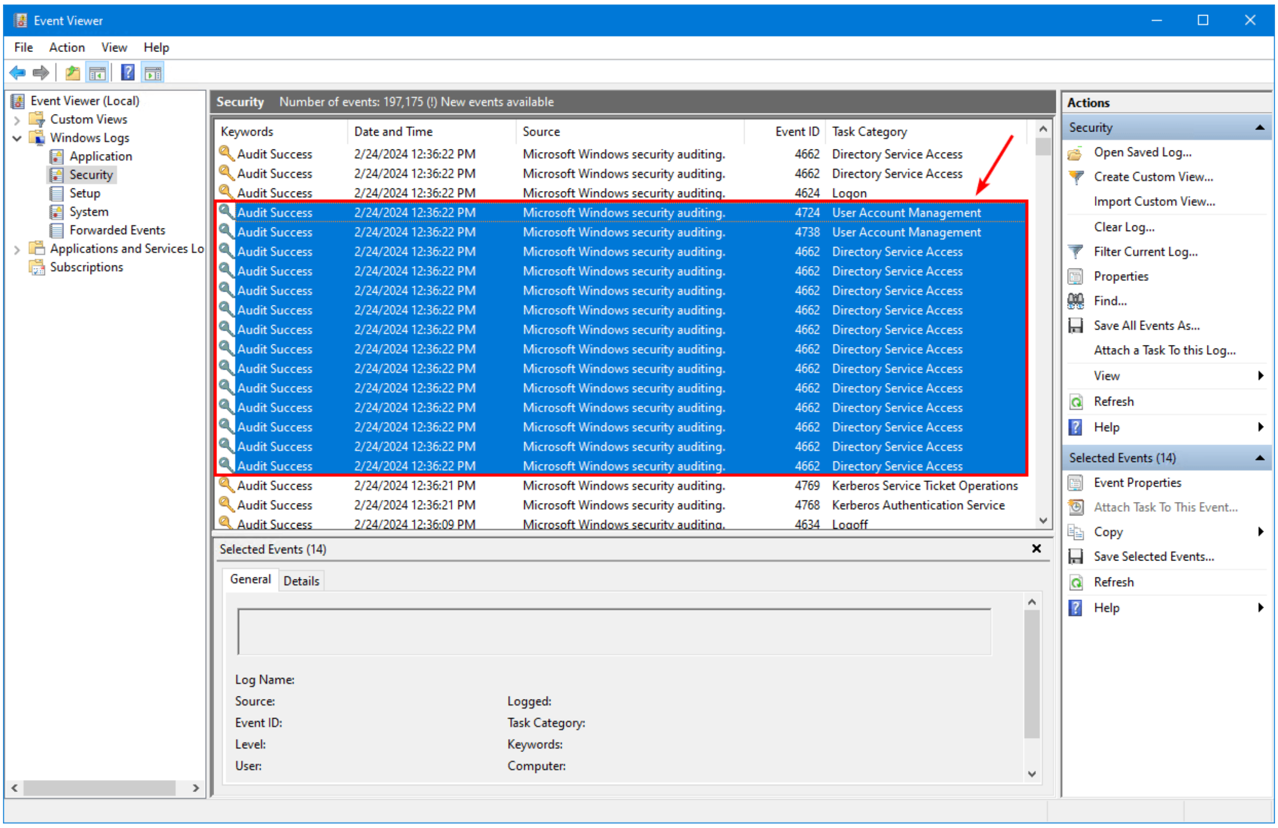
An operation was performed on an object.

Subject :

Log Name:	Security		
Source:	Microsoft Windows security	Logged:	2/24/2024 12:34:21 PM
Event ID:	4662	Task Category:	Directory Service Access
Level:	Information	Keywords:	Audit Success
User:	N/A	Computer:	DC01-2022.exoip.local

After you run *Mode 6 – Real Reset Mode*, the below events appear in the Security event logs:

- **ID 4662**
- **ID 4738**
- **ID 4724**



Security Number of events: 197,175 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4724	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:21 PM	Microsoft Windows security auditing.	4769	Kerberos Service Ticket Operations
Audit Success	2/24/2024 12:36:21 PM	Microsoft Windows security auditing.	4768	Kerberos Authentication Service
Audit Success	2/24/2024 12:36:09 PM	Microsoft Windows security auditing.	4634	Logoff

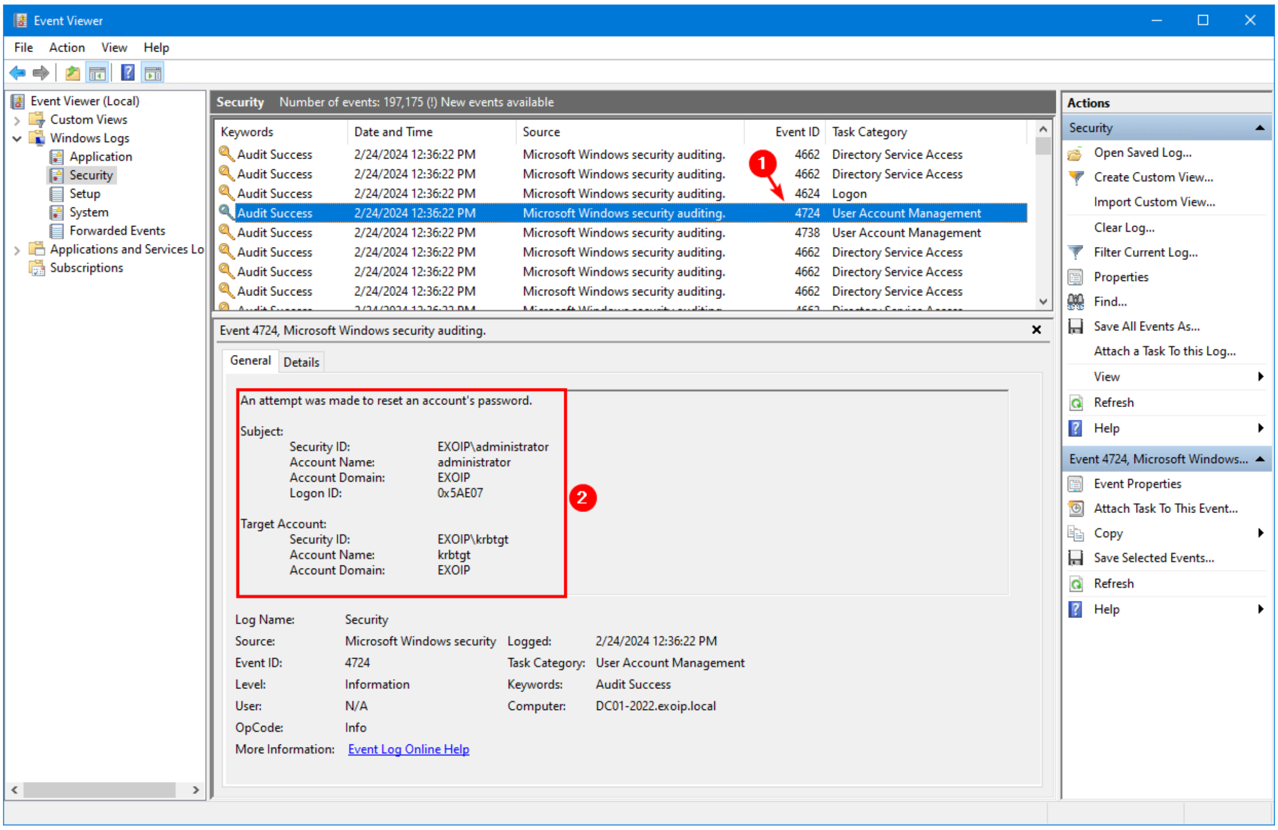
Selected Events (14)

General Details

Log Name:			
Source:		Logged:	
Event ID:		Task Category:	
Level:		Keywords:	
User:		Computer:	

This is what **Event ID 4724** looks like.

An attempt was made to reset an account’s password



Security Number of events: 197,175 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4724	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access

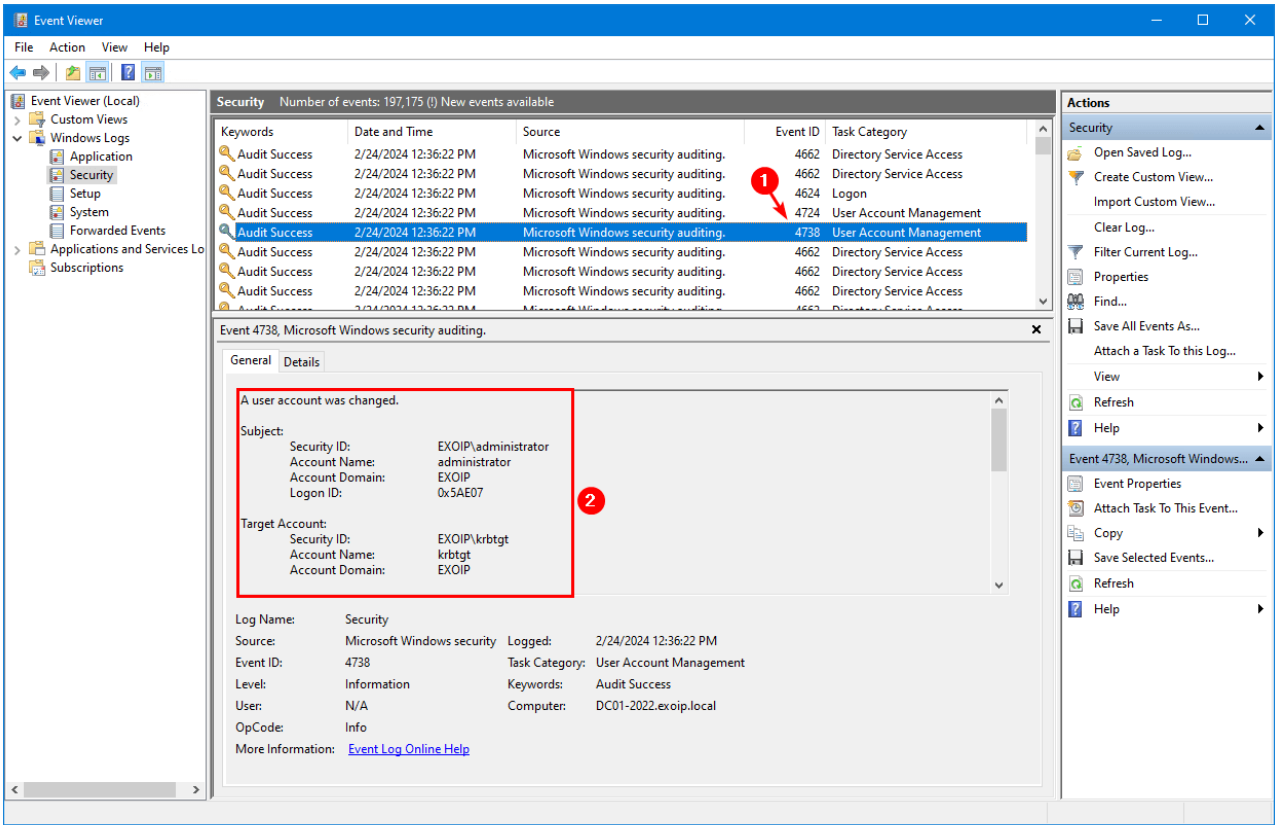
Event 4724, Microsoft Windows security auditing.

```
An attempt was made to reset an account's password.

Subject:
        Security ID:          EXOIP\administrator
        Account Name:         administrator
        Account Domain:       EXOIP
        Logon ID:             0x5AE07

Target Account:
        Security ID:          EXOIP\krbtgt
        Account Name:         krbtgt
        Account Domain:       EXOIP
```

Log Name: Security
Source: Microsoft Windows security
Logged: 2/24/2024 12:36:22 PM
Event ID: 4724
Task Category: User Account Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01-2022.exoip.local
OpCode: Info
More Information: Event Log Online Help

This is what **Event ID 4738** looks like.

A user account was changed.



Security Number of events: 197,175 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4624	Logon
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4724	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4738	User Account Management
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access
Audit Success	2/24/2024 12:36:22 PM	Microsoft Windows security auditing.	4662	Directory Service Access

Event 4738, Microsoft Windows security auditing.

```
A user account was changed.

Subject:
        Security ID:          EXOIP\administrator
        Account Name:         administrator
        Account Domain:       EXOIP
        Logon ID:             0x5AE07

Target Account:
        Security ID:          EXOIP\krbtgt
        Account Name:         krbtgt
        Account Domain:       EXOIP
```

Log Name: Security
Source: Microsoft Windows security
Logged: 2/24/2024 12:36:22 PM
Event ID: 4738
Task Category: User Account Management
Level: Information
Keywords: Audit Success
User: N/A
Computer: DC01-2022.exoip.local
OpCode: Info
More Information: Event Log Online Help

Reset KRBTGT account password twice

Wait for AD replication to complete and do the same step to change the KRBTGT password. If you have a multi-site and want to wait for replication to complete, that’s fine and recommended. Then, wait for the next day and run the script to change the KRBTGT account password.

The password must be changed twice to remove the password history effectively. Changing once, waiting for replication to complete, and changing again reduces the risk of issues.

Check the KRBTGT account **pwdLastSet** attribute after the second password reset.

That’s it!

Read more: Active Directory health check with PowerShell script »

Conclusion

You learned how to reset the KRBTGT account password. Run the reset KRBTGT account password PowerShell script in simulation mode first. After that, run the PowerShell script in real reset mode. Do not forget to wait for AD replication to complete and rerun the script again to remove the password history.

Did you enjoy this article? You may also like Export inactive users from Active Directory report. Don’t forget to follow us and share this article.