Krbtgt Key Reset Script Guidance

This document is a supplemental guide to the interactive krbtgt reset script (New-CtmADKrbtgtKeys.ps1). This guide describes the operating modes of the script and how to execute each of them.

# Requirements and Recommendations

* The script must be executed on a computer that is a member of the domain that is being targeted for krbtgt reset. The script does not allow the user to specify a different domain to be targeted.
* The script must be executed as an account with permissions to reset the password of the krbtgt account and permissions to initiate Active Directory replication between domain controllers. This will typically require membership in the Domain Admins group.
* The domain to be targeted must be at a domain functional level of ‘Windows2008Domain’ or higher.
* The script must be run on a computer that has RPC connectivity to every writable domain controller in the domain. The script (in Mode 2 and Mode 3) will initiate single object replication of the krbtgt account object to every writable domain controller in the domain.
* The script should be run on a computer that has high speed connectivity to the domain controller that holds the PDC emulator FSMO role (in the same site is recommended). The PDC emulator will be the target domain controller for the origination of the new krbtgt key. The PDC emulator will also be the source for single object replication of the krbtgt account object to every writable DC in the domain.
* The Powershell script execution policy of the computer on which the script will be run must be configured to allow execution of the script. The minimal execution policy required is ‘RemoteSigned’ (requires the script to be copied to the local computer). To configure this, open an elevated Powershell prompt:

Set-ExecutionPolicy RemoteSigned

* All three modes of the script should be executed on the same computer.
* Mode 1 should be executed repeatedly until all failures have been remediated and all checks have passed. Only then should the user proceed to execute Mode 2.
* Mode 2 should be executed repeatedly until all failures have been remediated, all checks have passed, and all single object replication has succeeded. Only then should the user proceed to execute Mode 3.
* Mode 2 should be executed immediately prior to Mode 3 every time that Mode 3 is executed to ensure that all checks have passed and all single object replication will succeed. Even if Mode 2 has succeeded in the past, running it immediately prior to Mode 3 will ensure that everything is still functioning as expected.
* It is generally recommended (though not required) that the script be executed on the domain controller which holds the PDC emulator FSMO role.
* It is generally recommended (though not required) that the PDC emulator be in a hub/central location to provide the best possible replication performance to all writable domain controllers in the domain.

# Script Execution

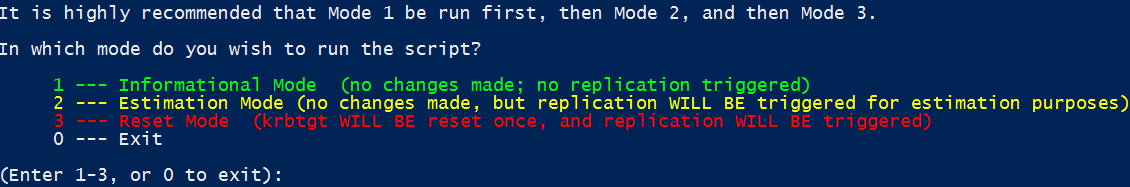
All three operating modes of the script require that the script be executed with no command-line input parameters required. The script will prompt the user to select the operating mode before any activities are performed, so it is safe to begin by executing the script.

* Open a Powershell prompt (does not need to be elevated).
* Execute the script with no command line parameters by running:

.\New-CtmADKrbtgtKeys.ps1

* The following information and menu will be presented:





* At the menu prompt, type the number of the mode you wish to execute and press ‘Enter’.
  + Execute Mode 1 first, then Mode 2, then Mode 3. Execute all three modes on the same computer. Do not switch computers without running Mode 2 before running mode 3.

# Mode 1 – Informational Mode

Mode 1 is the informational mode of the script. It will only perform read and connection operations in an effort to validate prerequisites and perform validation that the environment is ready for execution of the script and that the execution of the script will be successful. The results of the checks will be reported to the screen in green or red (pass/fail) while relevant information will be reported to the screen in cyan. Below are the activities that will be performed in Mode 1.

* Script dependency checks:
  + The script will check for the ‘ActiveDirectory’ Powershell module. The result of this check will be reported as PASSED (in green) or FAILED (in red).
  + The script will check for the RPCPING.EXE command line utility. The result of this check will be reported as PASSED (in green) or FAILED (in red).
  + The script will check for the REPADMIN.EXE command line utility. The result of this check will be reported as PASSED (in green) or FAILED (in red).
* Target domain checks:
  + The script will report the NetBIOS name of the target domain to the screen in cyan.
  + The script will report the DNS name of the target domain to the screen in cyan.
  + The script will report the FQDN of the PDC emulator for the target domain to the screen in cyan.
  + The script will report the domain functional mode of the target domain to the screen in cyan.
  + The script will check that the domain functional mode is ‘Windows2008Domain’ or higher. The result of this check will be reported as PASSED (in green) or FAILED (in red).
* Krbtgt account and Kerberos policy checks:
  + The script will report the distinguished name of the krbtgt account object to the screen in cyan.
  + The script will report the ‘PasswordLastSet’ of the krbtgt account object to the screen in cyan.
  + The script will report the Kerberos domain policy’s maximum user ticket lifetime to the screen in cyan.
  + The script will report the Kerberos domain policy’s maximum tolerance for computer clock synchronization to the screen in cyan.
  + The script will check that all tickets based on the previous (N-1) key have had a chance to expire. The result of this check will be reported as PASSED (in green) or FAILED (in red).

**Note: the N-1 ticket check only subtracts the maximum user ticket lifetime and the possible clock skew from the current time and validates that the ‘PasswordLastSet’ time of the krbtgt account is prior to that. This means that this check does not account for the time it takes for AD replication to occur throughout the domain. If a recent krbtgt reset has been performed, be sure that AD replication has had time to complete throughout the domain AND that the N-1 tickets have had time to expire. It is only safe to execute Mode 3 if the current time is later than:**

**KrbtgtAccountPasswordLastSet + DomainMaximumFullReplicationTime + KerberosPolicyMaximumUserTicketLifetime + (KerberosPolicyMaximumToleranceForComputerClockSynchronization \* 2)**

* Domain controller checks
  + The script will check for RPC connectivity to each writable domain controller in the domain. The result of this check will be reported for each writable domain controller as PASSED (in green) or FAILED (in red).

Basic results and information will be logged in a log file, the name of which will be reported to the screen.

Remediate any Mode 1 failures and re-run Mode 1 until it is completely successful.

# Mode 2 – Estimation Mode

Mode 2 is the estimation mode of the script. This mode allows the user to simulate Mode 3 without actually resetting the krbtgt key. The krbtgt key reset will not be performed, but the subsequent single object replication of the krbtgt account object to each writable domain controller will be performed and measured. The time this replication takes in Mode 2 will be provided to the user as an estimate for Mode 3. This estimate will give an approximation of the time that Mode 3 will take from resetting the krbtgt key to replicating that new key to all writable domain controllers. This time will be the duration of the impacts that are possible. (The impacts are described in the script output screen shot that was provided earlier in this document.) Below are the activities that will be performed in Mode 2.

* Mode 2 will perform all the activities that Mode 1 performs.
* After the Mode 1 activities are completed, Mode 2 will prompt the user for confirmation before proceeding to perform single object replication of the krbtgt account object from the PDC emulator to all other writable domain controllers in the domain.



If ready for the single object replication to be attempted, the user should enter ‘y’ and press ‘Enter’ to proceed. Note that no changes will be made to any Active Directory objects.

* Single object replication will be performed to each writable domain controller. The script will report the status of single object replication to each writable domain controller. The result of this check will be reported as SUCCEEDED (in green) or FAILED (in red). The elapsed time of the single object replication attempt to that domain controller will also be reported (in cyan).
* Once all replication is complete, the total duration of the single object replication to all writable domain controllers will be reported to the user as the estimated impact duration for Mode 3.

Basic results and information will be logged in a log file, the name of which will be reported to the screen.

Remediate any Mode 2 failures and re-run Mode 2 until it is completely successful.

# Mode 3 – Reset Mode

Mode 3 is the reset mode of the script. This mode will perform a single reset of the krbtgt key. The krbtgt key reset will be performed, followed by single object replication of the krbtgt account object to each writable domain controller. The total elapsed time in which the single reset effects may have been encountered will be reported and the writable domain controllers will be checked to ensure that their krbtgt key is in sync with the PDC emulator. Below are the activities that will be performed in Mode 3.

* Mode 3 will perform all the activities that Mode 1 performs.
* After the Mode 1 activities are completed, Mode 3 will prompt the user for confirmation before proceeding to perform the krbtgt key reset and the single object replication of the krbtgt account object from the PDC emulator to all other writable domain controllers in the domain.



If ready for the krbtgt key reset and the single object replication to be attempted, the user should enter ‘y’ and press ‘Enter’ to proceed.

* The krbtgt key reset will be performed against the PDC emulator. The script will report the status of the krbtgt key reset as SUCCEEDED (in green) or FAILED (in red).
* Once the krbtgt key reset is complete, single object replication will be performed to each writable domain controller. The script will report the status of single object replication to each writable domain controller. The result of this check will be reported as SUCCEEDED (in green) or FAILED (in red). The elapsed time of the single object replication attempt to that domain controller will also be reported (in cyan).
* Once all replication is complete, the total duration of the krbtgt key reset operation plus the single object replication to all writable domain controllers will be reported to the user as the impact duration for Mode 3.
* The script will then check every writable domain controller to check if the krbtgt account’s PasswordLastSet is in sync with the PDC emulator. The script will report the status of this check for each writable domain controller. The result of this check will be reported as PASSED (in green) or FAILED (in red). Once the checks for each domain controller are complete, the script will report the status of this check. If the krbtgt account object on one or more domain controllers is out of sync with the PDC emulator, this problem will be reported to the screen.

Basic results and information will be logged in a log file, the name of which will be reported to the screen.