

Re: Replication of password resets/unlocks

Source:

http://www.tech-archive.net/Archive/Windows/microsoft.public.windows.server.active_directory/2006-06/msg01413

- *From:* "Joe Richards [MVP]" <humorexpress@xxxxxxxxxxx>
 - *Date:* Tue, 20 Jun 2006 19:17:05 -0400
-

That is quite a hodgepodge from different documents. There are problems in there.

First off, I know it isn't your fault, but the name urgent replication implies something that it isn't guaranteed to be. Fast. The actual implementation is urgent queuing and the queued ops are the same priority as a normal queued op of the same type. So if you hit a bridgehead (which you must do if crossing site lines even if using change notification) that is backed up with inbound replication requests, even though the request was urgently queued, it can take awhile for that information to get into the bridgehead and then replicated back out.

Second off, there isn't such a thing as urgent replication to the PDC. There is an out of band update that occurs which is a special RPC call that isn't replication based to get info to the PDC.

To my knowledge, this occurs in the case of a password change (assuming AvoidPDCOnWan isn't set) but not for a lockout. What can occur for a lockout is that as a password is tested and is incorrect, the password attempt is chained to the PDC (again if AvoidPDCOnWan is not enabled) and the lockout will occur at the same time on the two DCs. In actual fact, the lockout can occur before the lockout on the local DC if for some reason another DC was queried along with the first, then two DCs are sending attempts to the PDC. For instance, say you send an auth request with a bad password to DC2 and to DC3, assuming a simple auth attempt with no additional auth providers that means one bad on password hit on DC2 and DC3 and 2 bad password hits on DC1 (the PDC).

- > Because a user cannot specify the domain controller on which
- > the password change is attempted, an attack of this type
- > requires an advanced tool.

Not really a very advanced tool, a two line script could be a good start. This is propaganda to make folks feel more secure. :)

Joe Richards Microsoft MVP Windows Server Directory Services
Author of O'Reilly Active Directory Third Edition
www.joeware.net

---O'Reilly Active Directory Third Edition now available---

<http://www.joeware.net/win/ad3e.htm>

Jorge Silva wrote:

Urgent Replications

– Certain important events trigger replication immediately, overriding existing change notification. Urgent replication is implemented immediately by using RPC/IP to notify replication partners that changes have occurred on a source domain controller. Urgent replication uses regular change notification between destination and source domain controller pairs that otherwise use change notification, but notification is sent immediately in response to urgent events instead of waiting the default period of 15 seconds (or 300 seconds on domain controllers that are running Windows 2000).

– Urgent Active Directory replication is always triggered by certain events on all domain controllers within the same site. When you have enabled change notification between sites, these triggering events also replicate immediately between sites.

Between Windows Server 2003–based and Windows 2000–based domain controllers in the same site, immediate notification is caused by the following events:

*Assigning an account lockout, which a domain controller performs to prohibit a user from logging on after a certain number of failed attempts.

*Changing the account lockout policy.

*Changing the domain password policy.

*Changing a Local Security Authority (LSA) secret, which is a secure form in which private data is stored by the LSA (for example, the password for a trust relationship).

*Changing the password on a domain controller computer account.

*Changing the relative identifier (known as a "RID") master role owner, which is the single domain controller in a domain that assigns relative identifiers to all domain controllers in that domain.

– Urgent Replication of Account Lockout Changes

Account lockout is a security feature that sets a limit on the number of failed authentication attempts that are allowed before the account is "locked out" from a further attempt to log on, in addition to a time limit for how long the lockout is in effect.

Re: Replication of password resets/unlocks

– The PDC emulator receives urgent replication of account lockouts. In Active Directory domains, a single domain controller in each domain holds the role of PDC emulator, which simulates the behavior of a Windows NT version 3.x-based or Windows NT 4.0-based PDC. In Windows NT domains, the only domain controller that can accept updates is the PDC. If authentication fails at a BDC, the authentication request is passed immediately to the PDC, which is guaranteed to have the current password.

– An account lockout is urgently replicated to the PDC emulator and is then urgently replicated to the following:

*Domain controllers in the same domain that are located in the same site as the PDC emulator.

*Domain controllers in the same domain that are located in the same site as the domain controller that handled the account lockout.

* Domain controllers in the same domain that are located in sites that have been configured to allow change notification between sites (and, therefore, urgent replication) with the site that contains the PDC emulator or with the site where the account lockout was handled.

– These sites include any site that is included in the same site link as the site that contains the PDC emulator or in the same site link as the site that contains the domain controller that handled the account lockout.

In addition, when authentication fails at a domain controller other than the PDC emulator, the authentication is retried at the PDC emulator. For this reason, the PDC emulator locks the account before the domain controller that handled the failed–password attempt if the bad–password–attempt threshold is reached.

– Note: When a bad password is used in an attempt to change a password, the lockout count is incremented on that domain controller only and is not replicated. As such, an attacker could try (of domain controllers)*(lockout threshold –1) + 1 guesses before the account is locked out. Although this scenario has a relatively small impact on account lockout security, domains with an exceptionally high number of domain controllers represent a significant increase in the total number of guesses available to an attacker. Because a user cannot specify the domain controller on which the password change is attempted, an attack of this type requires an advanced tool.

– Replication of Password Changes

Password changes are replicated differently than both normal (non–urgent) replication and urgent replication. Changes to security account passwords present a replication latency

Re: Replication of password resets/unlocks

problem wherein a user's password is changed on domain controller A and the user subsequently attempts to log on, being authenticated by domain controller B. If the password has not replicated from A to B, the attempt to log on fails. Active Directory replication remedies this situation by forwarding password changes immediately to a single domain controller in the domain, the PDC emulator.

– In Active Directory, when a user password is changed at a domain controller, that domain controller attempts to update the respective replica at the domain controller that holds the PDC emulator role. Update of the PDC emulator occurs immediately, without respect to schedules on site links. The updated password is propagated to other domain controllers by normal replication within a site.

– When the user logs on to a domain and is authenticated by a domain controller that does not have the updated password, the domain controller refers to the PDC emulator to check the credentials of the user name and password rather than denying authentication based on an invalid password. Therefore, the user can log on successfully even when the authenticating domain controller has not yet received the updated password. On domain controllers that are running Windows Server 2003 or Windows 2000 Server with SP4, if the authentication is successful at the PDC emulator, the PDC emulator replicates the password immediately to the requesting domain controller to prevent that domain controller from having to check the PDC emulator again.

– If the update at the PDC emulator fails for any reason, the password change is replicated non-urgently by normal replication.

For clients that are running Windows NT 4.0 or clients that are running Windows 95 or Windows 98 without the Directory Service Client Pack, the client attempts to contact the PDC emulator. If the client has the Directory Service Client Pack installed, the client contacts any domain controller and the contacted domain controller then attempts to contact the PDC emulator.

– Note: The Group Policy setting "Contact PDC on logon failure" can be disabled to keep a domain controller from contacting the PDC emulator if the PDC emulator role owner is not in the current site. If this setting is disabled, the password change reaches the PDC emulator non-urgently through normal replication.