

DSRAZOR Solution: Last Logon and Failed Logons



Determining when an account last logged in to Active Directory is a complex and time-consuming task. Additionally, discovering where accounts have failed logon attempts is a security concern. Understanding how the last logon and failed logon values function is important to managing your Active Directory. DSRAZOR for Windows solves the complex tasks of determining last logon and finding failed logon attempts.

Understanding Logon Events in Domains, Domain Controllers and Active Directory

The implementation of Active Directory is based upon its installation on Domain Controllers. The concept and use of Domain Controllers predates Active Directory by several years. When an account is created in Active Directory, that account and its attributes are replicated to each Domain Controller in the Domain. However, there are some attributes that are separately maintained per Domain Controller.

By default, Logon Event data is stored per Domain Controller and *is not* replicated between Domain Controllers. Logon events are handled locally by Domain Controllers. *Locally* means when you logon to one Domain Controller you are not automatically logged on to all other Domain Controllers in the Domain.

There are several Active Directory attributes maintained for each account that contain logon data:

Attribute Name	Usage
lastLogon	Stored per Domain Controller – value indicates the time an account last logged on
badPasswordCount	Stored per Domain Controller – value indicates the number of times a bad/incorrect password was specified for an account logon attempt as processed by the Domain Controller – the value is reset to zero when a logon attempt succeeds
badPasswordTime	Stored per Domain Controller – value indicates the time of the last failed logon attempt as processed by the Domain Controller – the value is never reset
logonCount	Stored per Domain Controller – value is an ever-increasing count of the number of times an account has logged onto the selected Domain Controller
lastLogoff	Stored per Domain Controller – value indicates the time an account last logged off
lastLogonTimeStamp	<i>Requires utilization of Windows 2003 Domain Mode on all Domain Controller</i> – value is replicated to all Domain Controllers and indicates the time an account last logged on – by default, value is replicated once every 7 days
Note: None of these values are stored in the Global Catalog	

Determining exactly when an account last logged on to the Domain requires interrogating each Domain Controller in the Domain. If your Domain is configured to use Windows 2003 Domain Mode you can use the `lastLogonTimeStamp` attribute to determine when the selected account logged on to the

Domain - this value is accurate within the past 13 days. The value is not exact because the `lastLogonTimeStamp` attribute is only replicated every 7 days (this is the default and it can be changed to a different replication frequency). Even when using Windows 2003 Domain Mode, knowing the actual last logon still requires contacting each Domain Controller.

Regardless of how your Active Directory is configured, discovering accounts that have failed logons requires interrogating every Domain Controller in the Domain. Failed logon data is maintained in two attributes, `badPasswordCount` and `badPasswordTime`. These attributes are maintained per Domain Controller. If the `badPasswordCount` has a value greater than zero this indicates the last logon attempt to the named account on that Domain Controller **failed**. The `badPasswordTime` attribute's value indicates the time of the last failed logon – this value is updated each time a failed logon occurs.

Solving the problem of determining last logon and where last logon failed

DSRAZOR for Windows solves the complex tasks of determining last logon and finding failed logon attempts by automatically retrieving logon data from all Domain Controllers where accounts exist.

The following image is from a ready-to-run DSRAZOR applet (`lastlogon1.dsr`):

The screenshot shows a window titled "Find all User Accounts and show last logon from selected container" with the container path "CN=Users,DC=visualclick,DC=local". It contains two tables. The top table lists users found via GC search, showing their latest logon server and the number of days since the latest logon. The bottom table shows domain controllers where users are defined, listing the last logon time, last bad password time, logon count, and bad password count for each user.

Users found (GC search)	Latest Logon Server	#days since latest logon
CN=Administrator,CN=Users,DC=visualclick,DC=local	monster	1 day
CN=Guest,CN=Users,DC=visualclick,DC=local	<nothing found>	<not set>
CN=HelpAssistant_4237d7,CN=Users,DC=visualclick,DC=local	<nothing found>	<not set>
CN=kribtgt,CN=Users,DC=visualclick,DC=local	<nothing found>	<not set>
CN=SUPPORT_388945a0,CN=Users,DC=visualclick,DC=local	<nothing found>	<not set>
CN=water,CN=Users,DC=visualclick,DC=local	visual-82	12 days

Domain Controllers where User is defined	Last Logon	Last Bad Password	Logon Count	Bad Password Count
monster	Tue Dec 20 01:57:00 2005	Tue Dec 20 01:57:00 2005	55	0
visual-80	Thu Dec 15 15:13:00 2005	Wed Dec 21 11:08:00 2005	88	1
visual-82	Wed Dec 7 09:24:00 2005	Tue Dec 20 01:57:00 2005	16	2
visual-94	<not set>	<not set>	0	0

In the image above, the *Last Logon* column indicates the most recent successful logon for the specified Domain Controller. The notation *<not set>* indicates a successful logon has not yet occurred for the selected account on the named Domain Controller. The *Latest Logon Server* and *#days since latest logon* columns indicate where the most recent successful logon occurred and how many days it has been since this logon occurred. These two values are derived by connecting to each Domain Controller and retrieving the value of `lastLogon` attribute for each account.

In the image above, the *Bad Password Count* column indicates where the last logon failed. If the value is zero (as seen for `monster` and `visual-94`) the latest logon attempt succeeded. If the value is not zero (as seen for `visual-80` and `visual-82`) the latest logon attempt **failed**. If this count exceeds the intruder detection threshold (as identified by the Domain Policy option: Account Lockout Threshold) the account will be locked. Because the Bad Password Count is reset after a successful logon, accounts with a Bad Password Count may indicate someone trying to break into an account. The *Last Bad Password* column indicates when the most recent unsuccessful logon attempt occurred – this value is never reset to zero it is only updated each time a logon attempt fails.

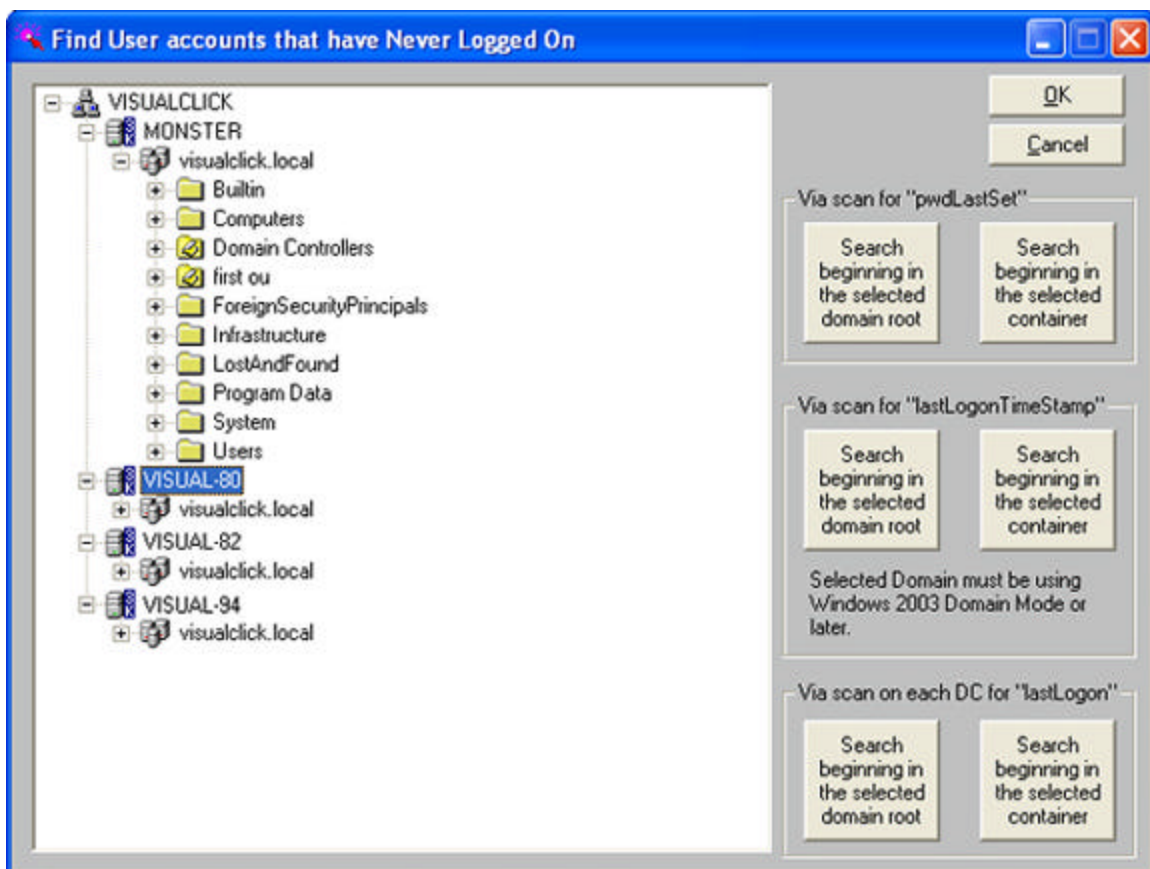
Alternate methods to detect unused accounts

Directly querying each Domain Controller for each account's logon attribute values can be time consuming, especially in a Domain with multiple sites. You may be interested in alternative methods of quickly determining account use.

If your Domain is using Windows 2003 Domain Mode you can use the value of the `lastLogonTimeStamp` attribute. This attribute is replicated every 7 days and therefore indicates the last logon within a window of the past 13 days – useful for detecting accounts with no logon for the past 2 weeks or longer.

If your Domain is not using Windows 2003 Domain Mode you will not be able to use `lastLogonTimeStamp` attribute. However, you may find the value of the `pwdLastSet` attribute to be good enough in detecting accounts that have not been recently used. This attribute is updated each time the account password is changed *and* this value is replicated to all Domain Controllers within a few minutes of the last password change. The relative worth of tracking the `pwdLastSet` attribute is dependent upon a password change policy being in-use and the frequency of forced password changes.

DSRAZOR for Windows provides an applet (`neverlog.dsr`) that includes all three last logon detection methods described in this document. The following is an image from this applet:



Summary

DSRAZOR for Windows solves the complex tasks of determining last logon and finding failed logon attempts. Use DSRAZOR to document your Active Directory today.