

Active Directory (Domain) Account Lockout, Audit and Password Policies

Period: **Dataset Wednesday, January 09, 2008 3:00:11 AM**

Generated: **Wednesday, January 09, 2008 11:20:32 AM**

For: **Brian Bartlett bbartlett@ecora.com**

By: Ecora Auditor Professional 4.5 - Active Directory Module 4.5.8007.18310

Using: Customized FFR Definition based on 'Active Directory (Domain) Account Lockout, Audit and Password Policies'

Description: A Fact-Finding report will show values greater than, less than, or unlike a threshold value you set. These reports are very surgical in their precision - you can pull precisely the data you need, but they also offer a wealth of data through hundreds of built-in reports created by experts.

Active Directory (Domain) Account Lockout, Audit and Password Policies

Table of Contents

Account Lockout Policy	1
Password Policy	2
Audit Policy	2

Collected Not-Collected Legend

DEFAULT	The value presented in the report was not directly reported by the target, but implied by the current value or lack of a value for the attribute
<i>*UA*</i>	Unavailable attribute. The current configuration or version of target platform does not provide a value for this attribute. More detail in logs
<i>*FC*</i>	Collection of value failed
<i>*NS*</i>	Value not selected for collection

Account Lockout Policy

Table 1. Account Lockout Policy

Category Name	Policy Name	Policy Setting
Account Lockout Policy	Account lockout duration	-1 minutes
Account Lockout Policy	Account lockout duration	30 minutes
Account Lockout Policy	Account lockout threshold	5 invalid logon attempts
Account Lockout Policy	Reset account lockout counter after	30 minutes

Password Policy

Table 2. Password Policy

Category Name	Policy Name	Policy Setting
Password Policy	Enforce password history	4 passwords remembered
Password Policy	Enforce password history	7 passwords remembered
Password Policy	Maximum password age	-1 days
Password Policy	Maximum password age	42 days
Password Policy	Minimum password age	0 days
Password Policy	Minimum password age	30 days
Password Policy	Minimum password length	0 characters
Password Policy	Minimum password length	8 characters
Password Policy	Password must meet complexity requirements	Disabled
Password Policy	Password must meet complexity requirements	Enabled
Password Policy	Store passwords using reversible encryption	Disabled

Audit Policy

Table 3. Audit Policy

Category Name	Policy Name	Policy Setting
Audit Policy	Audit account logon events	Failure
Audit Policy	Audit account logon events	Success, Failure
Audit Policy	Audit account management	Success, Failure
Audit Policy	Audit directory service access	Failure
Audit Policy	Audit directory service access	Success
Audit Policy	Audit directory service access	Success, Failure
Audit Policy	Audit logon events	Failure
Audit Policy	Audit logon events	Success
Audit Policy	Audit logon events	Success, Failure
Audit Policy	Audit object access	Failure
Audit Policy	Audit object access	No auditing
Audit Policy	Audit object access	Success, Failure
Audit Policy	Audit policy change	Success, Failure
Audit Policy	Audit privilege use	Failure
Audit Policy	Audit privilege use	No auditing

Category Name	Policy Name	Policy Setting
Audit Policy	Audit process tracking	No auditing
Audit Policy	Audit system events	Failure
Audit Policy	Audit system events	Success, Failure
User Rights Assignment	Generate security audits	NETWORK SERVICE, LOCAL SERVICE, Administrators, BSP\Administrator
User Rights Assignment	Manage auditing and security log	Administrators, *S-1-5-21-3734189588-1271080782-879282008-512, BSP\DB2ADMNS