

Domain Security Policies and Settings

Period: **Last 20 week(s)**
 Generated: **Tuesday, January 08, 2008 3:27:26 PM**
 For: **Brian Bartlett bbartlett@ecora.com**
 By: Ecora Auditor Professional 4.5 - Windows Module 4.5.8007.18310
 Using: FFR Definition 'Domain Security Policies and Settings'
 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.

Domain Security Policies and Settings

Table of Contents

- Domain Security Settings** **1**
- Account Lockout Policy** **2**
- Audit Policy** **2**
- Kerberos Policy** **2**
- Password Policy** **3**
- Security Options** **3**
- User Rights** **3**

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

Domain Security Settings

Table 1. Domain Security Settings

Domain Name	GPO Name
BSP	Default Domain Controllers Policy {6AC1786C-016F-11D2-945F-00C04fB984F9}

Domain Name	GPO Name
BSP	Default Domain Policy {31B2F340-016D-11D2-945F-00C04FB984F9}

Account Lockout Policy

Table 2. Account Lockout Policy

Account Lockout Policy Name	Account Lockout Security Settings
NULL	*NULL*
Account lockout duration	-1 minutes
Account lockout threshold	5 invalid logon attempts
Reset account lockout counter after	30 minutes

Audit Policy

Table 3. Audit Policy

Audit Policy Name	Audit Security Settings
Audit account logon events	Failure
Audit account management	Success, Failure
Audit directory service access	Failure
Audit logon events	Failure
Audit object access	Failure
Audit policy change	Success, Failure
Audit privilege use	Failure
Audit process tracking	No Auditing
Audit system events	Failure

Kerberos Policy

Table 4. Kerberos Policy

Kerberos Policy Name	Kerberos Security Settings
NULL	*NULL*
Enforce user logon restrictions	Enabled
Maximum lifetime for service ticket	600 minutes
Maximum lifetime for user ticket	10 hours
Maximum lifetime for user ticket renewal	7 days

Kerberos Policy Name	Kerberos Security Settings
Maximum tolerance for computer clock synchronization	5 minutes

Password Policy

Table 5. Password Policy

Password Policy Name	Password Security Settings
NULL	*NULL*
Enforce password history	4 passwords remembered
Maximum password age	-1 days
Minimum password age	0 days
Minimum password length	0 characters
Password must meet complexity requirements	Disabled
Store passwords using reversible encryption	Disabled

Security Options

Table 6. Security Options

Security Option Name	Security Option Settings
NULL	*NULL*
Domain controller: LDAP server signing requirements	None
Domain member: Digitally encrypt or sign secure channel data (always)	Enabled
Microsoft network server: Digitally sign communications (always)	Enabled
Microsoft network server: Digitally sign communications (if client agrees)	Enabled
Network security: LAN Manager authentication level	Send NTLM response only

User Rights

Table 7. User Rights

User List	User Privilege
NULL	*NULL*
BSP\Administrator (user)	Create permanent shared objects
BSP\Administrator (user)	Generate security audits
BSP\Administrator (user)	Load and unload device drivers
BSP\Administrator (user)	Log on as a batch job

User List	User Privilege
BSP\Administrator (user)	Log on as a service
BSP\Administrator (user)	Profile single process
BSP\Administrator (user)	Restore files and directories
BSP\bbartlett (user)	Act as part of the operating system
BSP\bbartlett (user)	Allow log on locally
BSP\bbartlett (user)	Log on as a batch job
BSP\bdb (user)	Log on as a batch job
BSP\db2admin (user)	Act as part of the operating system
BSP\db2admin (user)	Adjust memory quotas for a process
BSP\db2admin (user)	Lock pages in memory
BSP\db2admin (user)	Log on as a service
BSP\db2admin (user)	Replace a process level token
BSP\DB2ADMNS (alias)	Access this computer from the network
BSP\DB2ADMNS (alias)	Adjust memory quotas for a process
BSP\DB2ADMNS (alias)	Back up files and directories
BSP\DB2ADMNS (alias)	Debug programs
BSP\DB2ADMNS (alias)	Increase scheduling priority
BSP\DB2ADMNS (alias)	Log on as a service
BSP\DB2ADMNS (alias)	Manage auditing and security log
BSP\DB2ADMNS (alias)	Modify firmware environment values
BSP\DB2ADMNS (alias)	Replace a process level token
BSP\DB2ADMNS (alias)	Restore files and directories
BSP\DB2ADMNS (alias)	Take ownership of files or other objects
BSP\DB2USERS (alias)	Access this computer from the network
BSP\Domain Admins (group)	Adjust memory quotas for a process
BSP\Domain Admins (group)	Allow log on locally
BSP\Domain Users (group)	Access this computer from the network
BSP\exchsvc (user)	Act as part of the operating system
BSP\exchsvc (user)	Log on as a service
BSP\exchsvc (user)	Restore files and directories
BSP\IIS_WPG (alias)	Log on as a batch job
BSP\IUSR_BIGMOUNTAIN (user)	Access this computer from the network
BSP\IUSR_BIGMOUNTAIN (user)	Allow log on locally
BSP\IUSR_BIGMOUNTAIN (user)	Log on as a batch job
BSP\IUSR_PITA1 (user)	Access this computer from the network

User List	User Privilege
BSP\IUSR_PITA1 (user)	Allow log on locally
BSP\IUSR_PITA1 (user)	Log on as a batch job
BSP\IWAM_BIGMOUNTAIN (user)	Access this computer from the network
BSP\IWAM_BIGMOUNTAIN (user)	Adjust memory quotas for a process
BSP\IWAM_BIGMOUNTAIN (user)	Log on as a batch job
BSP\IWAM_BIGMOUNTAIN (user)	Replace a process level token
BSP\IWAM_PITA1 (user)	Access this computer from the network
BSP\IWAM_PITA1 (user)	Adjust memory quotas for a process
BSP\IWAM_PITA1 (user)	Log on as a batch job
BSP\IWAM_PITA1 (user)	Replace a process level token
BSP\RConsole Users (alias)	Log on as a batch job
BSP\SMS&_BIG-MOUNTAIN (user)	Act as part of the operating system
BSP\SMS&_BIG-MOUNTAIN (user)	Log on as a service
BSP\SMS&_BIG-MOUNTAIN (user)	Replace a process level token
BSP\SMSCliToknAcct& (user)	Act as part of the operating system
BSP\SMSCliToknAcct& (user)	Adjust memory quotas for a process
BSP\SMSCliToknAcct& (user)	Log on as a service
BSP\SMSCliToknAcct& (user)	Replace a process level token
BSP\SMSCliToknAcct& (user)	Shut down the system
BSP\SMSService_st (user)	Log on as a service
BSP\SQLServer2005DTSUser\$PITA1 (alias)	Bypass traverse checking
BSP\SQLServer2005DTSUser\$PITA1 (alias)	Log on as a service
BSP\SQLServer2005MSFTEUser\$PITA1\$BSPSQL2005 (alias)	Adjust memory quotas for a process
BSP\SQLServer2005MSFTEUser\$PITA1\$BSPSQL2005 (alias)	Bypass traverse checking
BSP\SQLServer2005MSFTEUser\$PITA1\$BSPSQL2005 (alias)	Log on as a batch job
BSP\SQLServer2005MSFTEUser\$PITA1\$BSPSQL2005 (alias)	Log on as a service
BSP\SQLServer2005MSFTEUser\$PITA1\$BSPSQL2005 (alias)	Replace a process level token
BSP\SQLServer2005MSOLAPUser\$PITA1\$BSPSQL2005 (alias)	Log on as a service
BSP\SQLServer2005MSSQLUser\$PITA1\$BSPSQL2005 (alias)	Adjust memory quotas for a process
BSP\SQLServer2005MSSQLUser\$PITA1\$BSPSQL2005 (alias)	Bypass traverse checking
BSP\SQLServer2005MSSQLUser\$PITA1\$BSPSQL2005 (alias)	Log on as a batch job
BSP\SQLServer2005MSSQLUser\$PITA1\$BSPSQL2005 (alias)	Log on as a service
BSP\SQLServer2005MSSQLUser\$PITA1\$BSPSQL2005 (alias)	Replace a process level token
BSP\SQLServer2005NotificationServicesUser\$PITA1 (alias)	Log on as a service
BSP\SQLServer2005ReportServerUser\$PITA1\$BSPSQL2005 (alias)	Log on as a service

User List	User Privilege
BSP\SQLServer2005SQLAgentUser\$PITA1\$BSPSQL2005 (alias)	Adjust memory quotas for a process
BSP\SQLServer2005SQLAgentUser\$PITA1\$BSPSQL2005 (alias)	Bypass traverse checking
BSP\SQLServer2005SQLAgentUser\$PITA1\$BSPSQL2005 (alias)	Log on as a batch job
BSP\SQLServer2005SQLAgentUser\$PITA1\$BSPSQL2005 (alias)	Log on as a service
BSP\SQLServer2005SQLAgentUser\$PITA1\$BSPSQL2005 (alias)	Replace a process level token
BSP\SQLServer2005SQLBrowserUser\$PITA1 (alias)	Log on as a service
BSP\SUPPORT_388945a0 (user)	Deny access to this computer from the network
BSP\SUPPORT_388945a0 (user)	Deny to log on locally
BSP\SUPPORT_388945a0 (user)	Log on as a batch job
BUILTIN\Administrators (alias)	Access this computer from the network
BUILTIN\Administrators (alias)	Act as part of the operating system
BUILTIN\Administrators (alias)	Add workstations to domain
BUILTIN\Administrators (alias)	Adjust memory quotas for a process
BUILTIN\Administrators (alias)	Allow log on locally
BUILTIN\Administrators (alias)	Back up files and directories
BUILTIN\Administrators (alias)	Change the system time
BUILTIN\Administrators (alias)	Create a pagefile
BUILTIN\Administrators (alias)	Create permanent shared objects
BUILTIN\Administrators (alias)	Debug programs
BUILTIN\Administrators (alias)	Enable computer and user accounts to be trusted for delegation
BUILTIN\Administrators (alias)	Force shutdown from a remote system
BUILTIN\Administrators (alias)	Generate security audits
BUILTIN\Administrators (alias)	Increase scheduling priority
BUILTIN\Administrators (alias)	Load and unload device drivers
BUILTIN\Administrators (alias)	Log on as a batch job
BUILTIN\Administrators (alias)	Manage auditing and security log
BUILTIN\Administrators (alias)	Modify firmware environment values
BUILTIN\Administrators (alias)	Profile single process
BUILTIN\Administrators (alias)	Profile system performance
BUILTIN\Administrators (alias)	Remove computer from docking station
BUILTIN\Administrators (alias)	Replace a process level token
BUILTIN\Administrators (alias)	Restore files and directories
BUILTIN\Administrators (alias)	Shut down the system
BUILTIN\Administrators (alias)	Synchronize directory service data
BUILTIN\Administrators (alias)	Take ownership of files or other objects

User List	User Privilege
BUILTIN\Backup Operators (alias)	Act as part of the operating system
BUILTIN\Backup Operators (alias)	Back up files and directories
BUILTIN\Backup Operators (alias)	Log on as a batch job
BUILTIN\Backup Operators (alias)	Log on as a service
BUILTIN\Backup Operators (alias)	Restore files and directories
BUILTIN\Backup Operators (alias)	Shut down the system
BUILTIN\Pre-Windows 2000 Compatible Access (alias)	Access this computer from the network
BUILTIN\Pre-Windows 2000 Compatible Access (alias)	Bypass traverse checking
BUILTIN\Print Operators (alias)	Load and unload device drivers
BUILTIN\Print Operators (alias)	Shut down the system
BUILTIN\Server Operators (alias)	Back up files and directories
BUILTIN\Server Operators (alias)	Change the system time
BUILTIN\Server Operators (alias)	Force shutdown from a remote system
BUILTIN\Server Operators (alias)	Restore files and directories
BUILTIN\Server Operators (alias)	Shut down the system
Everyone (well-known group)	Bypass traverse checking
NT AUTHORITY\Authenticated Users (well-known group)	Access this computer from the network
NT AUTHORITY\Authenticated Users (well-known group)	Add workstations to domain
NT AUTHORITY\ENTERPRISE DOMAIN CONTROLLERS (well-known group)	Access this computer from the network
NT AUTHORITY\LOCAL SERVICE (well-known group)	Adjust memory quotas for a process
NT AUTHORITY\LOCAL SERVICE (well-known group)	Change the system time
NT AUTHORITY\LOCAL SERVICE (well-known group)	Generate security audits
NT AUTHORITY\LOCAL SERVICE (well-known group)	Log on as a batch job
NT AUTHORITY\LOCAL SERVICE (well-known group)	Replace a process level token
NT AUTHORITY\NETWORK SERVICE (well-known group)	Adjust memory quotas for a process
NT AUTHORITY\NETWORK SERVICE (well-known group)	Generate security audits
NT AUTHORITY\NETWORK SERVICE (well-known group)	Log on as a service
NT AUTHORITY\NETWORK SERVICE (well-known group)	Replace a process level token
NT AUTHORITY\SYSTEM (well-known group)	Lock pages in memory
NT AUTHORITY\SYSTEM (well-known group)	Log on as a batch job
S-1-5-21-3734189588-1271080782-879282008-512	Manage auditing and security log
S-1-5-21-586393433-2332019824-216323568-1000	Log on as a batch job
S-1-5-21-586393433-2332019824-216323568-1001	Access this computer from the network
S-1-5-21-586393433-2332019824-216323568-1001	Adjust memory quotas for a process
S-1-5-21-586393433-2332019824-216323568-1001	Log on as a batch job

User List	User Privilege
S-1-5-21-586393433-2332019824-216323568-1001	Replace a process level token
S-1-5-21-586393433-2332019824-216323568-1002	Access this computer from the network
S-1-5-21-586393433-2332019824-216323568-1002	Allow log on locally
S-1-5-21-586393433-2332019824-216323568-1002	Log on as a batch job