

Security Event ID's To Log and Monitor In MonitorIT

A) Logon events:

Logon Events that Appear in Event Log

Event ID Description

528 A user successfully logged on to a computer.

529 The logon attempt was made with an unknown user name or a known user name with a bad password.

530 The user account tried to log on outside of the allowed time.

531 A logon attempt was made using a disabled account.

532 A logon attempt was made using an expired account.

533 The user is not allowed to log on at this computer.

534 The user attempted to log on with a logon type that is not allowed, such as network, interactive, batch, service, or remote interactive.

535 The password for the specified account has expired.

536 The Net Logon service is not active.

537 The logon attempt failed for other reasons.

538 A user logged off.

539 The account was locked out at the time the logon attempt was made. This event can indicate that a password attack was launched unsuccessfully resulting in the account being locked out.

540 Successful Network Logon. This event indicates that a remote user has connected from the network to a local resource on the server, generating a token for the network user.

682 A user has reconnected to a disconnected Terminal Services session. This event indicates that a previous Terminal Services session was connected to.

683 A user disconnected a Terminal Services session without logging off. This event is generated when a user is connected to a Terminal Services session over the network. It appears on the terminal server.

The following Logon security Event IDs should be logged and Watched by MonitorIT: 529, 531, 532, 533, 534, 537, 539

Action: Alert based on following criteria:

529: Min Notif Int=30 mins ; 5 occurrences within 120 secs

531: Min Notif Int=30 mins ; 5 occurrences within 120 secs

532: Min Notif Int=30 mins ; 5 occurrences within 120 secs

533: Min Notif Int=30 mins ; 5 occurrences within 120 secs

534: Min Notif Int=30 mins ; 5 occurrences within 120 secs

537: Min Notif Int=30 mins ; 5 occurrences within 120 secs

539: Min Notif Int=30 mins ; 5 occurrences within 120 secs

- **Local logon Attempt Failures:** The following Event IDs indicates failed logon attempts: 529, 531, 532, 533, 534, and 537. You will see events 529 and 534 if an attacker tries and fails to guess a username and password combination for a local account. However, these events can also occur when a user forgets their password, or starts browsing the network through My Network Places.
- **Account misuse:** Events 531, 532, and 533 can all represent misuse of a user account. The events indicate that the account/password combination was correctly entered, but other restrictions are preventing a successful log on.
- **Account lockouts:** Event 539 indicates that an account was locked out. This can indicate that a password attack has failed.

B) Account logon events:

Account Logon Events that Appear in Event Log

Event ID Description

672 An authentication service (AS) ticket was successfully issued and validated.

673 A ticket granting service (TGS) ticket was granted.

674 A security principal renewed an AS ticket or TGS ticket.

675 Pre-authentication failed.

676 Authentication Ticket Request Failed

677 A TGS ticket was not granted.

678 An account was successfully mapped to a domain account.

680 Identifies the account used for the successful logon attempt. This event also indicates the authentication package used to authenticate the account.

681 A domain account log on was attempted.

682 A user has reconnected to a disconnected Terminal Services session.

683 A user disconnected a Terminal Services session without logging off.

The following Account Logon security Event IDs should be logged by MonitorIT: 675, 677

Action: Alert based on following criteria:

675: Min Notif Int=30 mins ; 5 occurrences within 120 secs

677: Min Notif Int=30 mins ; 5 occurrences within 120 secs

- **Domain Logon Attempt Failures:** Event IDs **675** and **677** indicate failed attempts to logon to the domain.
- **Time Synchronization Issues:** If a client computer's time differs from the authenticating domain controller's by more than five minutes (by default), Event ID **675** will appear in the security log.

C) Account Management:

Account Management Events that Appear in Event Log

Event ID Description

624 User Account Created

625 User Account Type Change

626 User Account Enabled

627 Password Change Attempted

628 User Account Password Set

629 User Account Disabled

630 User Account Deleted

631 Security Enabled Global Group Created

632 Security Enabled Global Group Member Added

633 Security Enabled Global Group Member Removed

634 Security Enabled Global Group Deleted

635 Security Disabled Local Group Created

636 Security Enabled Local Group Member Added

637 Security Enabled Local Group Member Removed

638 Security Enabled Local Group Deleted
639 Security Enabled Local Group Changed
641 Security Enabled Global Group Changed
642 User Account Changed
643 Domain Policy Changed
644 User Account Locked Out

The following Account Management security Event IDs should be logged by MonitorIT: 624, 626, 632, 633, 642, 644

Action:

624: Record event ; Review all account activity on a weekly basis

626: Record event ; Review all account activity on a weekly basis

632: Record event ; Review all account activity on a weekly basis

633: Record event ; Review all account activity on a weekly basis

642: Record event ; Review all account activity on a weekly basis

644: Record event ; Review all account activity on a weekly basis

Creation of a User Account: Event IDs **624** and **626** identify when user accounts are created and enabled. If account creation is limited to specific individuals in the organization, you can use these events to identify whether unauthorized personnel have created user accounts.

Modification of Security Groups: For global group membership modifications, log Event IDs **632** and **633**. For domain local group membership modifications, log Event Ids **636** and **637**.

Account Lockout: Log events **642** and **644** in MonitorIT. When an account is locked out, two events will be logged at the PDC emulator operations master. A **644** event will indicate that the account name was locked out, and then a **642** event is recorded, indicating that the user account is changed to indicate that the account is now locked out. This event is only logged at the PDC emulator.

D) Privilege Use:

Privilege Use Events that Appear in Event Log

Event ID Description

576 Specified privileges were added to a user's access token. (This event is generated when the user logs on.)

577 A user attempted to perform a privileged system service operation.

578 Privileges were used on an already open handle to a protected object.

The following Privilege Use security Event IDs should be logged by MonitorIT: 577 and 578

Action:

577: Record event w/ appropriate sub-string ; Review all privilege change activity on a weekly basis

578: Record event w/ appropriate sub-string ; Review all privilege change activity on a weekly basis

- **Act as part of the operating system.** Look for Event ID **577** or **578** with SeTcbPrivilege privilege indicated. The user account that made use of the user right is identified in the event details. This event can indicate a user's attempt to elevate security privileges by acting as part of the operating system. For example, the GetAdmin attack, where a user attempted to add their account to the Administrators group used this privilege. The only entries for this event should be for the System account, and any service accounts assigned this user right.
- **Change the system time.** Look for Event ID **577** or **578** with SeSystemtimePrivilege privilege indicated. The user account that used the user right is identified in the event details. This event can indicate a user's attempt to change the system time to hide the true time that an event takes place.
- **Force shutdown from a remote system.** Look for Event IDs **577** and **578** with user right SeRemoteShutdownPrivilege. The specific security identifier (SID) the user right is assigned to and the user name of the security principal that assigned the right are included in the event details.
- **Load and unload device drivers.** Look for Event ID **577** or **578** with SeLoadDriverPrivilege privilege indicated. The user account that made use of this user right is identified in the event details.

This event can indicate a user's attempt to load an unauthorized or Trojan horse version of a device driver.

- **Manage auditing and security log.** Look for Event ID **577** or **578** with SeSecurityPrivilege privilege indicated. The user account that made use of this user right is identified in the event details. This event will occur both when the event log is cleared, and when events for privilege use are written to the security log.
- **Shut down the system.** Look for Event ID **577** with SeShutdownPrivilege privilege indicated. The user account that made use of this user right is identified in the event details. This event will occur when an attempt to shut down the computer takes place.
- **Take ownership of files or other objects.** Look for Event ID **577** or **578** with SeTakeOwnershipPrivilege privilege indicated. The user account that used the user right is identified in the event details. This event can indicate that an attacker is attempting to bypass current security settings by taking ownership of an object.

E) System Events:

System Events that Appear in Event Log

Event ID Description

512 Windows is starting up.

513 Windows is shutting down.

514 An authentication package was loaded by the Local Security Authority.

515 A trusted logon process has registered with the Local Security Authority.

516 Internal resources allocated for the queuing of security event messages have been exhausted, leading to the loss of some security event messages.

517 The security log was cleared.

518 A notification package was loaded by the Security Accounts Manager.

1001 System blue screen restart, with a source of Save Dump

The following System Event IDs should be logged by MonitorIT: 512, 513, 517, and 1001

Action:

512: Record event, but no alert. Other up/down alerting in place.

513: Record event, but no alert. Other up/down alerting in place.

517: Record event, but no alert. Other up/down alerting in place.

1001: Record event, but no alert. Other up/down alerting in place.

- **Computer shutdown/restart.** Event ID **513** shows Windows shutting down. It is important to know when servers have been shut down or rebooted.
- **System restart was due to a blue screen**, with a source of Save Dump. Event ID **1001**.
- **Modifying or Clearing of the Security Log.** All occurrences of Event ID **517** should be logged in MonitorIT . An unauthorized clearing of the security log can be an attempt to hide events that existed in the previous security log. The name of the user that cleared the log is included in the event details.

F) Policy Change:

Policy Change Events that Appear in Event Log

Event ID Description

608 A user right was assigned.

609 A user right was removed.

610 A trust relationship with another domain was created.

611 A trust relationship with another domain was removed.

612 An audit policy was changed.

768 A collision was detected between a namespace element in one forest and a namespace element in another forest (occurs when a namespace element in one forest overlaps a namespace element in another forest).

The following Policy Change Event IDs should be logged by MonitorIT: 608, 609, and 612

Action:

608: Record event w/ appropriate sub-string ; Review all policy activity on a weekly basis

609: Record event w/ appropriate sub-string ; Review all policy activity on a weekly basis

612: Record event w/ appropriate sub-string ; Review all policy activity on a weekly basis

The two most important events to look for here are Event IDs **608** and **609**. A number of attempted attacks may result in these events being recorded. The following examples will all generate Event ID **608** if the user right is assigned or **609** if it is removed. In each case the specific SID that the user right is assigned to, along with the user name of the security principal that assigned the right is included in the event details:

- **Act as part of the operating system.** Look for Event IDs 608 and 609 with user right `seTcbPrivilege` in the event details.
- **Add workstations to the domain.** Look for the events with user right `SeMachineAccountPrivilege` in the event details.
- **Back up files and directories.** Look for the events with user right `SeBackupPrivilege` in the event details.
- **Bypass traverse checking.** Look for events with user right `SeChangeNotifyPrivilege` in the event details. This user right allows users to traverse a directory tree even if the user has no other permissions to access that directory.
- **Change the system time.** Look for events with user right `SeSystemtimePrivilege` in the event details. This user right allows a security principal to change the system time, potentially masking when an event takes place.
- **Create permanent shared objects.** Look for events with user right `SeCreatePermanentPrivilege` in the event details. The holder of this user right can create file and print shares.
- **Debug programs.** Look for events with user right `SeDebugPrivilege` in the event details. A holder of this user right

can attach to any process. This right is, by default, only assigned to Administrators.

- **Force shutdown from a remote system.** Look for events with user right SeRemoteShutdownPrivilege in the event details.
- **Increase scheduling priority.** Look for events with user right SeIncreaseBasePriorityPrivilege in the event details. A user with this right can modify process priorities.
- **Load and unload device drivers.** Look for events with user right SeLoadDriverPrivilege in the event details. A user with this user right could load a Trojan horse version of a device driver.
- **Manage auditing and security log.** Look for events with user right SeSecurityPrivilege in the event details. A user with this user right can view and clear the security log.
- **Replace a process level token.** Look for events with user right SeAssignPrimaryTokenPrivilege in the event details. A user with this user right can change the default token associated with a started subprocess.
- **Restore files and directories.** Look for events with user right SeRestorePrivilege in the event details.
- **Shut down the system.** Look for events with user right SeShutdownPrivilege in the event details. A user with this user right could shut down the system to initialize the installation of a new device driver.
- **Take ownership of files or other objects.** Look for events with user right SeTakeOwnershipPrivilege in the event details. A user with this user right can access any object or file on an NTFS disk by taking ownership of the object or file.