Knowledge Base

Windows 2000 Security Event Descriptions (Part 1 of 2)

PSS ID Number: 299475

Article Last Modified on 12/3/2003

The information in this article applies to:

- Microsoft Windows 2000 Server SP1
- Microsoft Windows 2000 Server SP2
- Microsoft Windows 2000 Advanced Server SP1
- Microsoft Windows 2000 Advanced Server SP2
- Microsoft Windows 2000 Professional SP1
- Microsoft Windows 2000 Professional SP2
- Microsoft Windows 2000 Datacenter Server SP2

This article was previously published under Q299475

SUMMARY

This article contains descriptions of various security-related and auditing-related events, and information about how to interpret these events. These events will all appear in the Security event log and will be logged with a source of "Security." The following article in the Microsoft Knowledge Base is Part 2 of 2:

301677 Windows 2000 Security Event Descriptions (Part 2 of 2)

MORE INFORMATION

```
    Event ID: 512 (0x0200)
        Type: Success Audit
Description: Windows NT is starting up.


    Event ID: 513 (0x0201)
        Type: Success Audit
Description: Windows NT is shutting down.
             All logon sessions will be terminated by this shutdown.


    Event ID: 514 (0x0202)
        Type: Success Audit
Description: An authentication package has been loaded by the Local Security Authority.
             This authentication package will be used to authenticate logon attempts.
             Authentication Package Name: %1


    Event ID: 515 (0x0203)
        Type: Success Audit
Description: A trusted logon process has registered with the Local Security Authority.
             This logon process will be trusted to submit logon requests.
             Logon Process Name: %1


    Event ID: 516 (0x0204)

        Type: Success Audit
Description: Internal resources allocated for the queuing of audit messages have been
             exhausted, leading to the loss of some audits.
             Number of audit messages discarded: %1


    Event ID: 517 (0x0205)
        Type: Success Audit
Description: The audit log was cleared
             Primary User Name: %1    Primary Domain:    %2
             Primary Logon ID: %3     Client User Name: %4
             Client Domain:    %5     Client Logon ID:  %6


    Event ID: 518 (0x0206)
        Type: Success Audit
Description: An notification package has been loaded by the Security Account Manager.
             This package will be notified of any account or password changes.
             Notification Package Name: %1


    Event ID: 528 (0x0210)
        Type: Success Audit
Description: Successful Logon:
             User Name: %1            Domain: %2
             Logon ID: %3             Logon Type: %4
             Logon Process: %5        Authentication Package: %6
             Workstation Name: %7


    Event ID: 529 (0x0211)
        Type: Failure Audit
Description: Logon Failure
             Reason: Unknown user name or bad password
             User Name: %1            Domain: %2
             Logon Type: %3           Logon Process: %4
             Authentication Package: %5 Workstation Name: %6
```

```
   Event ID: 530 (0x0212)
       Type: Failure Audit
Description: Logon Failure
            Reason: Account logon time restriction violation
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 531 (0x0213)
       Type: Failure Audit
Description: Logon Failure
            Reason: Account currently disabled
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 532 (0x0214)
       Type: Failure Audit
Description: Logon Failure
            Reason: The specified user account has expired
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 533 (0x0215)
       Type: Failure Audit
Description: Logon Failure
            Reason: User not allowed to logon at this computer
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 534 (0x0216)
       Type: Failure Audit
Description: Logon Failure
            Reason:The user has not been granted the requested
            logon type at this machine
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 535 (0x0217)
       Type: Failure Audit
Description: Logon Failure
            Reason: The specified account's password has expired
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 536 (0x0218)
       Type: Failure Audit
Description: Logon Failure
            Reason: The NetLogon component is not active
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 537 (0x0219)
       Type: Failure Audit
Description: Logon Failure
            Reason: An unexpected error occurred during logon
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 538 (0x021A)
       Type: Success Audit
Description: User Logoff
            User Name: %1              Domain: %2
            Logon ID: %3               Logon Type: %4.


   Event ID: 539 (0x021B)
       Type: Failure Audit
Description: Logon Failure
            Reason: Account locked out
            User Name: %1              Domain: %2
            Logon Type: %3             Logon Process: %4
            Authentication Package: %5 Workstation Name: %6


   Event ID: 540 (0x021c)
       Type: Success Audit
Description: Successful Network Logon
            User Name: %1              Domain: %2
            Logon ID: %3               Logon Type: %4
            Logon Process: %5          Authentication Package: %6
            Workstation Name: %7


   Event ID: 541 (0x021d)
       Type: Success Audit
```

```
Description: IKE security association established.
            Mode: %1                    Peer Identity: %2
            Filter: %3                  Parameters: %4


    Event ID: 542 (0x021e)
        Type: Success Audit
Description: IKE security association ended.
            Mode: Data Protection (Quick mode)
            Filter: %1                  Inbound SPI: %2
            Outbound SPI: %3


    Event ID: 543 (0x021f)
        Type: Success Audit
Description: IKE security association ended.
            Mode: Key Exchange (Main mode)
            Filter: %1


    Event ID: 544 (0x0220)
        Type: Failure Audit
Description: IKE security association establishment failed because peer could not
            authenticate. The certificate trust could not be established.
            Peer Identity: %1          Filter: %2


    Event ID: 545 (0x0221)
        Type: Failure Audit
Description: IKE peer authentication failed.
            Peer Identity: %1          Filter: %2


    Event ID: 546 (0x0222)
        Type: Failure Audit
Description: IKE security association establishment failed because peer
            sent invalid proposal.
            Mode: %1                    Filter: %2
            Attribute: %3               Expected value: %4
            Received value: %5


    Event ID: 547 (0x0223)
        Type: Failure Audit
Description: IKE security association negotiation failed.
            Mode:         %1           Filter: %2
            Failure Point: %3          Failure Reason: %4


    Event ID: 560 (0x0230)
        Type: Success Audit
Description: Object Open
            Object Server: %1          Object Type: %2
            Object Name: %3            New Handle ID: %4
            Operation ID:{%5,%6}       Process ID: %7
            Primary User Name: %8      Primary Domain: %9
            Primary Logon ID: %10      Client User Name: %11
            Client Domain: %12         Client Logon ID: %13
            Accesses %14               Privileges %15


    Event ID: 561 (0x0231)
        Type: Success Audit
Description: Handle Allocated
            Handle ID: %1              Operation ID:{%2,%3}
            Process ID: %4


    Event ID: 562 (0x0232)
        Type: Success Audit
Description: Handle Closed
            Object Server: %1          Handle ID: %2
            Process ID: %3


    Event ID: 563 (0x0233)
        Type: Success Audit
Description: Object Open for Delete
            Object Server: %1          Object Type: %2
            Object Name: %3            New Handle ID: %4
            Operation ID:{%5,%6}       Process ID: %7
            Primary User Name: %8      Primary Domain: %9
            Primary Logon ID: %10      Client User Name: %11
            Client Domain: %12         Client Logon ID: %13
            Accesses %14               Privileges %15


    Event ID: 564 (0x0234)
        Type: Success Audit
Description: Object Deleted
            Object Server: %1          Handle ID: %2
            Process ID: %3


    Event ID: 565 (0x0235)
        Type: Success Audit
Description: Object Open
            Object Server: %1          Object Type: %2
            Object Name: %3            New Handle ID: %4
            Operation ID:{%5,%6}       Process ID: %7
            Primary User Name: %8      Primary Domain: %9
```

```
              Primary Logon ID: %10        Client User Name: %11
              Client Domain: %12           Client Logon ID: %13
              Accesses %14                 Privileges %15
              Properties:%16%17%18%19%20%21%22%23%24%25


   Event ID: 566 (0x0236)
       Type: Success Audit
Description: Object Operation
              Operation Type %1           Object Type: %2
              Object Name: %3             Handle ID: %4
              Operation ID:{%5,%6}        Primary User Name: %7
              Primary Domain: %8          Primary Logon ID: %9
              Client User Name: %10       Client Domain: %11
              Client Logon ID: %12        Requested Accesses %13


   Event ID: 576 (0x0240)
       Type: Success Audit
Description: Special privileges assigned to new logon:
              User Name: %1               Domain: %2
              Logon ID: %3                Assigned: %4


   Event ID: 577 (0x0241)
       Type: Success Audit
Description: Privileged Service Called
              Server: %1                  Service: %2
              Primary User Name: %3       Primary Domain: %4
              Primary Logon ID: %5        Client User Name: %6
              Client Domain: %7           Client Logon ID: %8
              Privileges: %9


   Event ID: 578 (0x0242)
       Type: Success Audit
Description: Privileged object operation
              Object Server: %1           Object Handle: %2
              Process ID: %3              Primary User Name: %4
              Primary Domain: %5          Primary Logon ID: %6
              Client User Name: %7        Client Domain: %8
              Client Logon ID: %9         Privileges: %10


   Event ID: 592 (0x0250)
       Type: Success Audit
Description: A new process has been created
              New Process ID: %1          Image File Name: %2
              Creator Process ID: %3      User Name: %4
              Domain: %5                  Logon ID: %6


   Event ID: 593 (0x0251)
       Type: Success Audit
Description: A process has exited
              Process ID: %1              User Name: %2
              Domain: %3                  Logon ID: %4


   Event ID: 594 (0x0252)
       Type: Success Audit
Description: A handle to an object has been duplicated
              Source Handle ID: %1        Source Process ID: %2
              Target Handle ID: %3        Target Process ID: %4


   Event ID: 595 (0x0253)
       Type: Success Audit
Description: Indirect access to an object has been obtained
              Object Type: %1             Object Name: %2
              Process ID: %3              Primary User Name: %4
              Primary Domain: %5          Primary Logon ID: %6
              Client User Name: %7        Client Domain: %8
              Client Logon ID: %9         Accesses: %10
```