Frequently Asked Questions

Question

0 A H 8 D @ > 2 : 0 : > 4 > 2 8 7 ; > 3 > 2 Event ID 4 ; O A 5 @ 2 5 @ > 2 Win

Answer

> = B @ > ; ; 5 @ K 4 > < 5 = > 2

Event ID (0 B 5 3 > @ 8 O) ? 8 A 0 = 8 5

1) 675 8 ; 8 4771
(C 4 8 B A > 1 K B 8 9 2 E > 4 0 2 A 8 A B 5 < C)
! > 1 K B 8 5 675/4771 = 0 : > = B @ > ; ; 5 @ 5 4 > < 5 = 0 C : 0 7 K 2 0 5 B = 0
= 5 C 4 0 G = C N ? > ? K B : C 2 > 9 B 8 G 5 @ 5 7 Kerberos = 0 @ 0 1 > G 5 9 A B 0 = F 8 8 A
4 > < 5 = = > 9 C G 5 B = > 9 7 0 ? 8 A L N. 1 K G = > ? @ 8 G 8 = > 9 M B > 3 >
O 2 ; O 5 B A O = 5 A > > B 2 5 B A B 2 C N I 8 9 ? 0 @ > ; L, = > : > 4 > H 8 1 : 8
C : 0 7 K 2 0 5 B, ? > G 5 < C 8 < 5 = = > 0 C B 5 = B 8 D 8 : 0 F 8 O 1 K ; 0
= 5 C 4 0 G = > 9. " 0 1 ; 8 F 0 : > 4 > 2 > H 8 1 > : Kerberos ? @ 8 2 5 4 5 = 0 = 8 6 5.

2) 676, 8 ; 8 Failed 672 8 ; 8 4768
(C 4 8 B A > 1 K B 8 9 2 E > 4 0 2 A 8 A B 5 < C)
! > 1 K B 8 5 676/4768 ; > 3 3 8 @ C 5 B A O 4 ; O 4 @ C 3 8 E B 8 ? > 2 = 5 C 4 0 G = > 9
0 C B 5 = B 8 D 8 : 0 F 8 8. " 0 1 ; 8 F 0 : > 4 > 2 Kerberos ? @ 8 2 5 4 5 = 0 = 8 6 5.
: Windows 2003 Server A > 1 K B 8 5 > B : 0 7 0 7 0 ? 8 A K 2 0 5 B A O : 0 : 672
2 < 5 A B > 676.

3) 681 8 ; 8 Failed 680 8 ; 8 4776
(C 4 8 B A > 1 K B 8 9 2 E > 4 0 2 A 8 A B 5 < C)
! > 1 K B 8 5 681/4776 = 0 : > = B @ > ; ; 5 @ 5 4 > < 5 = 0 C : 0 7 K 2 0 5 B = 0
= 5 C 4 0 G = C N ? > ? K B : C 2 E > 4 0 2 A 8 A B 5 < C G 5 @ 5 7
NTLM A 4 > < 5 = = > 9 C G 5 B = > 9 7 0 ? 8 A L N. > 4 > H 8 1 : 8 C : 0 7 K 2 0 5 B,
? > G 5 < C 8 < 5 = = > 0 C B 5 = B 8 D 8 : 0 F 8 O 1 K ; 0 = 5 C 4 0 G = > 9.
> 4 K > H 8 1 > : NTLM ? @ 8 2 5 4 5 = K = 8 6 5.
: Windows 2003 Server A > 1 K B 8 5 > B : 0 7 0 7 0 ? 8 A K 2 0 5 B A O : 0 : 680
2 < 5 A B > 681.

4) 642 8 ; 8 4738
(C 4 8 B C ? @ 0 2 ; 5 = 8 O C G 5 B = K < 8 7 0 ? 8 A O < 8)
! > 1 K B 8 5 642/4738 C : 0 7 K 2 0 5 B = 0 8 7 < 5 = 5 = 8 O 2 C : 0 7 0 = = > 9
C G 5 B = > 9 7 0 ? 8 A 8, B 0 : 8 5 : 0 : A 1 @ > A ? 0 @ > ; O 8 ; 8 0 : B 8 2 0 F 8 O
4 5 0 : B 8 2 8 @ > 2 0 = = > 9 4 > M B > 3 > C G 5 B = > 9 7 0 ? 8 A 8. ? 8 A 0 = 8 5
A > 1 K B 8 O C B > G = O 5 B A O 2 A > > B 2 5 B A B 2 8 5 A B 8 ? > < 8 7 < 5 = 5 = 8 O.

5) 632 8 ; 8 4728; 636 8 ; 8 4732; 660 8 ; 8 4756
(C 4 8 B C ? @ 0 2 ; 5 = 8 O C G 5 B = K < 8 7 0 ? 8 A O < 8)

A 5 B @ 8 A > 1 K B 8 O C : 0 7 K 2 0 N B = 0 B >, G B > C : 0 7 0 = = K 9
? > ; L 7 > 2 0 B 5 ; L 1 K ; 4 > 1 0 2 ; 5 = 2 > ? @ 5 4 5 ; 5 = = C N 3 @ C ? ? C.
1 > 7 = 0 G 5 = K ; > 1 0 ; L = 0 O (Global), > : 0 ; L = 0 O (Local) 8 1 I 0 O (Universal)
A > > B 2 5 B A B 2 5 = = > 4 ; O : 0 6 4 > 3 > ID.

6) 624 8 ; 8 4720
(C 4 8 B C ? @ 0 2 ; 5 = 8 O C G 5 B = K < 8 7 0 ? 8 A O < 8)
K ; 0 A > 7 4 0 = 0 = > 2 0 O C G 5 B = 0 O 7 0 ? 8 A L ? > ; L 7 > 2 0 B 5 ; O

7) 644 8 ; 8 4740
(C 4 8 B C ? @ 0 2 ; 5 = 8 O C G 5 B = K < 8 7 0 ? 8 A O < 8)
# G 5 B = 0 O 7 0 ? 8 A L C : 0 7 0 = = > 3 > ? > ; L 7 > 2 0 B 5 ; O 1 K ; 0
7 0 1 ; > : 8 @ > 2 0 = 0 ? > A ; 5 = 5 A : > ; L : 8 E ? > ? K B > : 2 E > 4 0

517 8 ; 8 1102
(C 4 8 B A 8 A B 5 < = K E A > 1 K B 8 9)
# : 0 7 0 = = K 9 ? > ; L 7 > 2 0 B 5 ; L > G 8 A B 8 ; 6 C @ = 0 ; 1 5 7 > ? 0 A = > A B 8

E > 4 8 2 K E > 4 8 7 A 8 A B 5 < K (Logon/Logoff)

Event Id ? 8 A 0 = 8 5

528 8 ; 8 4624 # A ? 5 H = K 9 2 E > 4 2 A 8 A B 5 < C
529 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C 5 8 7 2 5 A B = > 5 8 < O
? > ; L 7 > 2 0 B 5 ; O 8 ; 8 = 5 2 5 @ = K 9 ? 0 @ > ; L
530 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C E > 4 2 A 8 A B 5 < C = 5 1 K ;
> A C I 5 A B 2 ; 5 = 2 B 5 G 5 = 8 5 > 1 > 7 = 0 G 5 = = > 3 > ? 5 @ 8 > 4 0
2 @ 5 < 5 = 8
531 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C # G 5 B = 0 O 7 0 ? 8 A L
2 @ 5 < 5 = = > 4 5 0 : B 8 2 8 @ > 2 0 = 0
532 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C ! @ > : 8 A ? > ; L 7 > 2 0 = 8 O
C : 0 7 0 = = > 9 C G 5 B = > 9 7 0 ? 8 A 8 8 A B 5 :
533 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C > ; L 7 > 2 0 B 5 ; N = 5
@ 0 7 @ 5 H 0 5 B A O > A C I 5 A B 2 ; O B L 2 E > 4 2 A 8 A B 5 < C = 0 4 0 = = > <
: > < ? L N B 5 @ 5
534 8 ; 8 4625 8 ; 8 5461 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C > ; L 7 > 2 0 B 5 ; L = 5
1 K ; @ 0 7 @ 5 H 5 = 7 0 ? @ 0 H 8 2 0 5 < K 9 B 8 ? 2 E > 4 0 = 0 4 0 = = > <
: > < ? L N B 5 @ 5
535 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C ! @ > : 4 5 9 A B 2 8 O ? 0 @ > ; O
C : 0 7 0 = = > 9 C G 5 B = > 9 7 0 ? 8 A 8 8 A B 5 :
539 8 ; 8 4625 B : 0 7 2 E > 4 0 2 A 8 A B 5 < C # G 5 B = 0 O 7 0 ? 8 A L
7 0 1 ; > : 8 @ > 2 0 = 0
540 8 ; 8 4624 # A ? 5 H = K 9 A 5 B 5 2 > 9 2 E > 4 2 A 8 A B 5 < C (" > ; L : > Windows
2000, XP, 2003)

" 8 ? K 2 E > 4 > 2 2 A 8 A B 5 < C (Logon Types)

" 8 ? 2 E > 4 0 2 A 8 A B 5 < C   ? 8 A 0 = 8 5

2   = B 5 @ 0 : B 8 2 = K 9 (2 E > 4 A : ; 0 2 8 0 B C @ K 8 ; 8 M : @ 0 = 0 A 8 A B 5 < K)
3   ! 5 B 5 2 > 9 (= 0 ? @ 8 < 5 @, ? > 4 : ; N G 5 = 8 5 : > 1 I 5 9 ? 0 ? : 5 = 0
M B > < : > < ? L N B 5 @ 5 8 7 ; N 1 > 3 > < 5 A B 0 2 A 5 B 8 8 ; 8 IIS 2 E > 4
8 : > 3 4 0 = 5 7 0 E > 4 8 ; 528 = 0 Windows Server 2000 8 2 K H 5. ! <. A > 1 K B 8 5 540)
4   0 : 5 B (batch) (= 0 ? @ 8 < 5 @, 7 0 ? ; 0 = 8 @ > 2 0 = = 0 O 7 0 4 0 G 0)
5   ! ; C 6 1 0 (0 ? C A : A ; C 6 1 K)
7   0 7 1 ; > : 8 @ > 2 : 0 (= 0 ? @ 8 < 5 @, = 5 > 1 A ; C 6 8 2 0 5 < 0 O @ 0 1 > G 0 O
A B 0 = F 8 O A 7 0 I 8 I 5 = = K < ? 0 @ > ; 5 < A : @ 8 = A 5 9 2 5 @ > <)
8   NetworkCleartext (E > 4 A ? > ; = > < > G 8 O < 8 (credentials), > B ? @ 0 2 ; 5 = = K < 8 2
2 8 4 5 ? @ > A B > 3 > B 5 : A B. ' 0 A B > > 1 > 7 = 0 G 0 5 B 2 E > 4 2 IIS A
1 0 7 > 2 > 9 0 C B 5 = B 8 D 8 : 0 F 8 5 9)
9   NewCredentials
10   RemoteInteractive (" 5 @ < 8 = 0 ; L = K 5 A ; C 6 1 K, # 4 0 ; 5 = = K 9 @ 0 1 > G 8 9
A B > ; 8 ; 8 C 4 0 ; 5 = = K 9 ? > < > I = 8 :)
11   CachedInteractive (2 E > 4 A : 5 H 8 @ > 2 0 = = K < 8 4 > < 5 = = K < 8
? > ; = > < > G 8 O < 8, = 0 ? @ 8 < 5 @, 2 E > 4 = 0 @ 0 1 > G C N A B 0 = F 8 N,
: > B > @ 0 O = 0 E > 4 8 B A O = 5 2 A 5 B 8)

> 4 K > B : 0 7 > 2 Kerberos

> 4 > H 8 1 : 8   @ 8 G 8 = 0

6   < O ? > ; L 7 > 2 0 B 5 ; O = 5 A C I 5 A B 2 C 5 B
12   3 @ 0 = 8 G 5 = 8 5 @ 0 1 > G 5 9 < 0 H 8 = K; > 3 @ 0 = 8 G 5 = 8 5 2 @ 5 < 5 = 8
2 E > 4 0 2 A 8 A B 5 < C
18   # G 5 B = 0 O 7 0 ? 8 A L 4 5 0 : B 8 2 8 @ > 2 0 = 0, 7 0 1 ; > : 8 @ > 2 0 = 0 8 ; 8
8 A B 5 : A @ > : 5 5 4 5 9 A B 2 8 O
23   A B 5 : A @ > : 4 5 9 A B 2 8 O ? 0 @ > ; O ? > ; L 7 > 2 0 B 5 ; O
24   @ 5 4 2 0 @ 8 B 5 ; L = 0 O 0 C B 5 = B 8 D 8 : 0 F 8 O = 5 C 4 0 ; 0 A L; > 1 K G = >
? @ 8 G 8 = > 9 O 2 ; O 5 B A O = 5 2 5 @ = K 9 ? 0 @ > ; L
32   A B 5 : A @ > : 4 5 9 A B 2 8 O 7 0 O 2 : 8. - B > = > @ < 0 ; L = > 5 A > 1 K B 8 5,
: > B > @ > 5 ; > 3 3 8 @ C 5 B A O C G 5 B = K < 8 7 0 ? 8 A O < 8 : > < ? L N B 5 @ > 2
37   @ 5 < O = 0 @ 0 1 > G 5 9 < 0 H 8 = K 4 0 2 = > = 5
A 8 = E @ > = 8 7 8 @ > 2 0 ; > A L A > 2 @ 5 < 5 = 5 < = 0 : > = B @ > ; ; 5 @ 5
4 > < 5 = 0

> 4 K > H 8 1 > : NTLM

> 4 > H 8 1 : 8 (4 5 A O B 8 G = 0 O A 8 A B 5 < 0)   > 4 > H 8 1 : 8 (16- @ 8 G = 0 O
A 8 A B 5 < 0)   ? 8 A 0 = 8 5

3221225572   C0000064   " 0 : > 3 > 8 < 5 = 8 ? > ; L 7 > 2 0 B 5 ; O = 5 A C I 5 A B 2 C 5 B
3221225578   C000006A   5 @ = > 5 8 < O ? > ; L 7 > 2 0 B 5 ; O, = > = 5 2 5 @ = K 9
? 0 @ > ; L
3221226036   C0000234   # G 5 B = 0 O 7 0 ? 8 A L ? > ; L 7 > 2 0 B 5 ; O

701;>:8@>20=0

3221225586 C0000072 #G5B=0O 70?8AL 450:B828@>20=0

3221225583 C000006F >;L7>20B5;L ?KB05BAO 2>9B8 2 A8AB5<C 2=5
>1>7=0G5==>3> ?5@8>40 2@5<5=8 (@01>G53> 2@5<5=8)

3221225584 C0000070 3@0=8G5=85 @01>G59 AB0=F88

3221225875 C0000193 AB5: A@>: 459AB28O CG5B=>9 70?8A8

3221225585 C0000071 AB5: A@>: 459AB28O ?0@>;O

3221226020 C0000224 >;L7>20B5;L 4>;65= ?><5=OBL ?0@>;L
?@8 A;54CNI5< 2E>45 2 A8AB5<C

7OB> >BAN40 .

Details

Info Thursday 19 July 2018 - 17:28:29 by vampyr