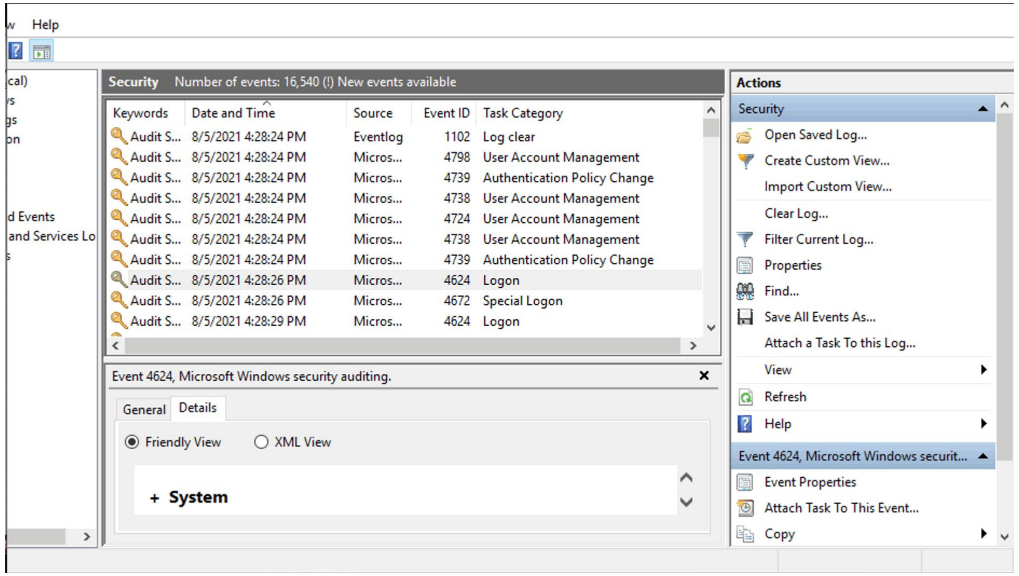
Data Parsing Narrative

Evan Noyes, Devin Rankin, Benjamin Kamide

Temple University

Event 4624 - Evan

- Event 4624 occurs on successful user logon.

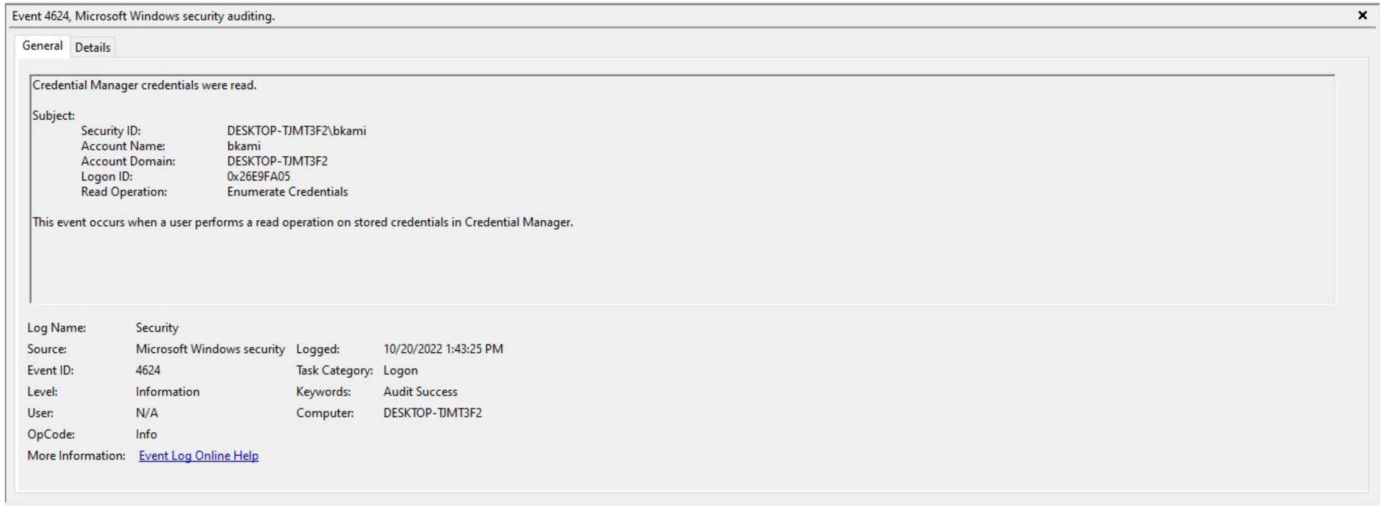


Security Number of events: 16,540 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	8/5/2021 4:28:24 PM	Eventlog	1102	Log clear
Audit S...	8/5/2021 4:28:24 PM	Micros...	4798	User Account Management
Audit S...	8/5/2021 4:28:24 PM	Micros...	4739	Authentication Policy Change
Audit S...	8/5/2021 4:28:24 PM	Micros...	4738	User Account Management
Audit S...	8/5/2021 4:28:24 PM	Micros...	4724	User Account Management
Audit S...	8/5/2021 4:28:24 PM	Micros...	4738	User Account Management
Audit S...	8/5/2021 4:28:24 PM	Micros...	4739	Authentication Policy Change
Audit S...	8/5/2021 4:28:26 PM	Micros...	4624	Logon
Audit S...	8/5/2021 4:28:26 PM	Micros...	4672	Special Logon
Audit S...	8/5/2021 4:28:29 PM	Micros...	4624	Logon

Event 4624, Microsoft Windows security auditing.

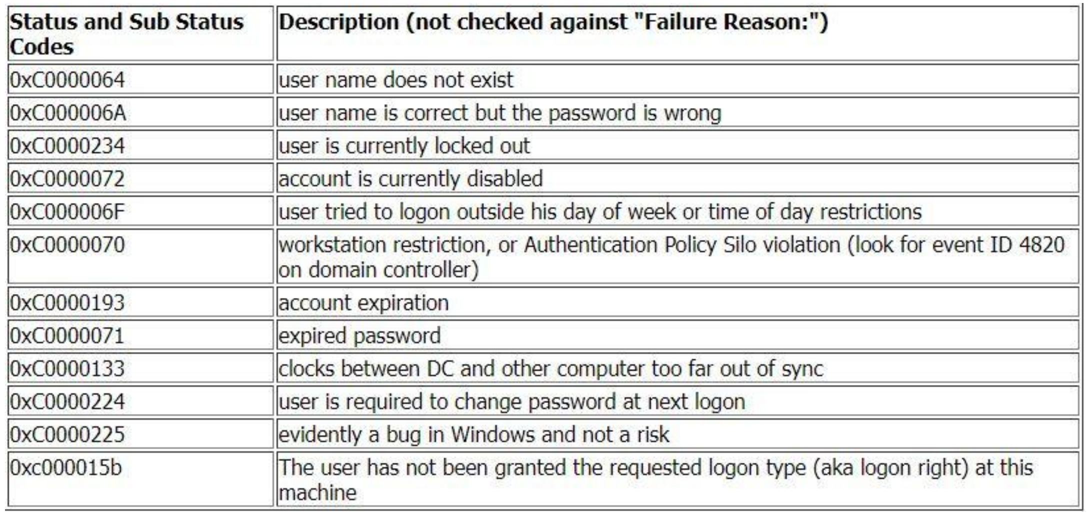
● Friendly View ○ XML View



Event 4624, Microsoft Windows security auditing.

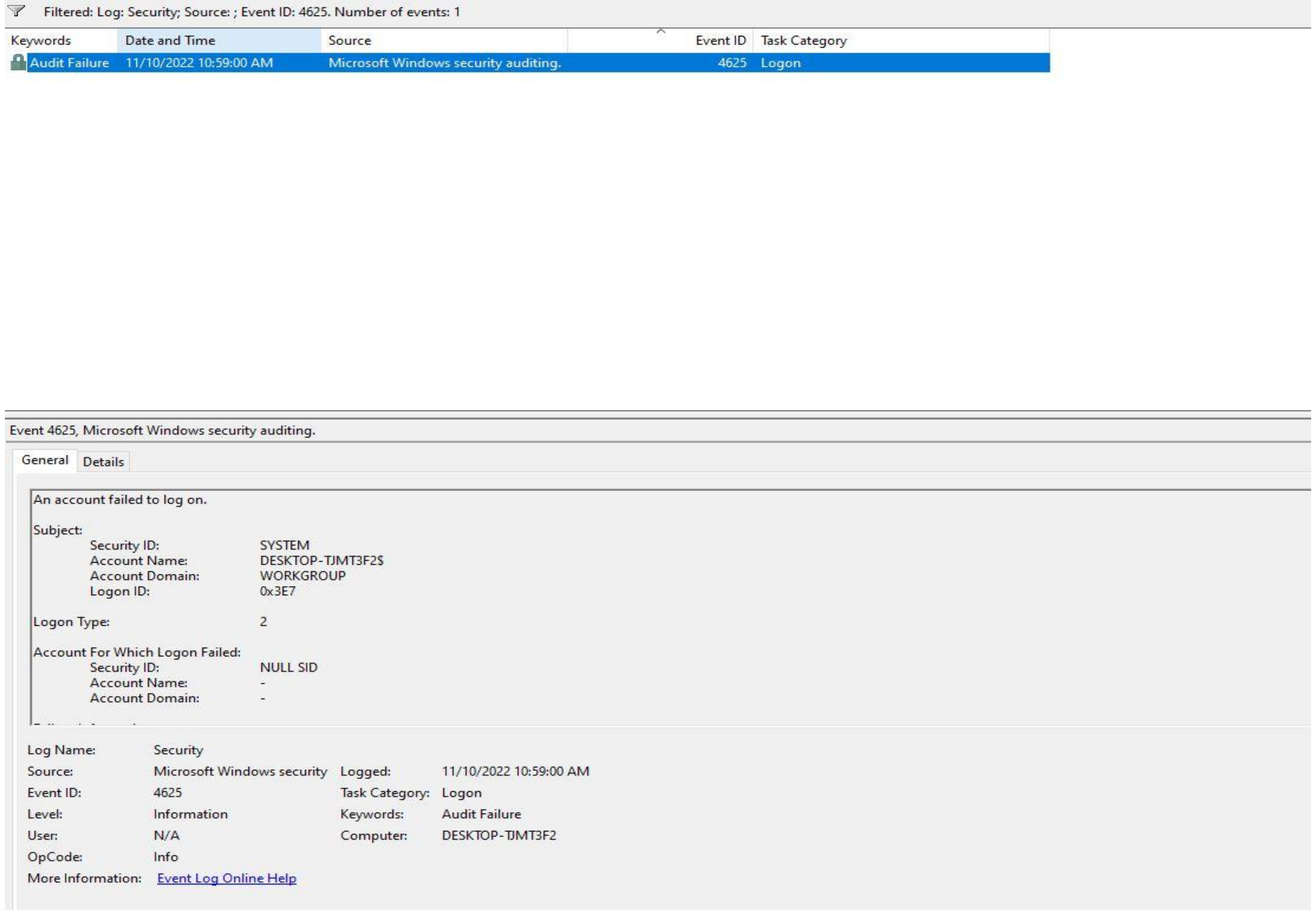
```
Credential Manager credentials were read.

Subject:
        Security ID:          DESKTOP-TJMT3F2\bkami
        Account Name:         bkami
        Account Domain:       DESKTOP-TJMT3F2
        Logon ID:             0x26E9FA05
        Read Operation:       Enumerate Credentials

This event occurs when a user performs a read operation on stored credentials in Credential Manager.

Log Name:          Security
Source:            Microsoft Windows security   Logged:          10/20/2022 1:43:25 PM
Event ID:          4624                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Success
User:              N/A                          Computer:        DESKTOP-TJMT3F2
OpCode:            Info
More Information:  Event Log Online Help
```

Logon Failure Event 4625 - Ben



Status and Sub Status Codes	Description (not checked against "Failure Reason:")
0xC0000064	user name does not exist
0xC000006A	user name is correct but the password is wrong
0xC0000234	user is currently locked out
0xC0000072	account is currently disabled
0xC000006F	user tried to logon outside his day of week or time of day restrictions
0xC0000070	workstation restriction, or Authentication Policy Silo violation (look for event ID 4820 on domain controller)
0xC0000193	account expiration
0xC0000071	expired password
0xC0000133	clocks between DC and other computer too far out of sync
0xC0000224	user is required to change password at next logon
0xC0000225	evidently a bug in Windows and not a risk
0xc000015b	The user has not been granted the requested logon type (aka logon right) at this machine

- Codes for login failure
- Example of failed logins code was 0xC000006D
- This code says “An Error Occurred During Login”



```
Filtered: Log: Security; Source: ; Event ID: 4625. Number of events: 1

Keywords        Date and Time            Source                                   Event ID  Task Category
Audit Failure   11/10/2022 10:59:00 AM   Microsoft Windows security auditing.         4625  Logon
```

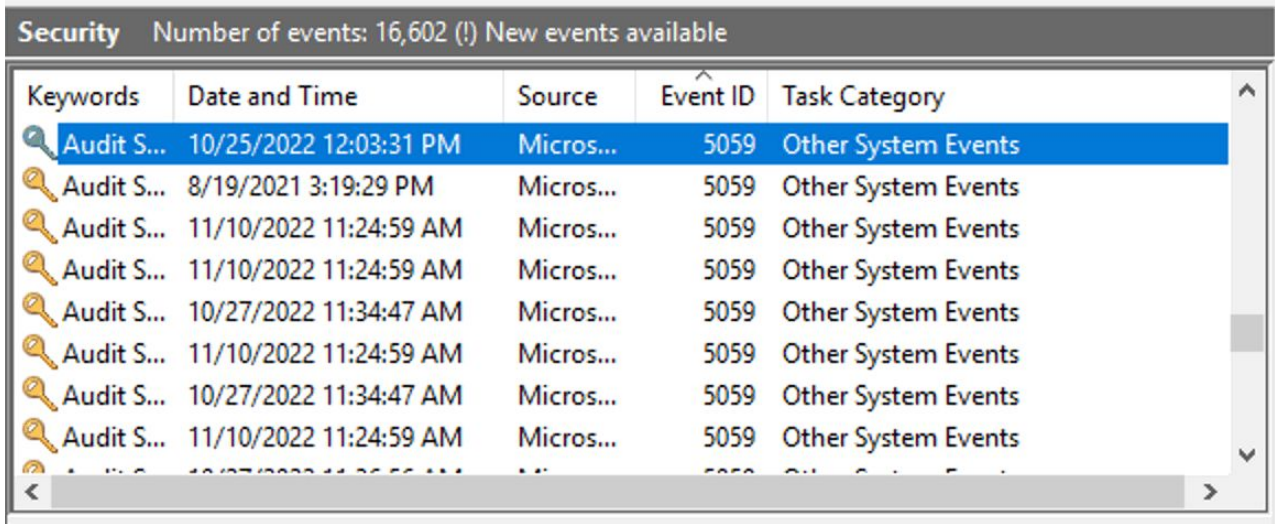
```
Event 4625, Microsoft Windows security auditing.
```

```
An account failed to log on.

Subject:
        Security ID:            SYSTEM
        Account Name:           DESKTOP-TJMT3F2$
        Account Domain:         WORKGROUP
        Logon ID:               0x3E7

Logon Type:                     2

Account For Which Logon Failed:
        Security ID:            NULL SID
        Account Name:           -
        Account Domain:         -
```

```
Log Name:          Security
Source:            Microsoft Windows security   Logged:          11/10/2022 10:59:00 AM
Event ID:          4625                         Task Category:   Logon
Level:             Information                  Keywords:        Audit Failure
User:              N/A                          Computer:        DESKTOP-TJMT3F2
OpCode:            Info
More Information:  Event Log Online Help
```

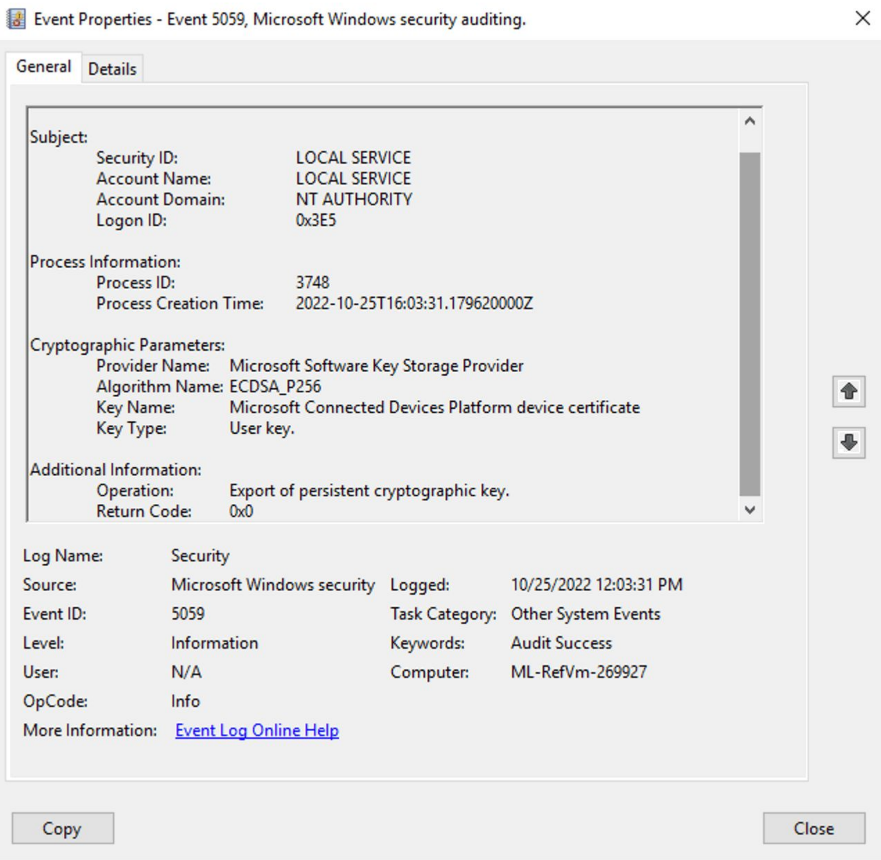
Key Migration Event 5059 - Devin

- Event 5059 generates when a cryptographic key is exported or imported using a Key Storage Provider. 5059 specifically only generates when the following Key Storage Providers are used:
  - Microsoft Software Key Storage Provider
  - Microsoft Smart



Security Number of events: 16,602 (!) New events available

Keywords	Date and Time	Source	Event ID	Task Category
Audit S...	10/25/2022 12:03:31 PM	Micros...	5059	Other System Events
Audit S...	8/19/2021 3:19:29 PM	Micros...	5059	Other System Events
Audit S...	11/10/2022 11:24:59 AM	Micros...	5059	Other System Events
Audit S...	11/10/2022 11:24:59 AM	Micros...	5059	Other System Events
Audit S...	10/27/2022 11:34:47 AM	Micros...	5059	Other System Events
Audit S...	11/10/2022 11:24:59 AM	Micros...	5059	Other System Events
Audit S...	10/27/2022 11:34:47 AM	Micros...	5059	Other System Events
Audit S...	11/10/2022 11:24:59 AM	Micros...	5059	Other System Events



Event Properties - Event 5059, Microsoft Windows security auditing.

Subject:
Security ID: LOCAL SERVICE
Account Name: LOCAL SERVICE
Account Domain: NT AUTHORITY
Logon ID: 0x3E5

Process Information:
Process ID: 3748
Process Creation Time: 2022-10-25T16:03:31.179620000Z

Cryptographic Parameters:
Provider Name: Microsoft Software Key Storage Provider
Algorithm Name: ECDSA_P256
Key Name: Microsoft Connected Devices Platform device certificate
Key Type: User key.

Additional Information:
Operation: Export of persistent cryptographic key.
Return Code: 0x0

Log Name: Security
Source: Microsoft Windows security
Logged: 10/25/2022 12:03:31 PM
Event ID: 5059
Task Category: Other System Events
Level: Information
Keywords: Audit Success
User: N/A
Computer: ML-RefVm-269927
OpCode: Info
More Information: Event Log Online Help

- Some interesting information:
  - PID
  - Creation Time
  - Provider Name

Temple University