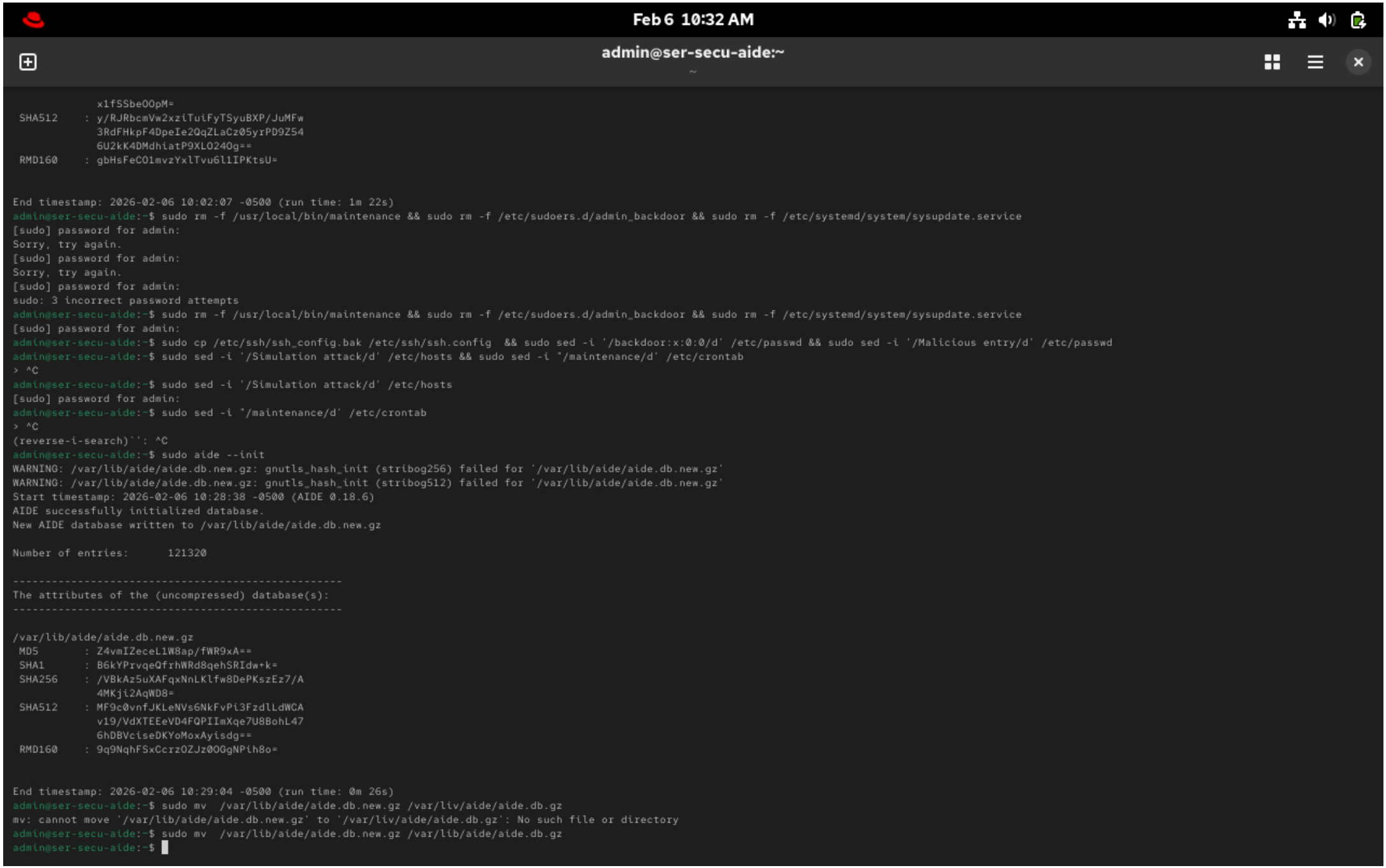
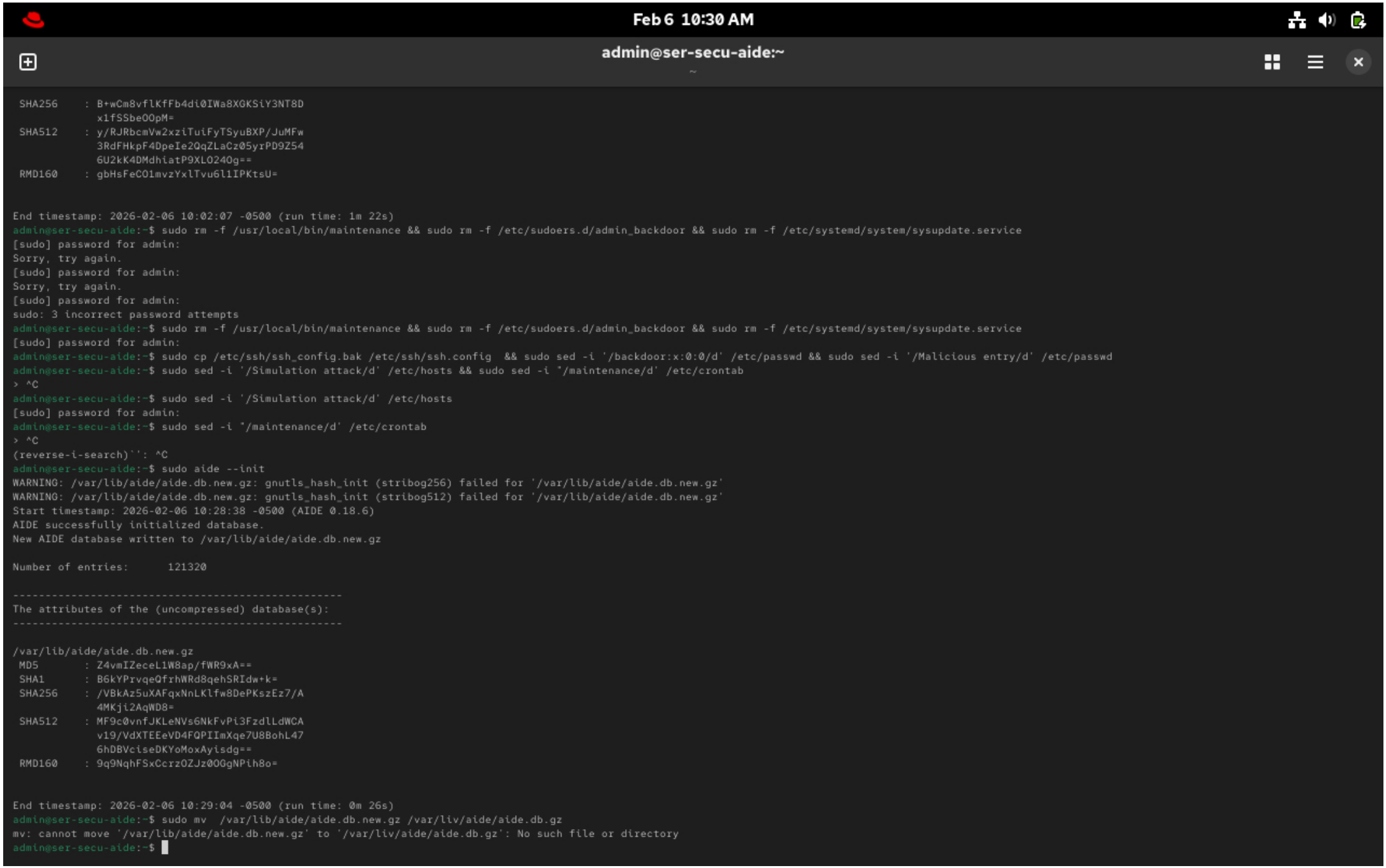
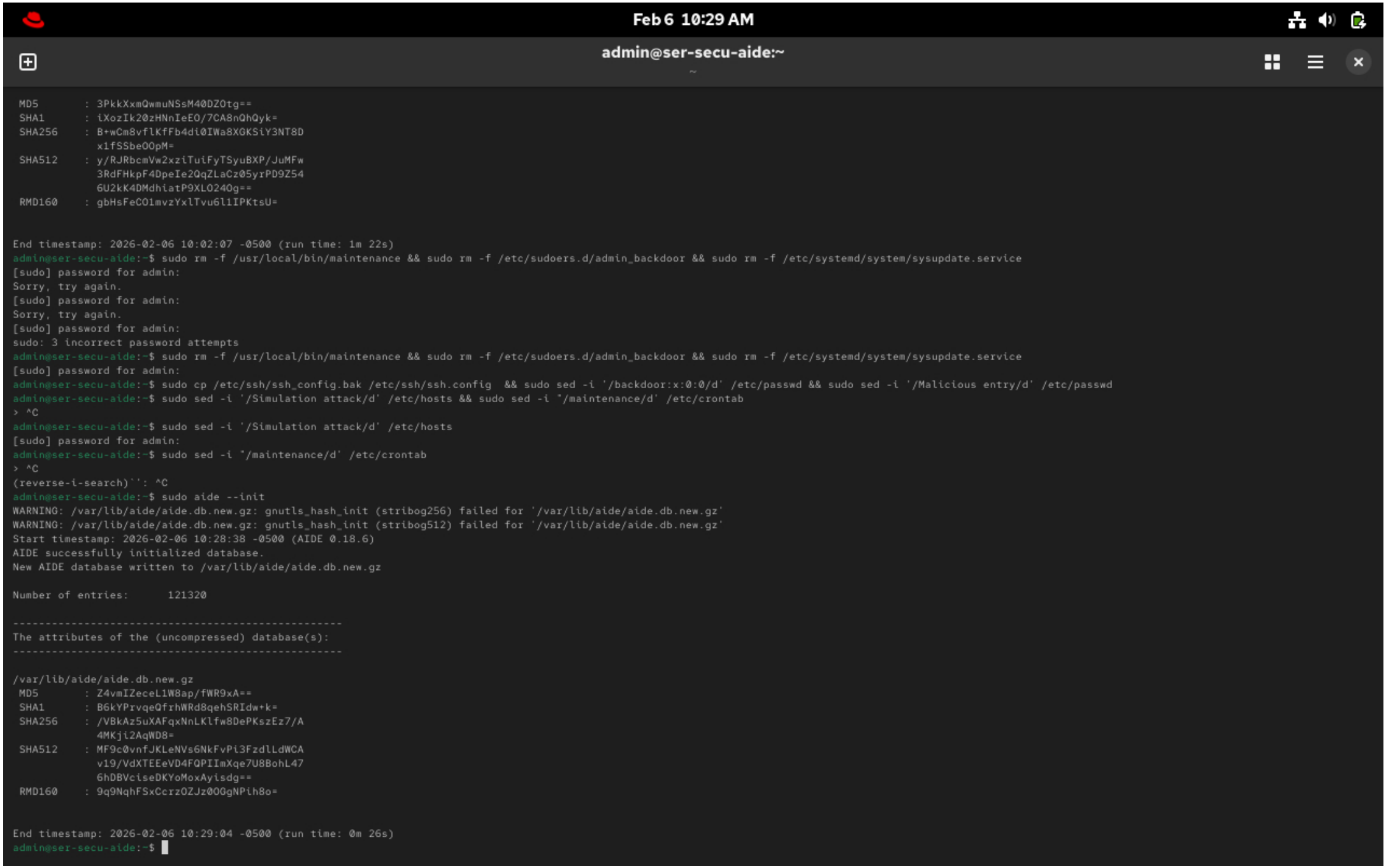
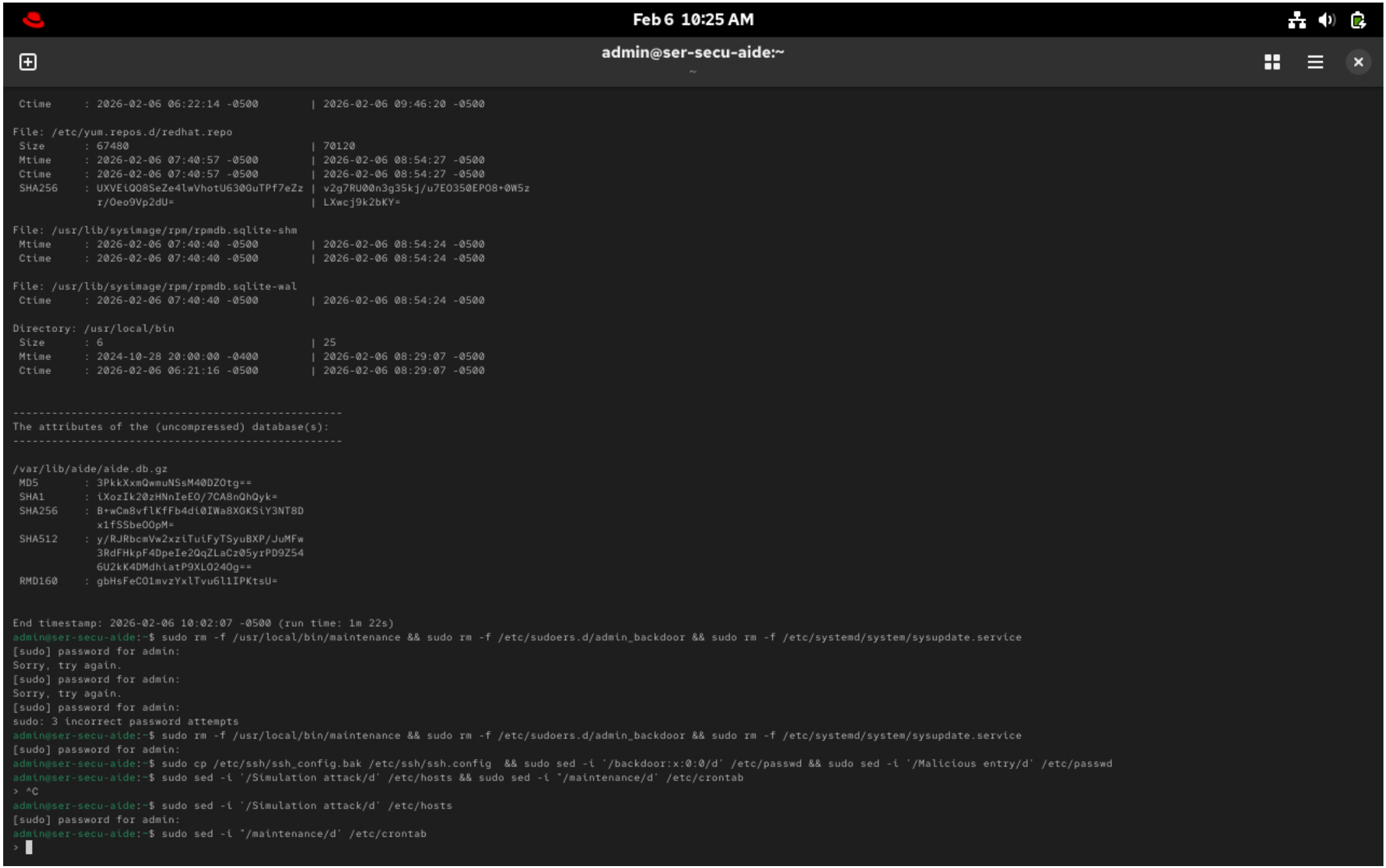

Feb 6 10:32 AM
admin@ser-secu-aide:~
~
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO240g==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 10:02:07 -0500 (run time: 1m 22s)
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
sudo: 3 incorrect password attempts
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config.bak /etc/ssh/ssh.config && sudo sed -i '/backdoor:x:0:0/d' /etc/passwd && sudo sed -i '/Malicious entry/d' /etc/passwd
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts && sudo sed -i "/maintenance/d' /etc/crontab
> ^C
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo sed -i "/maintenance/d' /etc/crontab
> ^C
(reverse-i-search)'': ^C
admin@ser-secu-aide:~$ sudo aide --init
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 10:28:38 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121320
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : Z4vmIZeceL1W8ap/fWR9xA==
SHA1 : B6kYPrvqeQfrhWRd8qehSRIdw+k=
SHA256 : /VBkAz5uXAFqxNnLKlfw8DePKszEz7/A
4MKji2AqWD8=
SHA512 : MF9c0vnfJKLeNVs6NkFvPi3FzdlLdWCA
v19/VdXTEEeVD4FQPIImXqe7U8BohL47
6hDBVciseDKYoMoxAyisdg==
RMD160 : 9q9NqhFSxCcrzOZJz0OGgNPih8o=
End timestamp: 2026-02-06 10:29:04 -0500 (run time: 0m 26s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/liv/aide/aide.db.gz
mv: cannot move '/var/lib/aide/aide.db.new.gz' to '/var/liv/aide/aide.db.gz': No such file or directory
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
admin@ser-secu-aide:~$

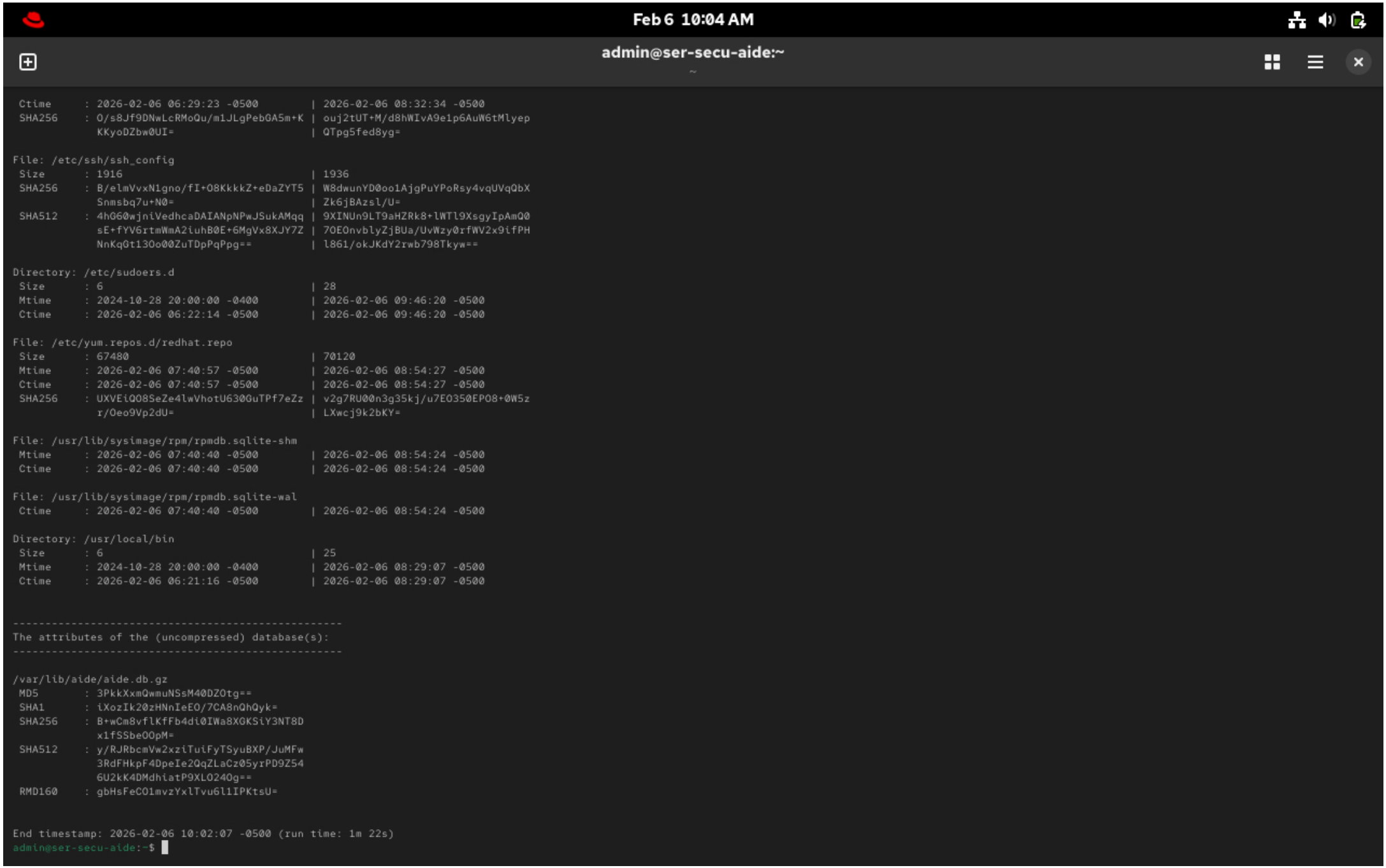

Feb 6 10:30 AM
admin@ser-secu-aide:~
~
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1f5SbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 10:02:07 -0500 (run time: 1m 22s)
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
sudo: 3 incorrect password attempts
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config.bak /etc/ssh/ssh.config && sudo sed -i '/backdoor:x:0:0/d' /etc/passwd && sudo sed -i '/Malicious entry/d' /etc/passwd
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts && sudo sed -i "/maintenance/d' /etc/crontab
> ^C
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo sed -i "/maintenance/d' /etc/crontab
> ^C
(reverse-i-search)'': ^C
admin@ser-secu-aide:~$ sudo aide --init
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 10:28:38 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121320

The attributes of the (uncompressed) database(s):

/var/lib/aide/aide.db.new.gz
MD5 : Z4vmIZeceL1W8ap/fWR9xA==
SHA1 : B6kYPrvqeQfrhWRd8qehSRIdw+k=
SHA256 : /VBkAz5uXAFqxNnLKlfw8DePKszEz7/A
4MKji2AqWD8=
SHA512 : MF9c0vnfJKLeNVs6NkFvPi3FzdlLdWCA
v19/VdXTEEeVD4FQPIImXqe7U8BohL47
6hDBVciseDKYoMoxAyisdg==
RMD160 : 9q9NqhFSxCcrzOZJz0OGgNPih8o=
End timestamp: 2026-02-06 10:29:04 -0500 (run time: 0m 26s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/liv/aide/aide.db.gz
mv: cannot move '/var/lib/aide/aide.db.new.gz' to '/var/liv/aide/aide.db.gz': No such file or directory
admin@ser-secu-aide:~$

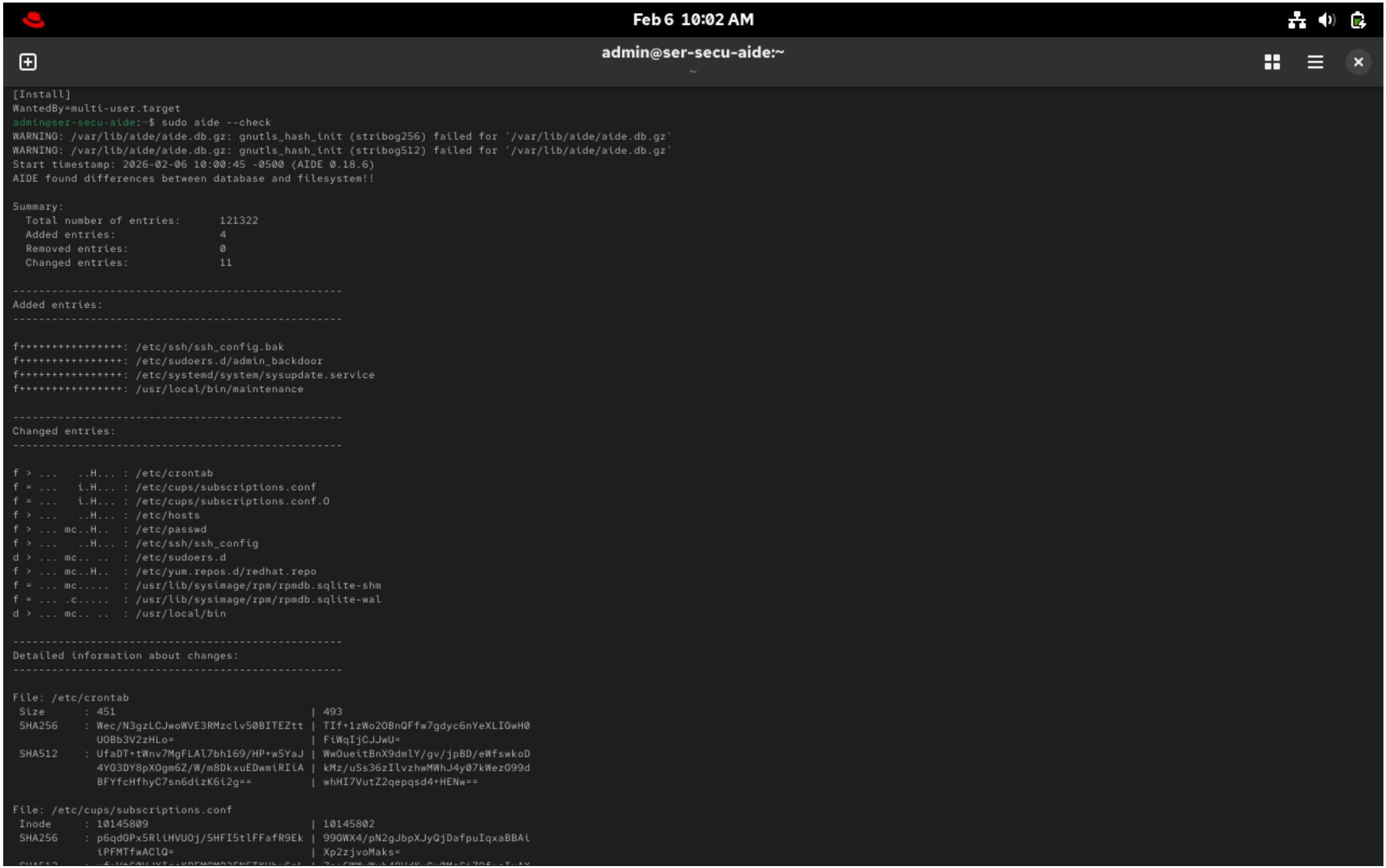

Feb 6 10:29 AM
admin@ser-secu-aide:~
~
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fS5beOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 10:02:07 -0500 (run time: 1m 22s)
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
sudo: 3 incorrect password attempts
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config.bak /etc/ssh/ssh.config && sudo sed -i '/backdoor:x:0:0/d' /etc/passwd && sudo sed -i '/Malicious entry/d' /etc/passwd
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts && sudo sed -i "/maintenance/d' /etc/crontab
> ^C
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo sed -i "/maintenance/d' /etc/crontab
> ^C
(reverse-i-search)'': ^C
admin@ser-secu-aide:~$ sudo aide --init
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 10:28:38 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121320
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : Z4vmIZeceL1W8ap/fWR9xA==
SHA1 : B6kYPrvqeQfrhWRd8qehSRIdw+k=
SHA256 : /VBkAz5uXAFqxNnLKlfw8DePKszEz7/A
4MKji2AqWD8=
SHA512 : MF9c0vnfJKLeNVs6NkFvPi3FzdlLdWCA
v19/VdXTEEeVD4FQPIImXqe7U8BohL47
6hDBVciseDKYoMoxAyisdg==
RMD160 : 9q9NqhFSxCcrzOZJz0OGgNPih8o=
End timestamp: 2026-02-06 10:29:04 -0500 (run time: 0m 26s)
admin@ser-secu-aide:~$

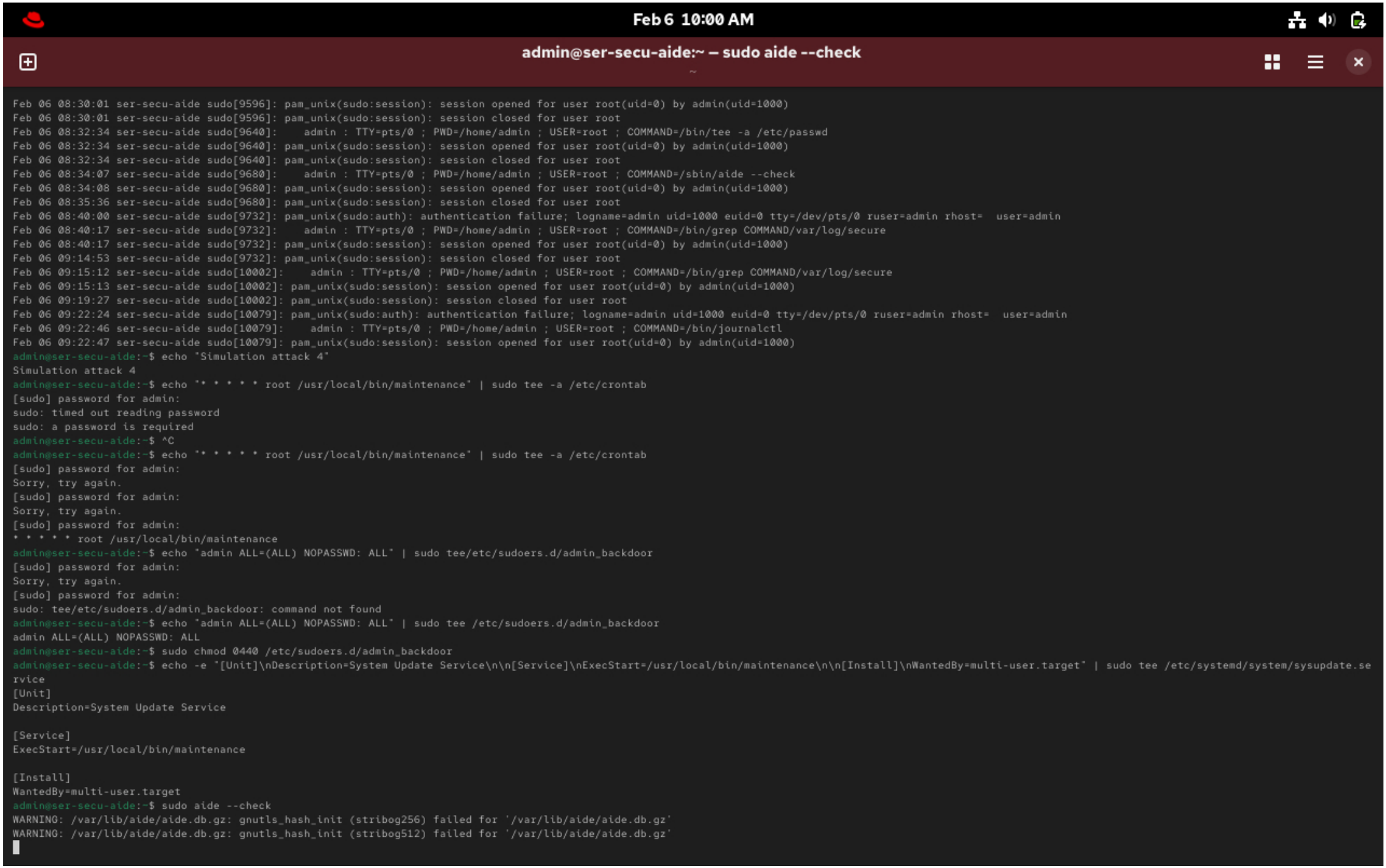

Feb 6 10:25 AM
admin@ser-secu-aide:~
~
Ctime : 2026-02-06 06:22:14 -0500 | 2026-02-06 09:46:20 -0500
File: /etc/yum.repos.d/redhat.repo
Size : 67480 | 70120
Mtime : 2026-02-06 07:40:57 -0500 | 2026-02-06 08:54:27 -0500
Ctime : 2026-02-06 07:40:57 -0500 | 2026-02-06 08:54:27 -0500
SHA256 : UXVEiQO8SeZe4lwVhotU630GuTPf7eZz | v2g7RU00n3g35kj/u7EO350EPO8+0W5z
r/Oeo9Vp2dU= | LXwcj9k2bKY=
File: /usr/lib/sysimage/rpm/rpmdb.sqlite-shm
Mtime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
Ctime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
File: /usr/lib/sysimage/rpm/rpmdb.sqlite-wal
Ctime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
Directory: /usr/local/bin
Size : 6 | 25
Mtime : 2024-10-28 20:00:00 -0400 | 2026-02-06 08:29:07 -0500
Ctime : 2026-02-06 06:21:16 -0500 | 2026-02-06 08:29:07 -0500
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 10:02:07 -0500 (run time: 1m 22s)
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
sudo: 3 incorrect password attempts
admin@ser-secu-aide:~$ sudo rm -f /usr/local/bin/maintenance && sudo rm -f /etc/sudoers.d/admin_backdoor && sudo rm -f /etc/systemd/system/sysupdate.service
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config.bak /etc/ssh/ssh.config && sudo sed -i '/backdoor:x:0:0/d' /etc/passwd && sudo sed -i '/Malicious entry/d' /etc/passwd
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts && sudo sed -i "/maintenance/d' /etc/crontab
> ^C
admin@ser-secu-aide:~$ sudo sed -i '/Simulation attack/d' /etc/hosts
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo sed -i "/maintenance/d' /etc/crontab
>

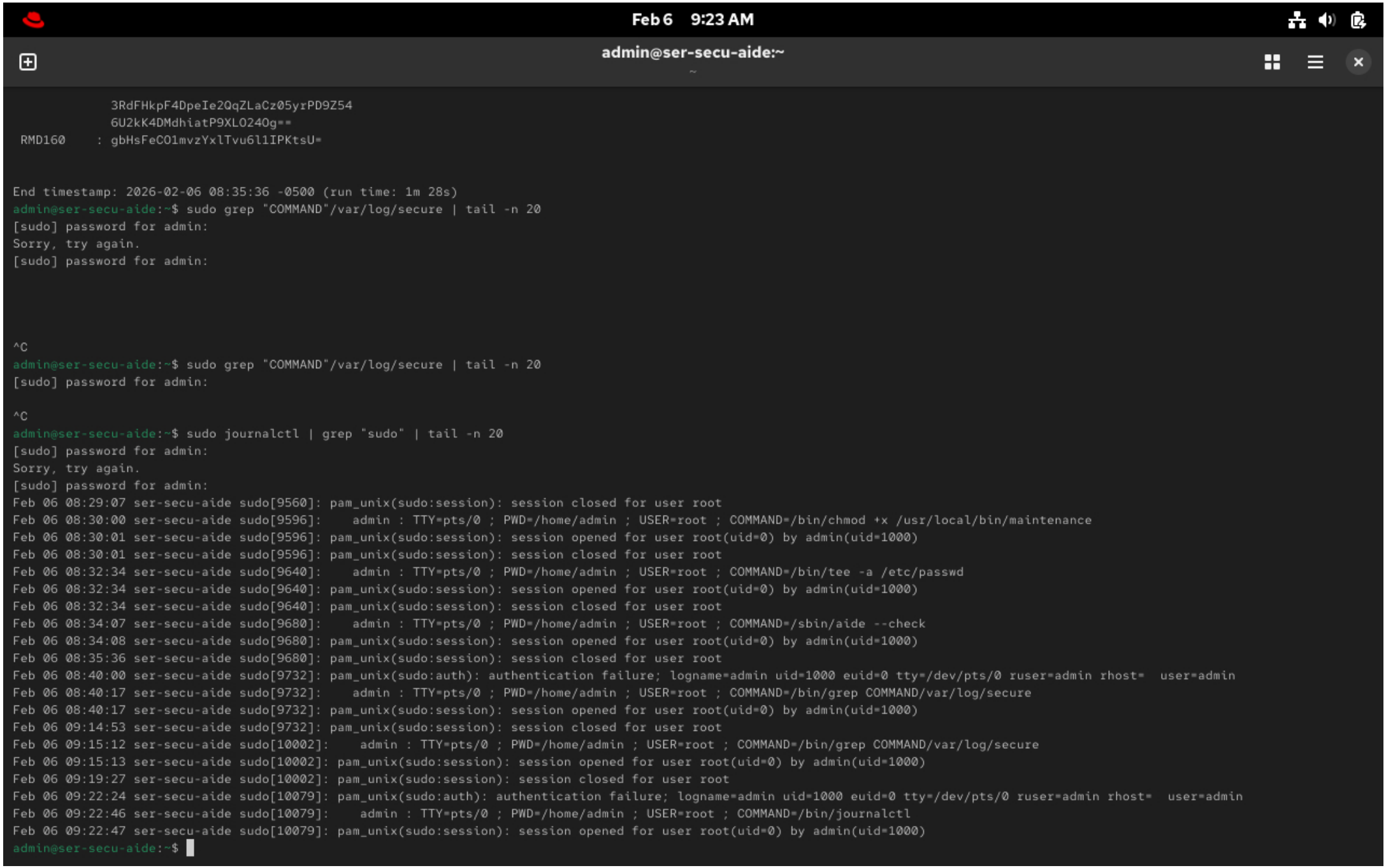

Feb 6 10:04 AM
admin@ser-secu-aide:~
~
Ctime : 2026-02-06 06:29:23 -0500 | 2026-02-06 08:32:34 -0500
SHA256 : O/s8Jf9DNwLcRMoQu/m1JLgPebGA5m+K | ouj2tUT+M/d8hWIvA9e1p6AuW6tMlyep
KKyoDZbw0UI= | QTpg5fed8yg=
File: /etc/ssh/ssh_config
Size : 1916 | 1936
SHA256 : B/elmVvxN1gno/fI+O8KkkkZ+eDaZYT5 | W8dwunYD0oo1AjgPuYPoRsy4vqUVqQbX
Snmsbq7u+N0= | Zk6jBAzsl/U=
SHA512 : 4hG60wjniVedhcaDAIANpNPwJSukAMqq | 9XINUn9LT9aHZRk8+lWTl9XsgyIpAmQ0
sE+fYV6rtmWmA2iuhB0E+6MgVx8XJY7Z | 7OEOnvblyZjBUa/UvWzy0rfWV2x9ifPH
NnKqGt13Oo00ZuTDpPqPpg== | l861/okJKdY2rwb798Tkyw==
Directory: /etc/sudoers.d
Size : 6 | 28
Mtime : 2024-10-28 20:00:00 -0400 | 2026-02-06 09:46:20 -0500
Ctime : 2026-02-06 06:22:14 -0500 | 2026-02-06 09:46:20 -0500
File: /etc/yum.repos.d/redhat.repo
Size : 67480 | 70120
Mtime : 2026-02-06 07:40:57 -0500 | 2026-02-06 08:54:27 -0500
Ctime : 2026-02-06 07:40:57 -0500 | 2026-02-06 08:54:27 -0500
SHA256 : UXVEiQO8SeZe4lwVhotU630GuTPf7eZz | v2g7RU00n3g35kj/u7EO350EPO8+0W5z
r/Oeo9Vp2dU= | LXwcj9k2bKY=
File: /usr/lib/sysimage/rpm/rpmdb.sqlite-shm
Mtime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
Ctime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
File: /usr/lib/sysimage/rpm/rpmdb.sqlite-wal
Ctime : 2026-02-06 07:40:40 -0500 | 2026-02-06 08:54:24 -0500
Directory: /usr/local/bin
Size : 6 | 25
Mtime : 2024-10-28 20:00:00 -0400 | 2026-02-06 08:29:07 -0500
Ctime : 2026-02-06 06:21:16 -0500 | 2026-02-06 08:29:07 -0500
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 10:02:07 -0500 (run time: 1m 22s)
admin@ser-secu-aide:~$

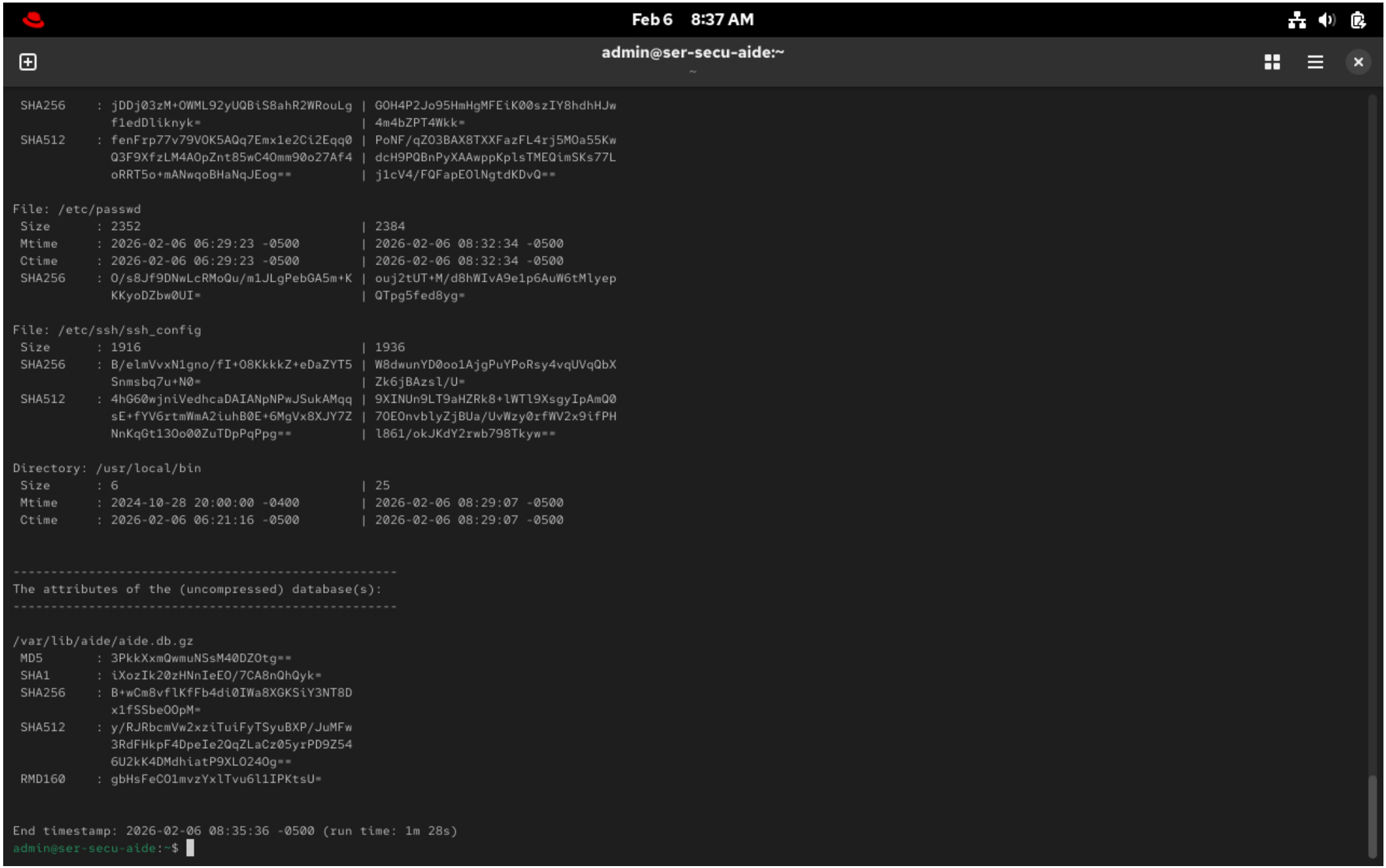
```
            f1edDliknyk=                      | 4m4bZPT4Wkk=
 SHA512     : fenFrp77v79VOK5AQq7Emx1e2Ci2Eqq0 | PoNF/qZO3BAX8TXXFazFL4rj5MOa55Kw
              Q3F9XfzLM4AOpZnt85wC4Omm90o27Af4 | dcH9PQBnPyXAAwppKplsTMEQimSKs77L
              oRRT5o+mANwqoBHaNqJEog==         | j1cV4/FQFapEOlNgtdKDvQ==

File: /etc/passwd
 Size       : 2352                            | 2384
 Mtime      : 2026-02-06 06:29:23 -0500       | 2026-02-06 08:32:34 -0500
 Ctime      : 2026-02-06 06:29:23 -0500       | 2026-02-06 08:32:34 -0500
 SHA256     : O/s8Jf9DNwLcRMoQu/m1JLgPebGA5m+K | ouj2tUT+M/d8hWIvA9e1p6AuW6tMlyep
              KKyoDZbw0UI=                    | QTpg5fed8yg=

File: /etc/ssh/ssh_config
 Size       : 1916                            | 1936
 SHA256     : B/elmVvxN1gno/fI+O8KkkkZ+eDaZYT5 | W8dwunYD0oo1AjgPuYPoRsy4vqUVqQbX
              Snmsbq7u+N0=                    | Zk6jBAzsl/U=
 SHA512     : 4hG60wjniVedhcaDAIANpNPwJSukAMqq | 9XINUn9LT9aHZRk8+lWTl9XsgyIpAmQ0
              sE+fYV6rtmWmA2iuhB0E+6MgVx8XJY7Z | 7OEOnvblyZjBUa/UvWzy0rfWV2x9ifPH
              NnKqGt13Oo00ZuTDpPqPpg==         | l861/okJKdY2rwb798Tkyw==

Directory: /etc/sudoers.d
 Size       : 6                               | 28
 Mtime      : 2024-10-28 20:00:00 -0400       | 2026-02-06 09:46:20 -0500
 Ctime      : 2026-02-06 06:22:14 -0500       | 2026-02-06 09:46:20 -0500

File: /etc/yum.repos.d/redhat.repo
 Size       : 67480                           | 70120
 Mtime      : 2026-02-06 07:40:57 -0500       | 2026-02-06 08:54:27 -0500
 Ctime      : 2026-02-06 07:40:57 -0500       | 2026-02-06 08:54:27 -0500
 SHA256     : UXVEiQO8SeZe4lwVhotU630GuTPf7eZz | v2g7RU00n3g35kj/u7EO350EPO8+0W5z
              r/Oeo9Vp2dU=                    | LXwcj9k2bKY=

File: /usr/lib/sysimage/rpm/rpmdb.sqlite-shm
 Mtime      : 2026-02-06 07:40:40 -0500       | 2026-02-06 08:54:24 -0500
 Ctime      : 2026-02-06 07:40:40 -0500       | 2026-02-06 08:54:24 -0500

File: /usr/lib/sysimage/rpm/rpmdb.sqlite-wal
 Ctime      : 2026-02-06 07:40:40 -0500       | 2026-02-06 08:54:24 -0500

Directory: /usr/local/bin
 Size       : 6                               | 25
 Mtime      : 2024-10-28 20:00:00 -0400       | 2026-02-06 08:29:07 -0500
 Ctime      : 2026-02-06 06:21:16 -0500       | 2026-02-06 08:29:07 -0500


---------------------------------------------------
The attributes of the (uncompressed) database(s):
---------------------------------------------------

/var/lib/aide/aide.db.gz
 MD5        : 3PkkXxmQwmuNSsM40DZOtg==
 SHA1       : iXozIk20zHNnIeEO/7CA8nQhQyk=
 SHA256     : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
              x1fSSbeOOpM=
 SHA512     : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
```

```
d > ... mc.. ..  : /usr/local/bin

-------------------------------------------------
Detailed information about changes:
-------------------------------------------------

File: /etc/crontab
 Size      : 451                           | 493
 SHA256    : Wec/N3gzLCJwoNVE3RMzclv50BITEZtt | TIf+1zWo2OBnQFfw7gdyc6nYeXLIGwH0
             UOBb3V2zHLo=                  | FiWqIjCJJwU=
 SHA512    : UfaDT+tWnv7MgFLAl7bh169/HP+w5YaJ | WwOueitBnX9dmlY/gv/jpBD/eWfswkoD
             4YG3DY8pXOgm6Z/W/m8DkxuEDwmiRIiA | kMz/uSs36zIlvzhwMWhJ4y07kWezG99d
             BFYfcHfhyC7sn6dizK6i2g==      | whHI7VutZ2qepqsd4+HENw==

File: /etc/cups/subscriptions.conf
 Inode     : 10145809                      | 10145802
 SHA256    : p6qdGPx5RliHVUOj/5HFI5tlFFafR9Ek | 99GWX4/pN2gJbpXJyQjDafpuIqxaBBAi
             iPFMTfwAClQ=                  | Xp2zjvoMaks=
 SHA512    : xfwVtS0VJXIqoKPEMGMQ3FN5TKHbwSgL | 7o+6WWuWxb48VdKvCw0MgSiZOf+eIuAX
             ytkFWi9JpYeRwIuWAxjAA7XO+tvp52zL | ahB8ce9nRvZwFaB0KNsk+uCukw8uARkV
             FyHtjIjXpvQ94rZFZL8KgA==      | PlEBbZnWpyr6yGNiwa5fXw==

File: /etc/cups/subscriptions.conf.O
 Inode     : 10145802                      | 10145798
 SHA256    : VTJuX7hCQ//sTIok5X2zIZWXihQIQstz | YvAx3C6l1tVvn8NE6UJNHZCnX8L8Qejs
             r17qk9B/RKs=                  | 99lC70KSV+c=
 SHA512    : 7/AkIOJBFqf3kaCo4dDRmNc1Hz8q4MJc | EpmXvckhG+mxtB2HBbM2QUyWSjWcpFUK
             cQifD9LnvYTt4txVeTIONFO5OxtnNOQN | NdPaONEzB7TtlW2sLeMs647hOt12y5tJ
             cgd+9HASwvN0pBhJegXDtg==      | BhbOD6vj6EH8qoIEYG649g==

File: /etc/hosts
 Size      : 384                           | 402
 SHA256    : jDDj03zM+OWML92yUQBiS8ahR2WRouLg | GOH4P2Jo95HmHgMFEiK00szIY8hdhHJw
             f1edDliknyk=                  | 4m4bZPT4Wkk=
 SHA512    : fenFrp77v79VOK5AQq7Emx1e2Ci2Eqq0 | PoNF/qZO3BAX8TXXFazFL4rj5MOa55Kw
             Q3F9XfzLM4AOpZnt85wC4Omm90o27Af4 | dcH9PQBnPyXAAwppKplsTMEQimSKs77L
             oRRT5o+mANwqoBHaNqJEog==      | j1cV4/FQFapEOlNgtdKDvQ==

File: /etc/passwd
 Size      : 2352                          | 2384
 Mtime     : 2026-02-06 06:29:23 -0500     | 2026-02-06 08:32:34 -0500
 Ctime     : 2026-02-06 06:29:23 -0500     | 2026-02-06 08:32:34 -0500
 SHA256    : O/s8Jf9DNwLcRMoQu/m1JLgPebGA5m+K | ouj2tUT+M/d8hWIvA9e1p6AuW6tMlyep
             KKyoDZbw0UI=                  | QTpg5fed8yg=

File: /etc/ssh/ssh_config
 Size      : 1916                          | 1936
 SHA256    : B/elmVvxN1gno/fI+O8KkkkZ+eDaZYT5 | W8dwunYD0oo1AjgPuYPoRsy4vqUVqQbX
             Snmsbq7u+N0=                  | Zk6jBAzsl/U=
 SHA512    : 4hG60wjniVedhcaDAIANpNPwJSukAMqq | 9XINUn9LT9aHZRk8+lWTl9XsgyIpAmQ0
             sE+fYV6rtmWmA2iuhB0E+6MgVx8XJY7Z | 7OEOnvblyZjBUa/UvWzy0rfWV2x9ifPH
             NnKqGt13Oo00ZuTDpPqPpg==      | l861/okJKdY2rwb798Tkyw==

Directory: /etc/sudoers.d
 Size      : 6                             | 28
```

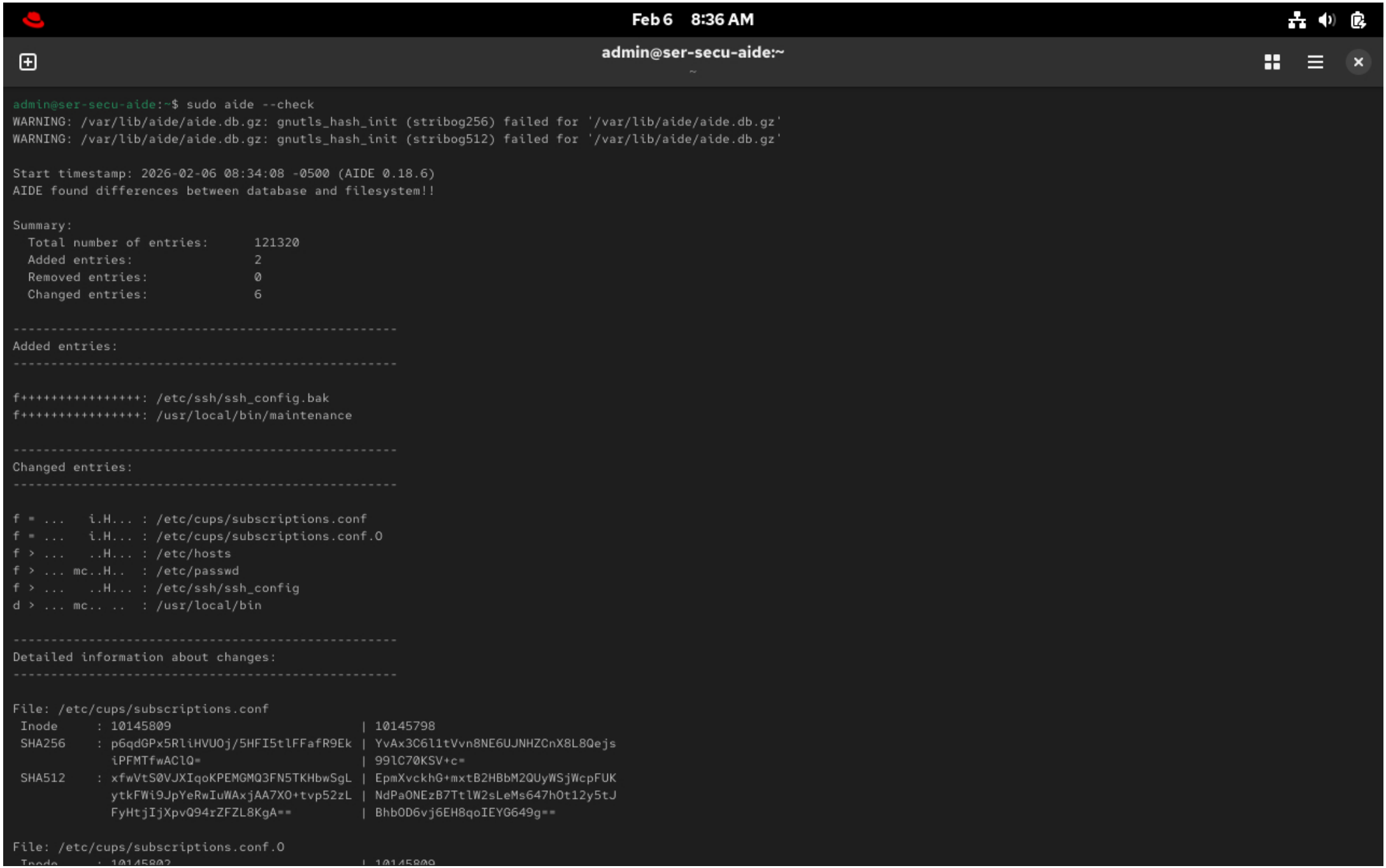

Feb 6 10:02 AM
admin@ser-secu-aide:~
[Install]
WantedBy=multi-user.target
admin@ser-secu-aide:~$ sudo aide --check
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.gz'
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.gz'
Start timestamp: 2026-02-06 10:00:45 -0500 (AIDE 0.18.6)
AIDE found differences between database and filesystem!!
Summary:
Total number of entries: 121322
Added entries: 4
Removed entries: 0
Changed entries: 11
Added entries:
f++++++++++++++++: /etc/ssh/ssh_config.bak
f++++++++++++++++: /etc/sudoers.d/admin_backdoor
f++++++++++++++++: /etc/systemd/system/sysupdate.service
f++++++++++++++++: /usr/local/bin/maintenance
Changed entries:
f > ... ..H... : /etc/crontab
f = ... i.H... : /etc/cups/subscriptions.conf
f = ... i.H... : /etc/cups/subscriptions.conf.O
f > ... ..H... : /etc/hosts
f > ... mc..H.. : /etc/passwd
f > ... ..H... : /etc/ssh/ssh_config
d > ... mc.. .. : /etc/sudoers.d
f > ... mc..H.. : /etc/yum.repos.d/redhat.repo
f = ... mc..... : /usr/lib/sysimage/rpm/rpmdb.sqlite-shm
f = ...c..... : /usr/lib/sysimage/rpm/rpmdb.sqlite-wal
d > ... mc.. .. : /usr/local/bin
Detailed information about changes:
File: /etc/crontab
Size : 451 | 493
SHA256 : Wec/N3gzLCJwoWVE3RMzclv50BITEZtt | TIf+1zWo2OBnQFfw7gdyc6nYeXLIGwH0
UOBb3V2zHLo= | FiWqIjCJJwU=
SHA512 : UfaDT+tWnv7MgFLAl7bh169/HP+w5YaJ | WwOueitBnX9dmlY/gv/jpBD/eWfswkoD
4YG3DY8pXOgm6Z/W/m8DkxuEDwmiRIiA | kMz/uSs36zIlvzhwMWhJ4y07kWezG99d
BFYfcHfhyC7sn6dizK6i2g== | whHI7VutZ2qepqsd4+HENw==
File: /etc/cups/subscriptions.conf
Inode : 10145809 | 10145802
SHA256 : p6qdGPx5RliHVUOj/5HFI5tlFFafR9Ek | 99GWX4/pN2gJbpXJyQjDafpuIqxaBBAi
iPFMTfwAClQ= | Xp2zjvoMaks=

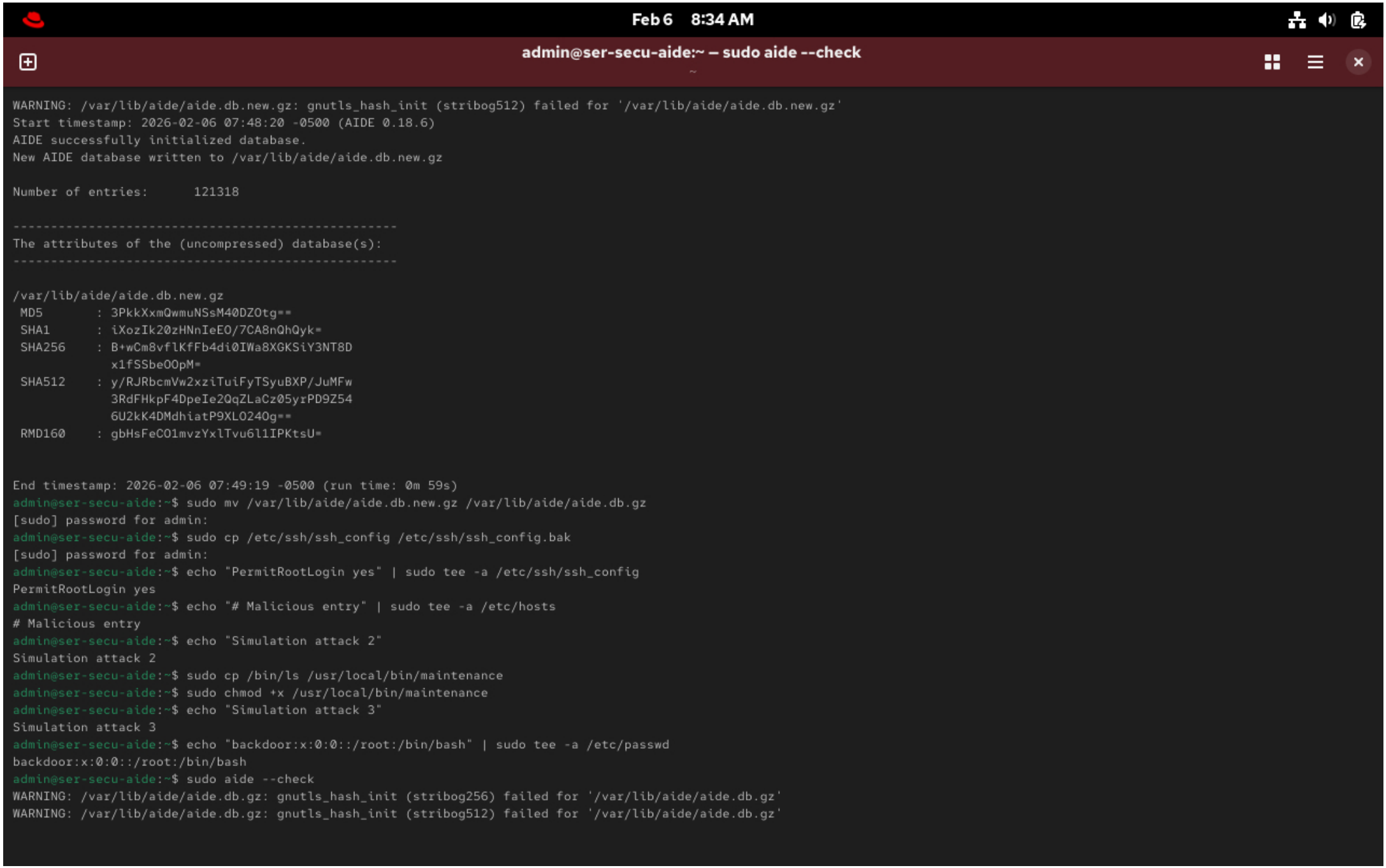

Feb 6 10:00 AM
admin@ser-secu-aide:~ — sudo aide --check
Feb 06 08:30:01 ser-secu-aide sudo[9596]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:30:01 ser-secu-aide sudo[9596]: pam_unix(sudo:session): session closed for user root
Feb 06 08:32:34 ser-secu-aide sudo[9640]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/tee -a /etc/passwd
Feb 06 08:32:34 ser-secu-aide sudo[9640]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:32:34 ser-secu-aide sudo[9640]: pam_unix(sudo:session): session closed for user root
Feb 06 08:34:07 ser-secu-aide sudo[9680]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/sbin/aide --check
Feb 06 08:34:08 ser-secu-aide sudo[9680]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:35:36 ser-secu-aide sudo[9680]: pam_unix(sudo:session): session closed for user root
Feb 06 08:40:00 ser-secu-aide sudo[9732]: pam_unix(sudo:auth): authentication failure; logname=admin uid=1000 euid=0 tty=/dev/pts/0 ruser=admin rhost= user=admin
Feb 06 08:40:17 ser-secu-aide sudo[9732]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/grep COMMAND/var/log/secure
Feb 06 08:40:17 ser-secu-aide sudo[9732]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 09:14:53 ser-secu-aide sudo[9732]: pam_unix(sudo:session): session closed for user root
Feb 06 09:15:12 ser-secu-aide sudo[10002]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/grep COMMAND/var/log/secure
Feb 06 09:15:13 ser-secu-aide sudo[10002]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 09:19:27 ser-secu-aide sudo[10002]: pam_unix(sudo:session): session closed for user root
Feb 06 09:22:24 ser-secu-aide sudo[10079]: pam_unix(sudo:auth): authentication failure; logname=admin uid=1000 euid=0 tty=/dev/pts/0 ruser=admin rhost= user=admin
Feb 06 09:22:46 ser-secu-aide sudo[10079]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/journalctl
Feb 06 09:22:47 ser-secu-aide sudo[10079]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
admin@ser-secu-aide:~$ echo "Simulation attack 4"
Simulation attack 4
admin@ser-secu-aide:~$ echo "* * * * * root /usr/local/bin/maintenance" | sudo tee -a /etc/crontab
[sudo] password for admin:
sudo: timed out reading password
sudo: a password is required
admin@ser-secu-aide:~$ ^C
admin@ser-secu-aide:~$ echo "* * * * * root /usr/local/bin/maintenance" | sudo tee -a /etc/crontab
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
* * * * * root /usr/local/bin/maintenance
admin@ser-secu-aide:~$ echo "admin ALL=(ALL) NOPASSWD: ALL" | sudo tee/etc/sudoers.d/admin_backdoor
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
sudo: tee/etc/sudoers.d/admin_backdoor: command not found
admin@ser-secu-aide:~$ echo "admin ALL=(ALL) NOPASSWD: ALL" | sudo tee /etc/sudoers.d/admin_backdoor
admin ALL=(ALL) NOPASSWD: ALL
admin@ser-secu-aide:~$ sudo chmod 0440 /etc/sudoers.d/admin_backdoor
admin@ser-secu-aide:~$ echo -e "[Unit]\nDescription=System Update Service\n\n[Service]\nExecStart=/usr/local/bin/maintenance\n\n[Install]\nWantedBy=multi-user.target" | sudo tee /etc/systemd/system/sysupdate.service
[Unit]
Description=System Update Service
[Service]
ExecStart=/usr/local/bin/maintenance
[Install]
WantedBy=multi-user.target
admin@ser-secu-aide:~$ sudo aide --check
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.gz'
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.gz'

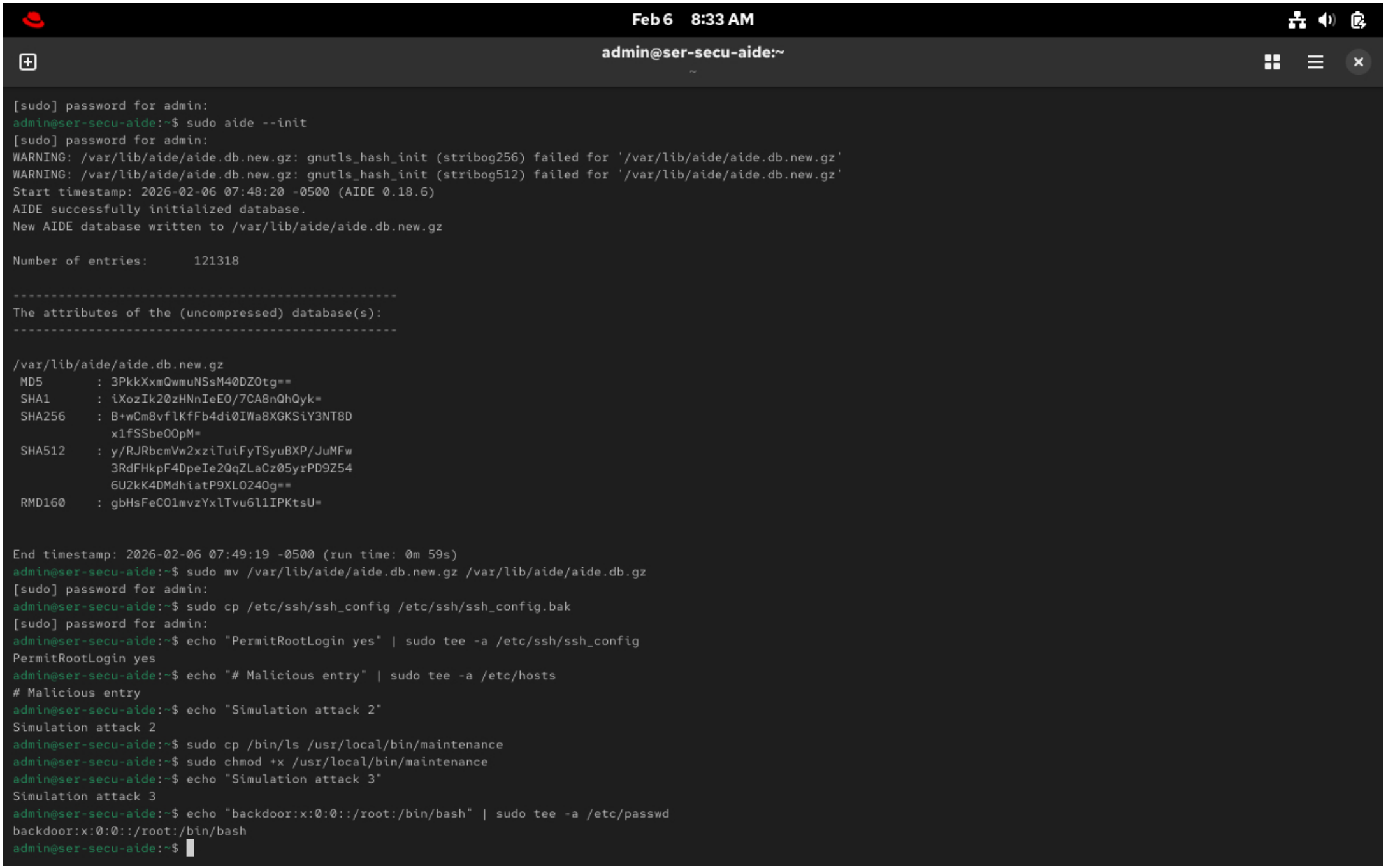

Feb 6 9:23 AM
admin@ser-secu-aide:~
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 08:35:36 -0500 (run time: 1m 28s)
admin@ser-secu-aide:~$ sudo grep "COMMAND"/var/log/secure | tail -n 20
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
^C
admin@ser-secu-aide:~$ sudo grep "COMMAND"/var/log/secure | tail -n 20
[sudo] password for admin:
^C
admin@ser-secu-aide:~$ sudo journalctl | grep "sudo" | tail -n 20
[sudo] password for admin:
Sorry, try again.
[sudo] password for admin:
Feb 06 08:29:07 ser-secu-aide sudo[9560]: pam_unix(sudo:session): session closed for user root
Feb 06 08:30:00 ser-secu-aide sudo[9596]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/chmod +x /usr/local/bin/maintenance
Feb 06 08:30:01 ser-secu-aide sudo[9596]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:30:01 ser-secu-aide sudo[9596]: pam_unix(sudo:session): session closed for user root
Feb 06 08:32:34 ser-secu-aide sudo[9640]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/tee -a /etc/passwd
Feb 06 08:32:34 ser-secu-aide sudo[9640]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:32:34 ser-secu-aide sudo[9640]: pam_unix(sudo:session): session closed for user root
Feb 06 08:34:07 ser-secu-aide sudo[9680]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/sbin/aide --check
Feb 06 08:34:08 ser-secu-aide sudo[9680]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 08:35:36 ser-secu-aide sudo[9680]: pam_unix(sudo:session): session closed for user root
Feb 06 08:40:00 ser-secu-aide sudo[9732]: pam_unix(sudo:auth): authentication failure; logname=admin uid=1000 euid=0 tty=/dev/pts/0 ruser=admin rhost= user=admin
Feb 06 08:40:17 ser-secu-aide sudo[9732]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/grep COMMAND/var/log/secure
Feb 06 08:40:17 ser-secu-aide sudo[9732]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 09:14:53 ser-secu-aide sudo[9732]: pam_unix(sudo:session): session closed for user root
Feb 06 09:15:12 ser-secu-aide sudo[10002]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/grep COMMAND/var/log/secure
Feb 06 09:15:13 ser-secu-aide sudo[10002]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
Feb 06 09:19:27 ser-secu-aide sudo[10002]: pam_unix(sudo:session): session closed for user root
Feb 06 09:22:24 ser-secu-aide sudo[10079]: pam_unix(sudo:auth): authentication failure; logname=admin uid=1000 euid=0 tty=/dev/pts/0 ruser=admin rhost= user=admin
Feb 06 09:22:46 ser-secu-aide sudo[10079]: admin : TTY=pts/0 ; PWD=/home/admin ; USER=root ; COMMAND=/bin/journalctl
Feb 06 09:22:47 ser-secu-aide sudo[10079]: pam_unix(sudo:session): session opened for user root(uid=0) by admin(uid=1000)
admin@ser-secu-aide:~$

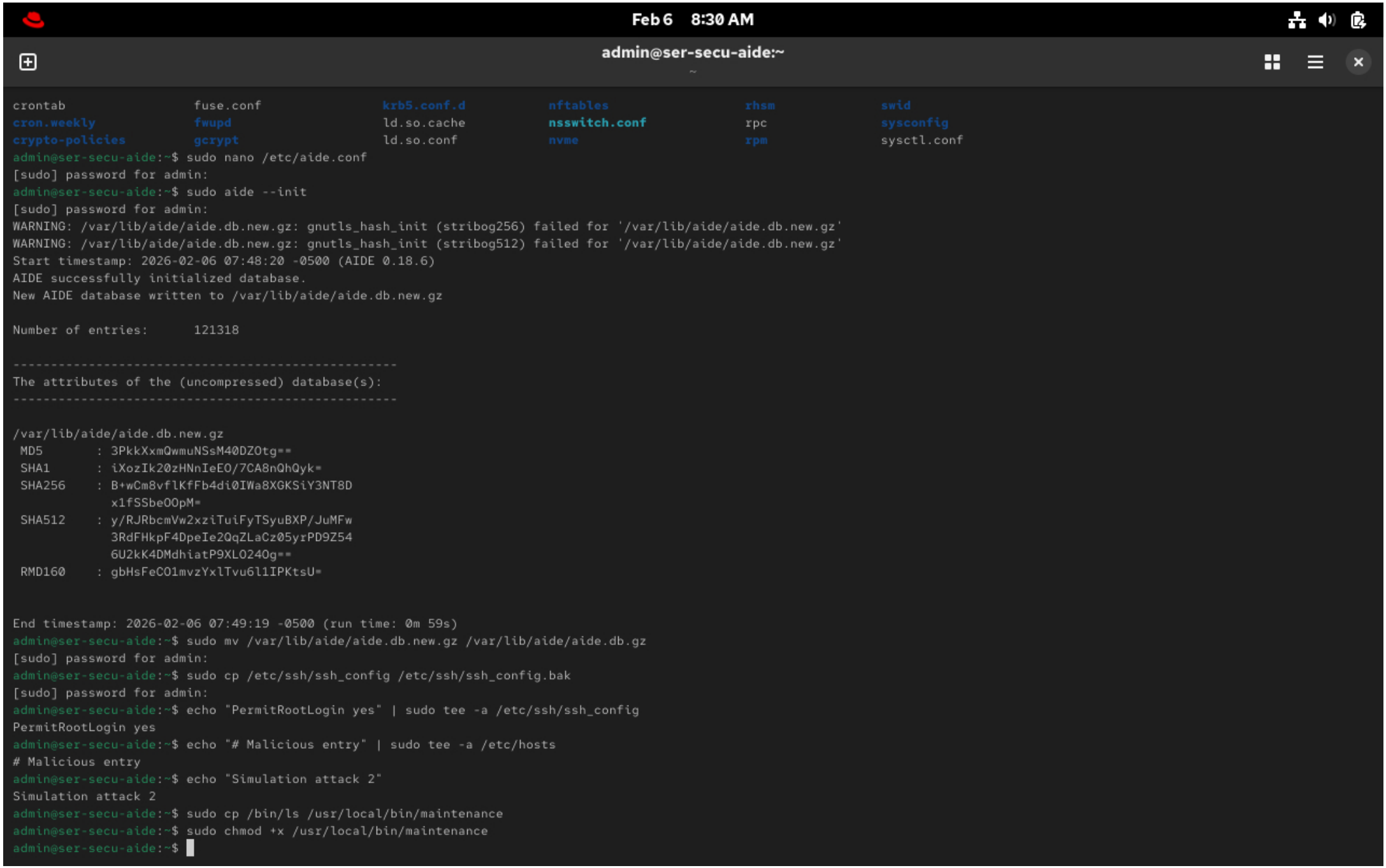

Feb 6 8:37 AM
admin@ser-secu-aide:~
SHA256 : jDDj03zM+OWML92yUQBiS8ahR2WRouLg | GOH4P2Jo95HmHgMFEiK00szIY8hdhHJw
f1edDliknyk= | 4m4bZPT4Wkk=
SHA512 : fenFrp77v79VOK5AQq7Emx1e2Ci2Eqq0 | PoNF/qZO3BAX8TXXFazFL4rj5MOa55Kw
Q3F9XfzLM4AOpZnt85wC4Omm90o27Af4 | dcH9PQBnPyXAAwppKplsTMEQimSKs77L
oRRT5o+mANwqoBHaNqJEog== | j1cV4/FQFapEOlNgtdKDvQ==
File: /etc/passwd
Size : 2352 | 2384
Mtime : 2026-02-06 06:29:23 -0500 | 2026-02-06 08:32:34 -0500
Ctime : 2026-02-06 06:29:23 -0500 | 2026-02-06 08:32:34 -0500
SHA256 : O/s8Jf9DNwLcRMoQu/m1JLgPebGA5m+K | ouj2tUT+M/d8hWIvA9e1p6AuW6tMlyep
KKyoDZbw0UI= | QTpg5fed8yg=
File: /etc/ssh/ssh_config
Size : 1916 | 1936
SHA256 : B/elmVvxN1gno/fI+O8KkkkZ+eDaZYT5 | W8dwunYD0oo1AjgPuYPoRsy4vqUVqQbX
Snmsbq7u+N0= | Zk6jBAzsl/U=
SHA512 : 4hG60wjniVedhcaDAIANpNPwJSukAMqq | 9XINUn9LT9aHZRk8+lWTl9XsgyIpAmQ0
sE+fYV6rtmWmA2iuhB0E+6MgVx8XJY7Z | 7OEOnvblyZjBUa/UvWzy0rfWV2x9ifPH
NnKqGt13Oo00ZuTDpPqPpg== | l861/okJKdY2rwb798Tkyw==
Directory: /usr/local/bin
Size : 6 | 25
Mtime : 2024-10-28 20:00:00 -0400 | 2026-02-06 08:29:07 -0500
Ctime : 2026-02-06 06:21:16 -0500 | 2026-02-06 08:29:07 -0500
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 08:35:36 -0500 (run time: 1m 28s)
admin@ser-secu-aide:~$

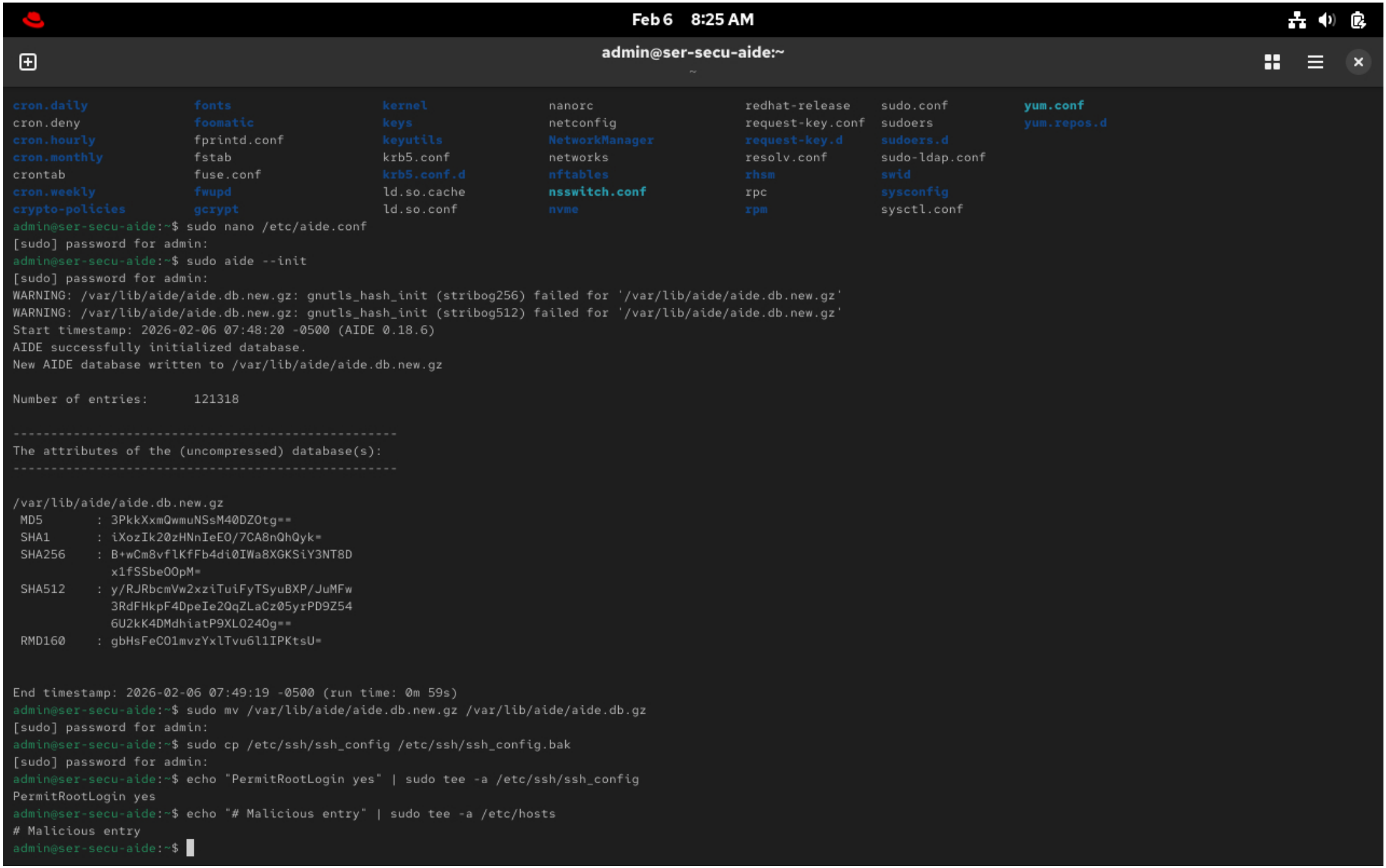
```
---------------------------------------------
Detailed information about changes:
---------------------------------------------

File: /etc/cups/subscriptions.conf
 Inode     : 10145809                        | 10145798
 SHA256    : p6qdGPx5RliHVUOj/5HFI5tlFFafR9Ek | YvAx3C6l1tVvn8NE6UJNHZCnX8L8Qejs
             iPFMTfwAClQ=                     | 99lC70KSV+c=
 SHA512    : xfwVtS0VJXIqoKPEMGMQ3FN5TKHbwSgL | EpmXvckhG+mxtB2HBbM2QUyWSjWcpFUK
             ytkFWi9JpYeRwIuWAxjAA7XO+tvp52zL | NdPaONEzB7TtlW2sLeMs647hOt12y5tJ
             FyHtjIjXpvQ94rZFZL8KgA==         | BhbOD6vj6EH8qoIEYG649g==

File: /etc/cups/subscriptions.conf.O
 Inode     : 10145802                        | 10145809
 SHA256    : VTJuX7hCQ//sTIok5X2zIZWXihQIQstz | p6qdGPx5RliHVUOj/5HFI5tlFFafR9Ek
             r17qk9B/RKs=                     | iPFMTfwAClQ=
 SHA512    : 7/AkIOJBFqf3kaCo4dDRmNc1Hz8q4MJc | xfwVtS0VJXIqoKPEMGMQ3FN5TKHbwSgL
             cQifD9LnvYTt4txVeTIONFO5OxtnNOQN | ytkFWi9JpYeRwIuWAxjAA7XO+tvp52zL
             cgd+9HASwvN0pBhJegXDtg==         | FyHtjIjXpvQ94rZFZL8KgA==

File: /etc/hosts
 Size      : 384                             | 402
 SHA256    : jDDj03zM+OWML92yUQBiS8ahR2WRouLg | GOH4P2Jo95HmHgMFEiK00szIY8hdhHJw
             f1edDliknyk=                     | 4m4bZPT4Wkk=
 SHA512    : fenFrp77v79VOK5AQq7Emx1e2Ci2Eqq0 | PoNF/qZO3BAX8TXXFazFL4rj5MOa55Kw
             Q3F9XfzLM4AOpZnt85wC4Omm90o27Af4 | dcH9PQBnPyXAAwppKplsTMEQimSKs77L
             oRRT5o+mANwqoBHaNqJEog==         | j1cV4/FQFapEOlNgtdKDvQ==

File: /etc/passwd
 Size      : 2352                            | 2384
 Mtime     : 2026-02-06 06:29:23 -0500       | 2026-02-06 08:32:34 -0500
 Ctime     : 2026-02-06 06:29:23 -0500       | 2026-02-06 08:32:34 -0500
 SHA256    : O/s8Jf9DNwLcRMoQu/m1JLgPebGA5m+K | ouj2tUT+M/d8hWIvA9e1p6AuW6tMlyep
             KKyoDZbw0UI=                     | QTpg5fed8yg=

File: /etc/ssh/ssh_config
 Size      : 1916                            | 1936
 SHA256    : B/elmVvxN1gno/fI+O8KkkkZ+eDaZYT5 | W8dwunYD0oo1AjgPuYPoRsy4vqUVqQbX
             Snmsbq7u+N0=                     | Zk6jBAzsl/U=
 SHA512    : 4hG60wjniVedhcaDAIANpNPwJSukAMqq | 9XINUn9LT9aHZRk8+lWTl9XsgyIpAmQ0
             sE+fYV6rtmWmA2iuhB0E+6MgVx8XJY7Z | 7OEOnvblyZjBUa/UvWzy0rfWV2x9ifPH
             NnKqGt13Oo00ZuTDpPqPpg==         | l861/okJKdY2rwb798Tkyw==

Directory: /usr/local/bin
 Size      : 6                               | 25
```

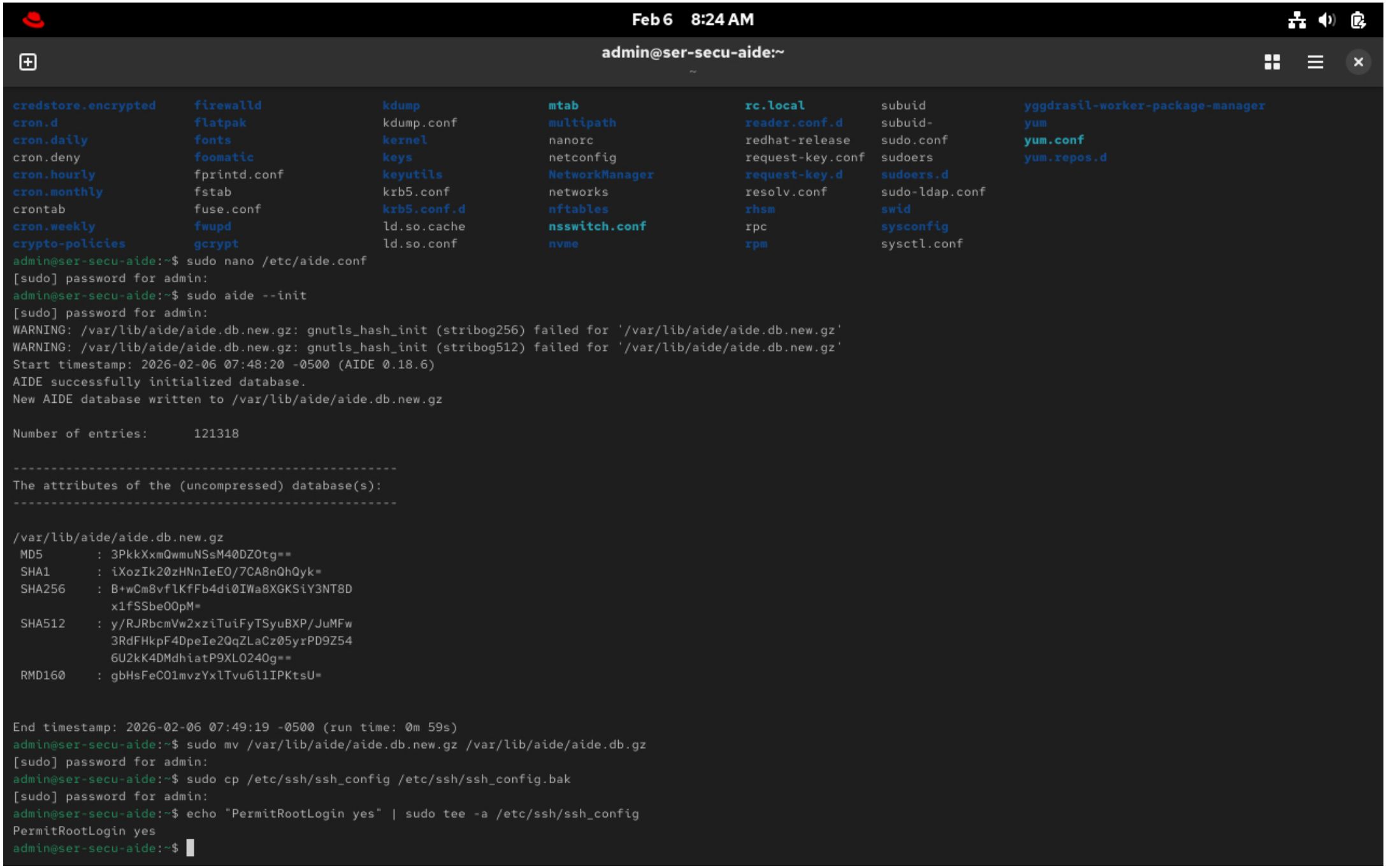

Feb 6 8:36 AM
admin@ser-secu-aide:~
admin@ser-secu-aide:~$ sudo aide --check
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.gz'
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.gz'
Start timestamp: 2026-02-06 08:34:08 -0500 (AIDE 0.18.6)
AIDE found differences between database and filesystem!!
Summary:
Total number of entries: 121320
Added entries: 2
Removed entries: 0
Changed entries: 6
Added entries:
f++++++++++++++++: /etc/ssh/ssh_config.bak
f++++++++++++++++: /usr/local/bin/maintenance
Changed entries:
f = ... i.H... : /etc/cups/subscriptions.conf
f = ... i.H... : /etc/cups/subscriptions.conf.O
f > ... ..H... : /etc/hosts
f > ... mc..H.. : /etc/passwd
f > ... ..H... : /etc/ssh/ssh_config
d > ... mc.. .. : /usr/local/bin
Detailed information about changes:
File: /etc/cups/subscriptions.conf
Inode : 10145809 | 10145798
SHA256 : p6qdGPx5RliHVUOj/5HFI5tlFFafR9Ek | YvAx3C6l1tVvn8NE6UJNHZCnX8L8Qejs
iPFMTfwAClQ= | 99lC70KSV+c=
SHA512 : xfwVtS0VJXIqoKPEMGMQ3FN5TKHbwSgL | EpmXvckhG+mxtB2HBbM2QUyWSjWcpFUK
ytkFWi9JpYeRwIuWAxjAA7XO+tvp52zL | NdPaONEzB7TtlW2sLeMs647hOt12y5tJ
FyHtjIjXpvQ94rZFZL8KgA== | BhbOD6vj6EH8qoIEYG649g==
File: /etc/cups/subscriptions.conf.O


Feb 6 8:34 AM
admin@ser-secu-aide:~ — sudo aide --check
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$ echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/ssh_config
PermitRootLogin yes
admin@ser-secu-aide:~$ echo "# Malicious entry" | sudo tee -a /etc/hosts
Malicious entry
admin@ser-secu-aide:~$ echo "Simulation attack 2"
Simulation attack 2
admin@ser-secu-aide:~$ sudo cp /bin/ls /usr/local/bin/maintenance
admin@ser-secu-aide:~$ sudo chmod +x /usr/local/bin/maintenance
admin@ser-secu-aide:~$ echo "Simulation attack 3"
Simulation attack 3
admin@ser-secu-aide:~$ echo "backdoor:x:0:0::/root:/bin/bash" | sudo tee -a /etc/passwd
backdoor:x:0:0::/root:/bin/bash
admin@ser-secu-aide:~$ sudo aide --check
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.gz'
WARNING: /var/lib/aide/aide.db.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.gz'


Feb 6 8:33 AM
admin@ser-secu-aide:~
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$ echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/ssh_config
PermitRootLogin yes
admin@ser-secu-aide:~$ echo "# Malicious entry" | sudo tee -a /etc/hosts
Malicious entry
admin@ser-secu-aide:~$ echo "Simulation attack 2"
Simulation attack 2
admin@ser-secu-aide:~$ sudo cp /bin/ls /usr/local/bin/maintenance
admin@ser-secu-aide:~$ sudo chmod +x /usr/local/bin/maintenance
admin@ser-secu-aide:~$ echo "Simulation attack 3"
Simulation attack 3
admin@ser-secu-aide:~$ echo "backdoor:x:0:0::/root:/bin/bash" | sudo tee -a /etc/passwd
backdoor:x:0:0::/root:/bin/bash
admin@ser-secu-aide:~$

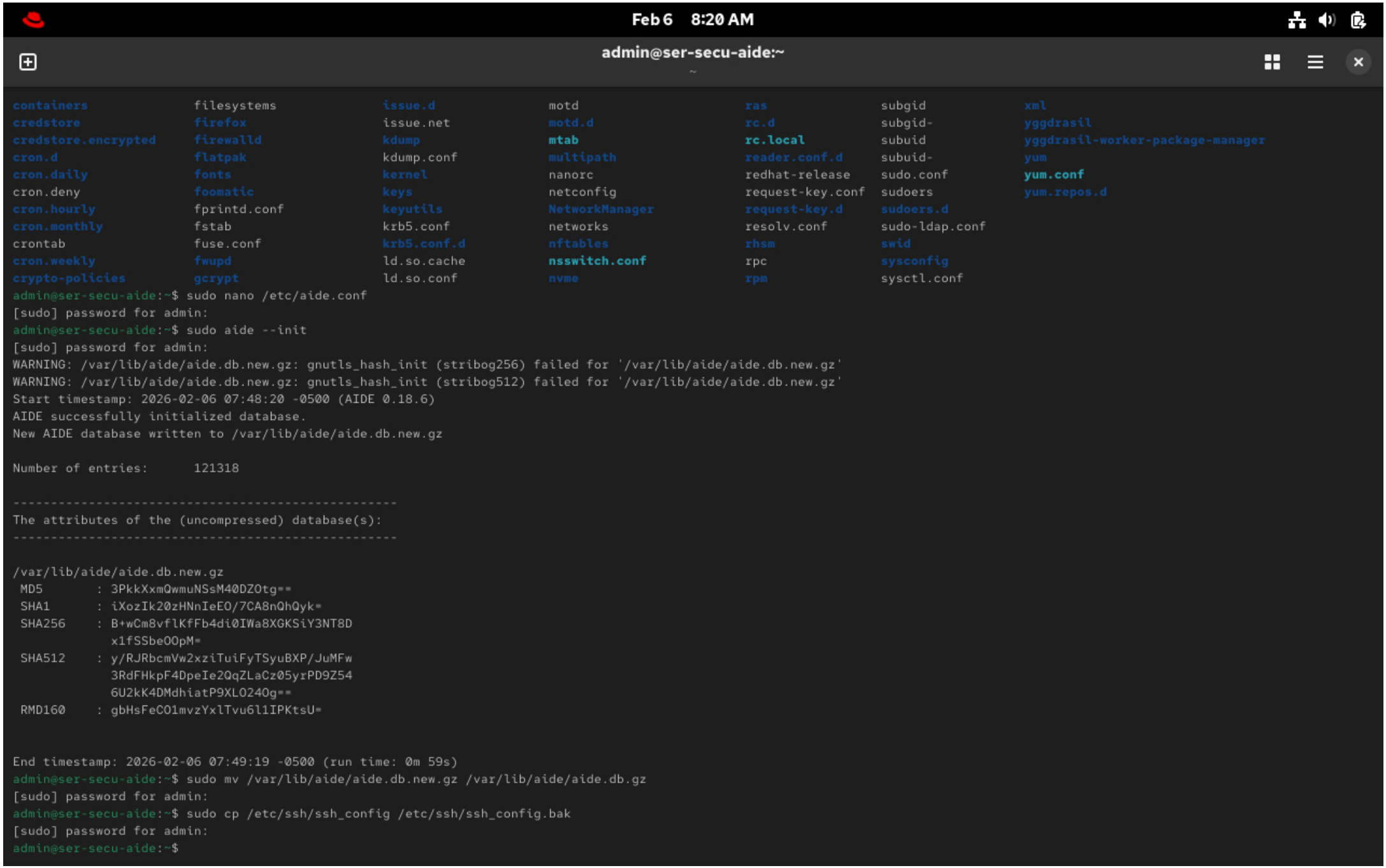

Feb 6 8:30 AM
admin@ser-secu-aide:~
~
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$ echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/ssh_config
PermitRootLogin yes
admin@ser-secu-aide:~$ echo "# Malicious entry" | sudo tee -a /etc/hosts
Malicious entry
admin@ser-secu-aide:~$ echo "Simulation attack 2"
Simulation attack 2
admin@ser-secu-aide:~$ sudo cp /bin/ls /usr/local/bin/maintenance
admin@ser-secu-aide:~$ sudo chmod +x /usr/local/bin/maintenance
admin@ser-secu-aide:~$

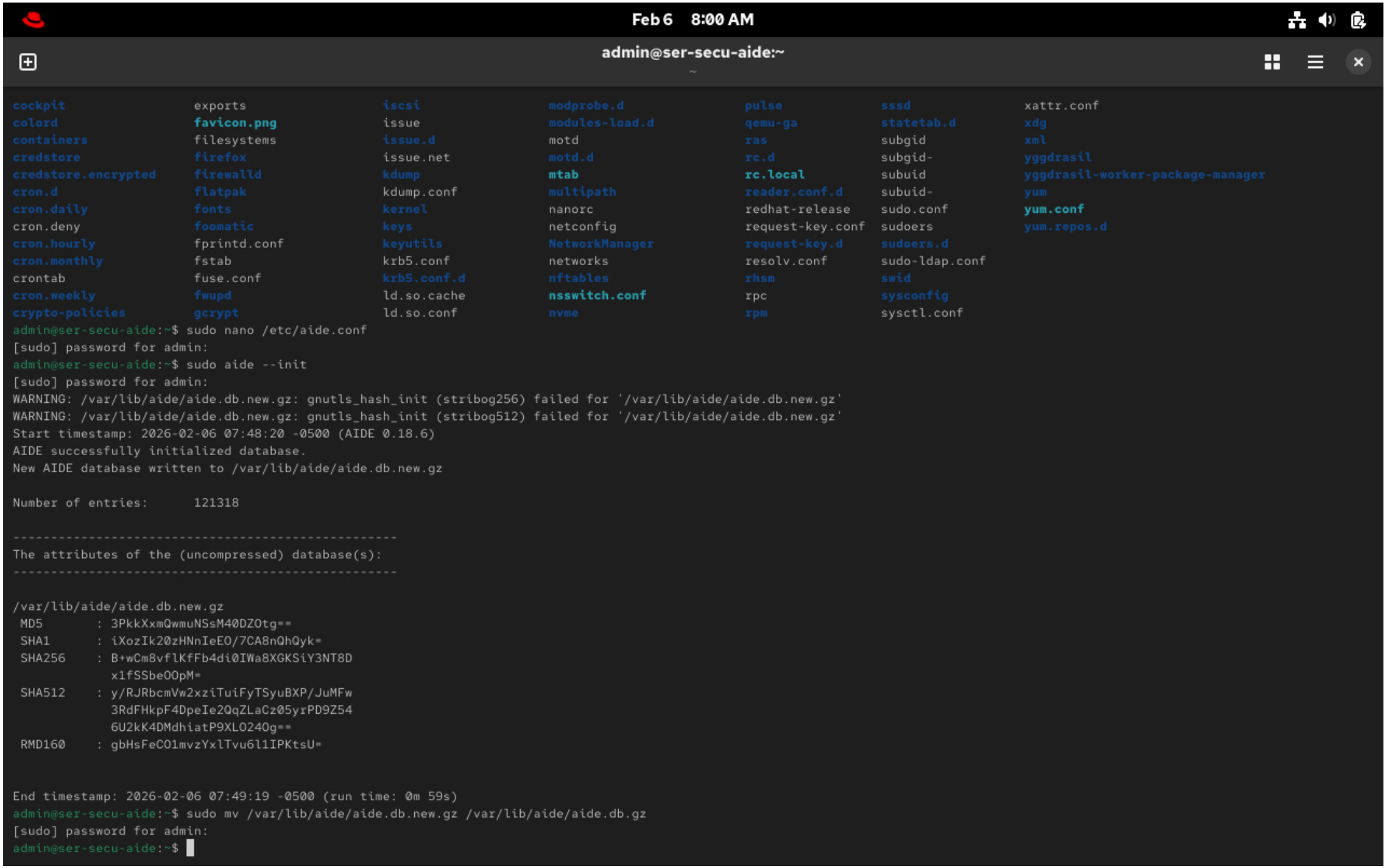

Feb 6 8:25 AM
admin@ser-secu-aide:~
cron.daily fonts kernel nanorc redhat-release sudo.conf yum.conf
cron.deny foomatic keys netconfig request-key.conf sudoers yum.repos.d
cron.hourly fprintd.conf keyutils NetworkManager request-key.d sudoers.d
cron.monthly fstab krb5.conf networks resolv.conf sudo-ldap.conf
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$ echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/ssh_config
PermitRootLogin yes
admin@ser-secu-aide:~$ echo "# Malicious entry" | sudo tee -a /etc/hosts
Malicious entry
admin@ser-secu-aide:~$


Feb 6 8:24 AM
admin@ser-secu-aide:~
credstore.encrypted firewalld kdump mtab rc.local subuid yggdrasil-worker-package-manager
cron.d flatpak kdump.conf multipath reader.conf.d subuid- yum
cron.daily fonts kernel nanorc redhat-release sudo.conf yum.conf
cron.deny foomatic keys netconfig request-key.conf sudoers yum.repos.d
cron.hourly fprintd.conf keyutils NetworkManager request-key.d sudoers.d
cron.monthly fstab krb5.conf networks resolv.conf sudo-ldap.conf
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318

The attributes of the (uncompressed) database(s):

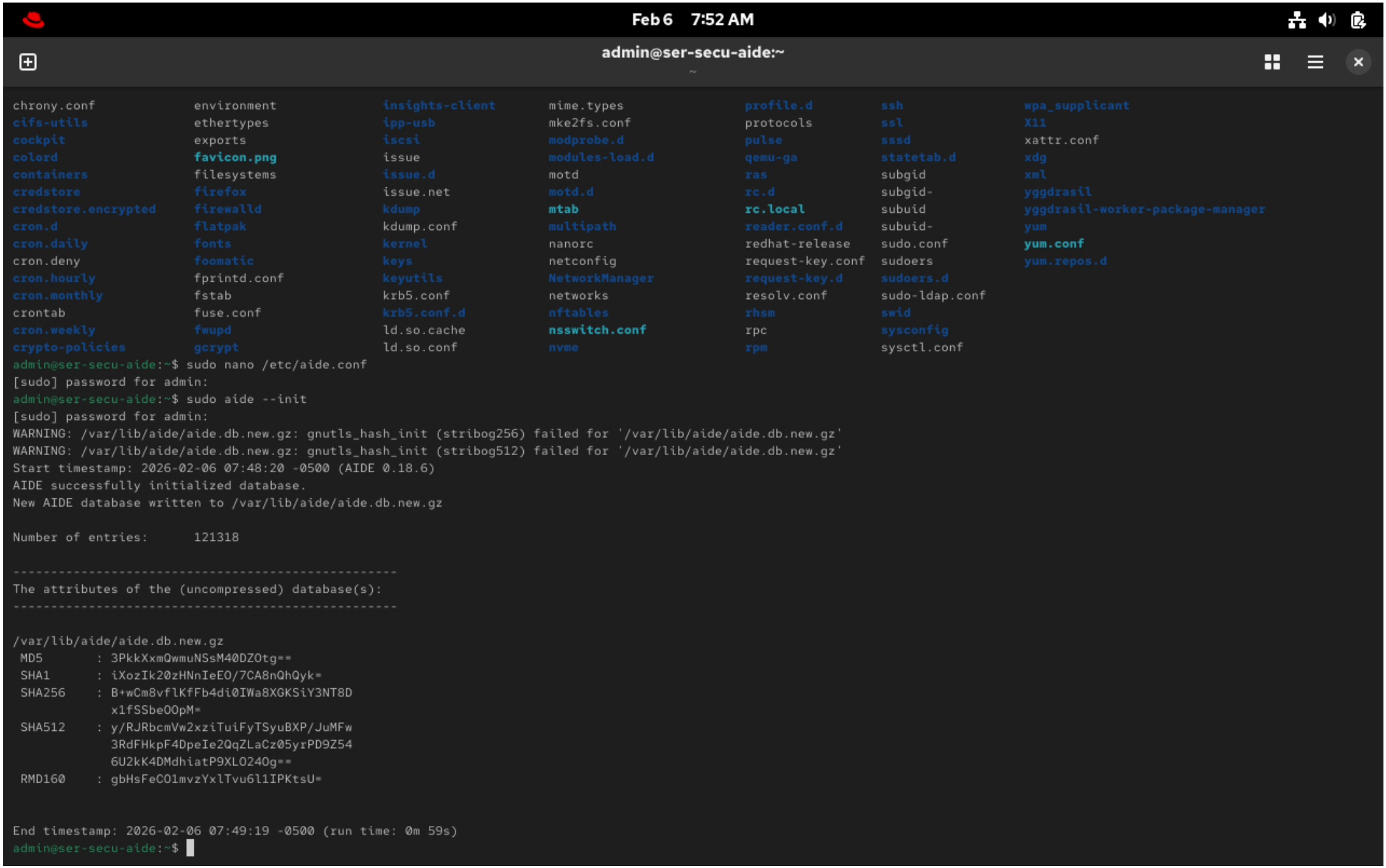
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$ echo "PermitRootLogin yes" | sudo tee -a /etc/ssh/ssh_config
PermitRootLogin yes
admin@ser-secu-aide:~$

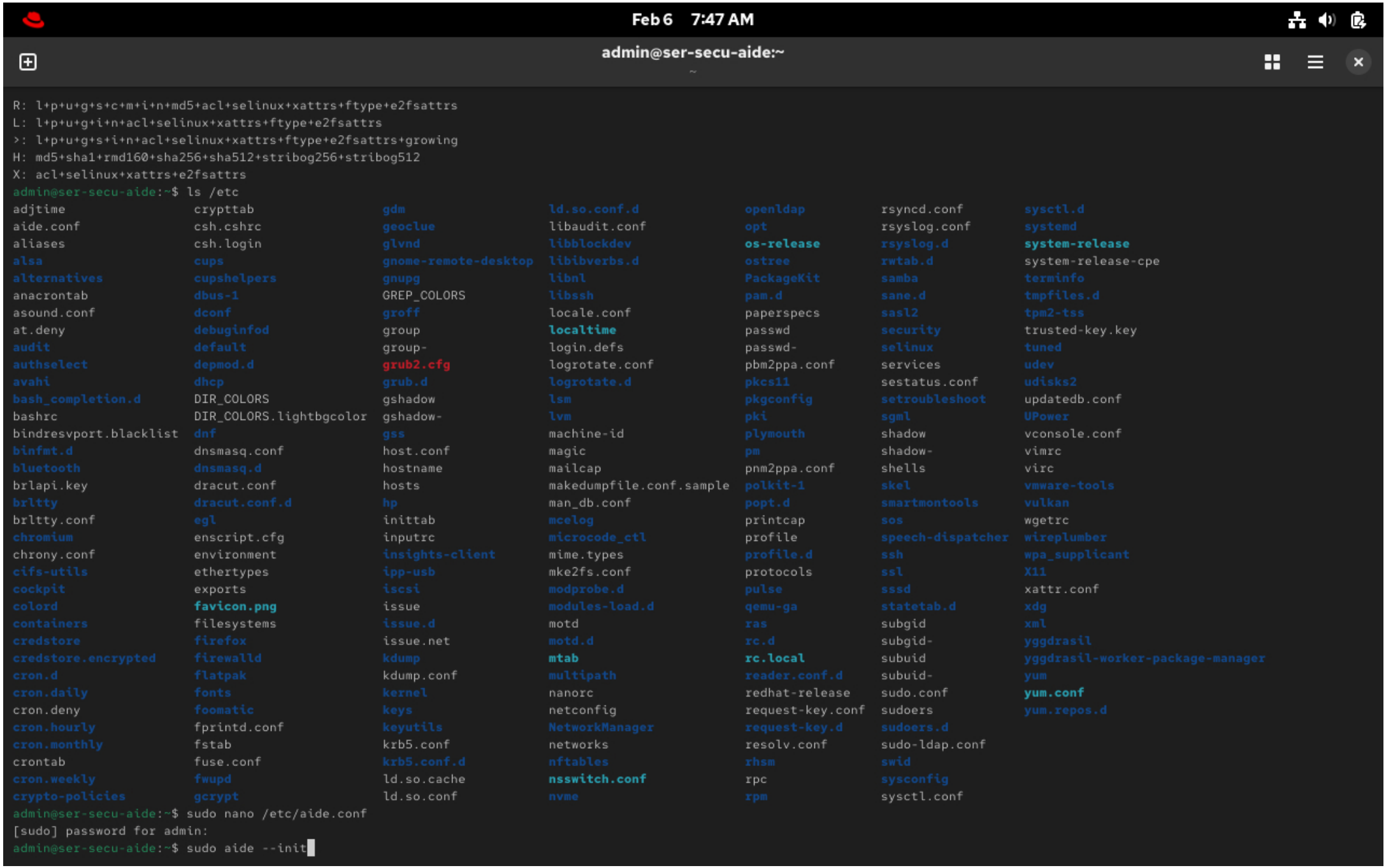

Feb 6 8:20 AM
admin@ser-secu-aide:~
containers filesystems issue.d motd ras subgid xml
credstore firefox issue.net motd.d rc.d subgid- yggdrasil
credstore.encrypted firewalld kdump mtab rc.local subuid yggdrasil-worker-package-manager
cron.d flatpak kdump.conf multipath reader.conf.d subuid- yum
cron.daily fonts kernel nanorc redhat-release sudo.conf yum.conf
cron.deny foomatic keys netconfig request-key.conf sudoers yum.repos.d
cron.hourly fprintd.conf keyutils NetworkManager request-key.d sudoers.d
cron.monthly fstab krb5.conf networks resolv.conf sudo-ldap.conf
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo cp /etc/ssh/ssh_config /etc/ssh/ssh_config.bak
[sudo] password for admin:
admin@ser-secu-aide:~$

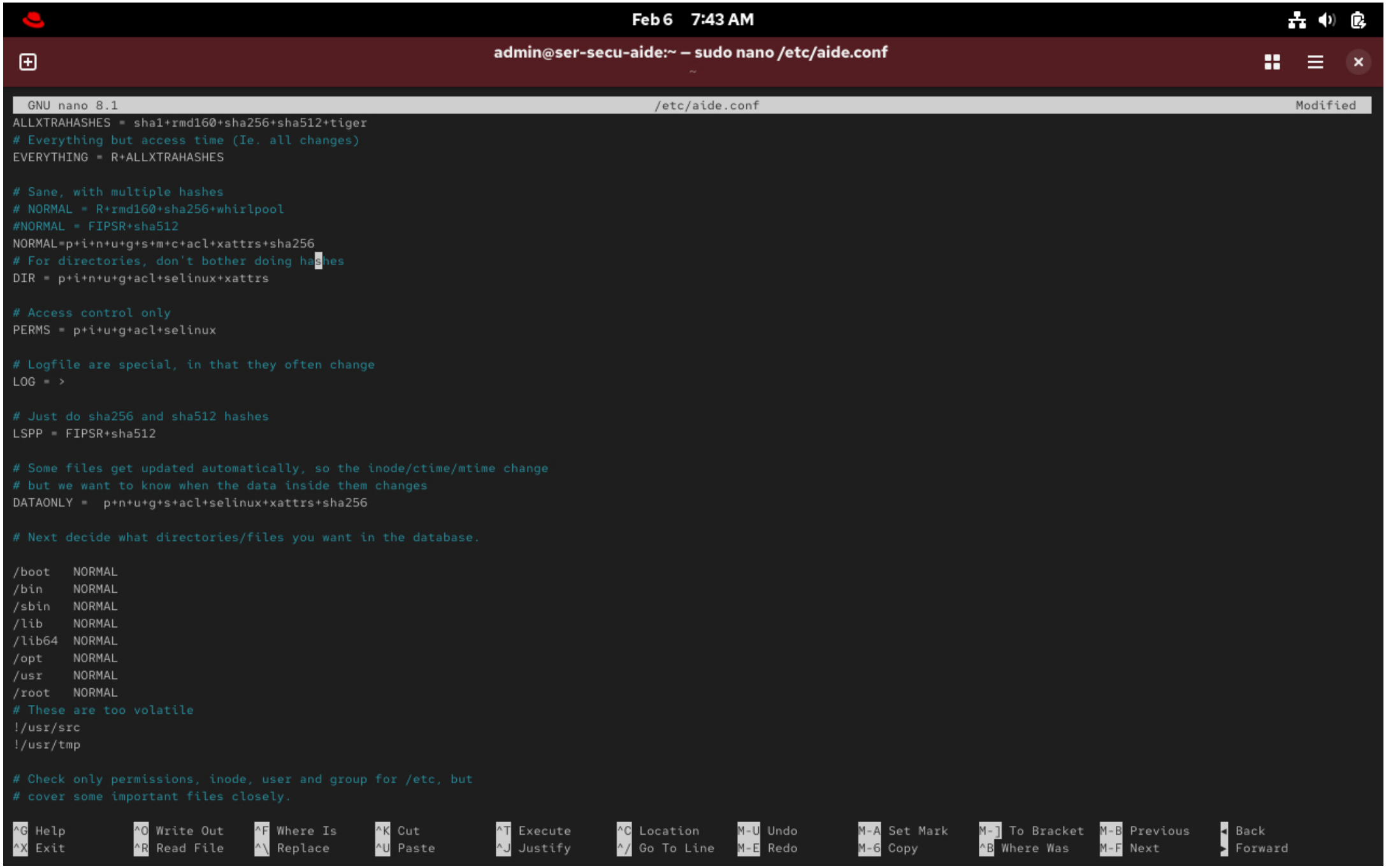

Feb 6 8:00 AM
admin@ser-secu-aide:~
~
cockpit exports iscsi modprobe.d pulse sssd xattr.conf
colord favicon.png issue modules-load.d qemu-ga statetab.d xdg
containers filesystems issue.d motd ras subgid xml
credstore firefox issue.net motd.d rc.d subgid- yggdrasil
credstore.encrypted firewalld kdump mtab rc.local subuid yggdrasil-worker-package-manager
cron.d flatpak kdump.conf multipath reader.conf.d subuid- yum
cron.daily fonts kernel nanorc redhat-release sudo.conf yum.conf
cron.deny foomatic keys netconfig request-key.conf sudoers yum.repos.d
cron.hourly fprintd.conf keyutils NetworkManager request-key.d sudoers.d
cron.monthly fstab krb5.conf networks resolv.conf sudo-ldap.conf
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318

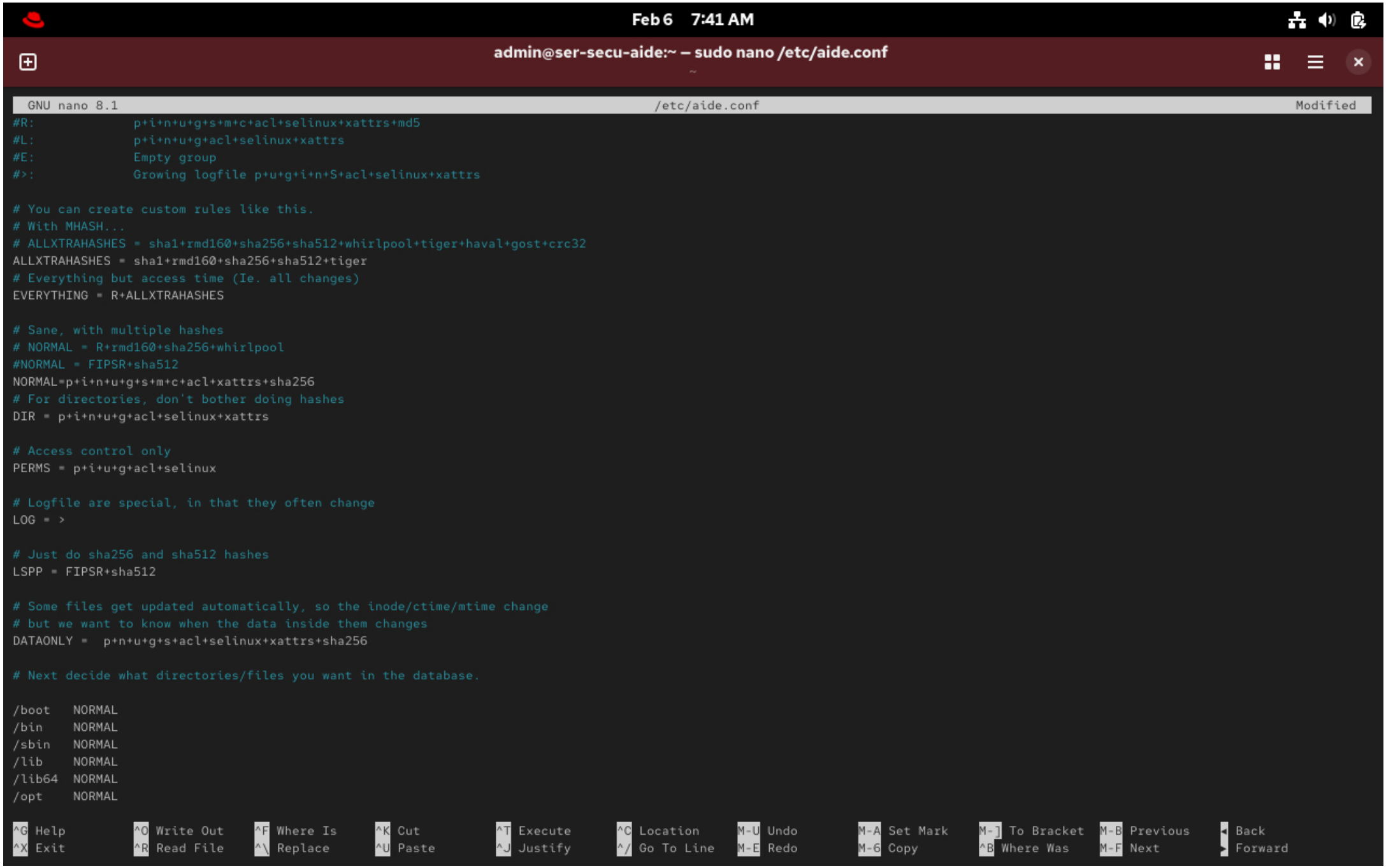
The attributes of the (uncompressed) database(s):

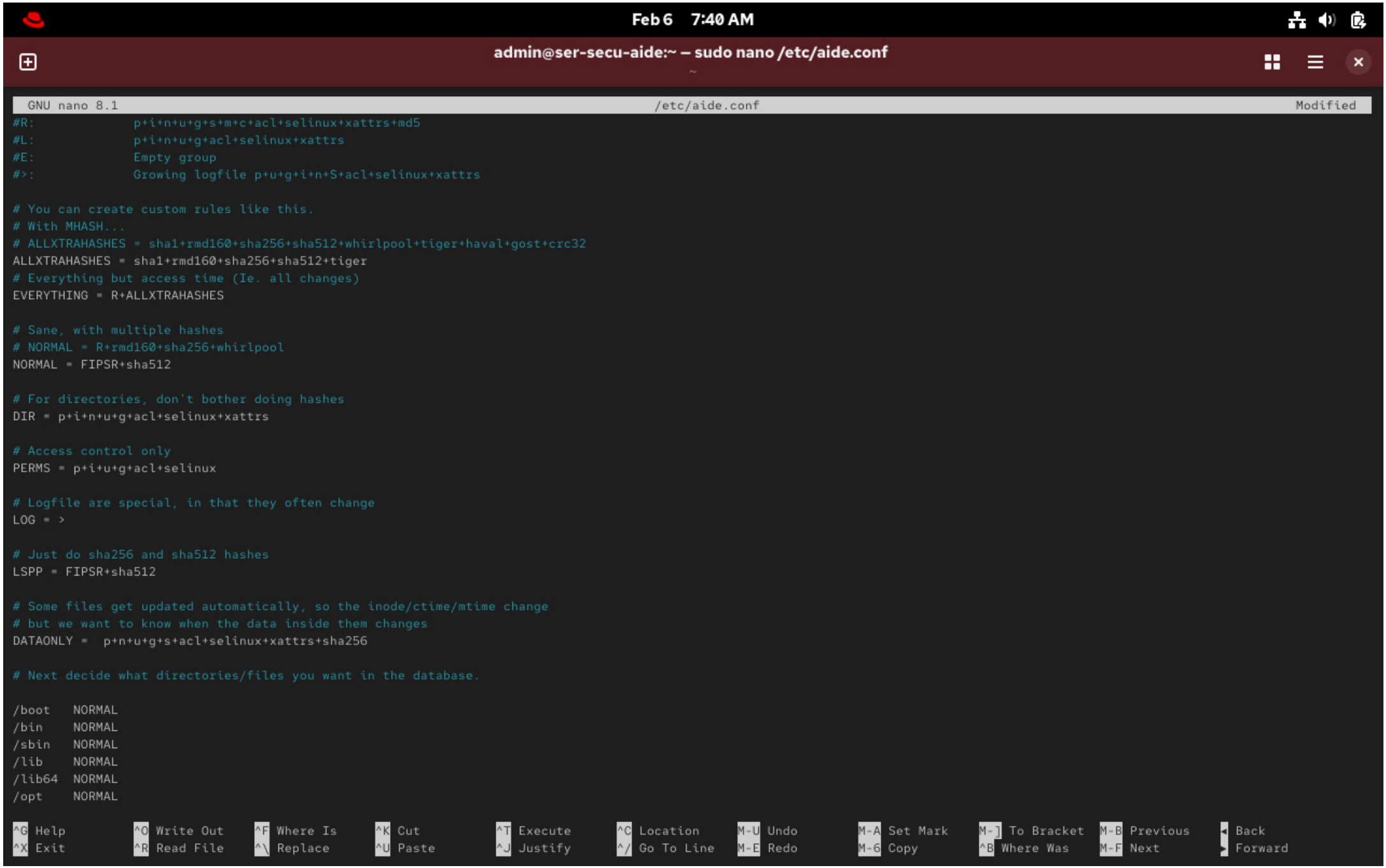
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$ sudo mv /var/lib/aide/aide.db.new.gz /var/lib/aide/aide.db.gz
[sudo] password for admin:
admin@ser-secu-aide:~$

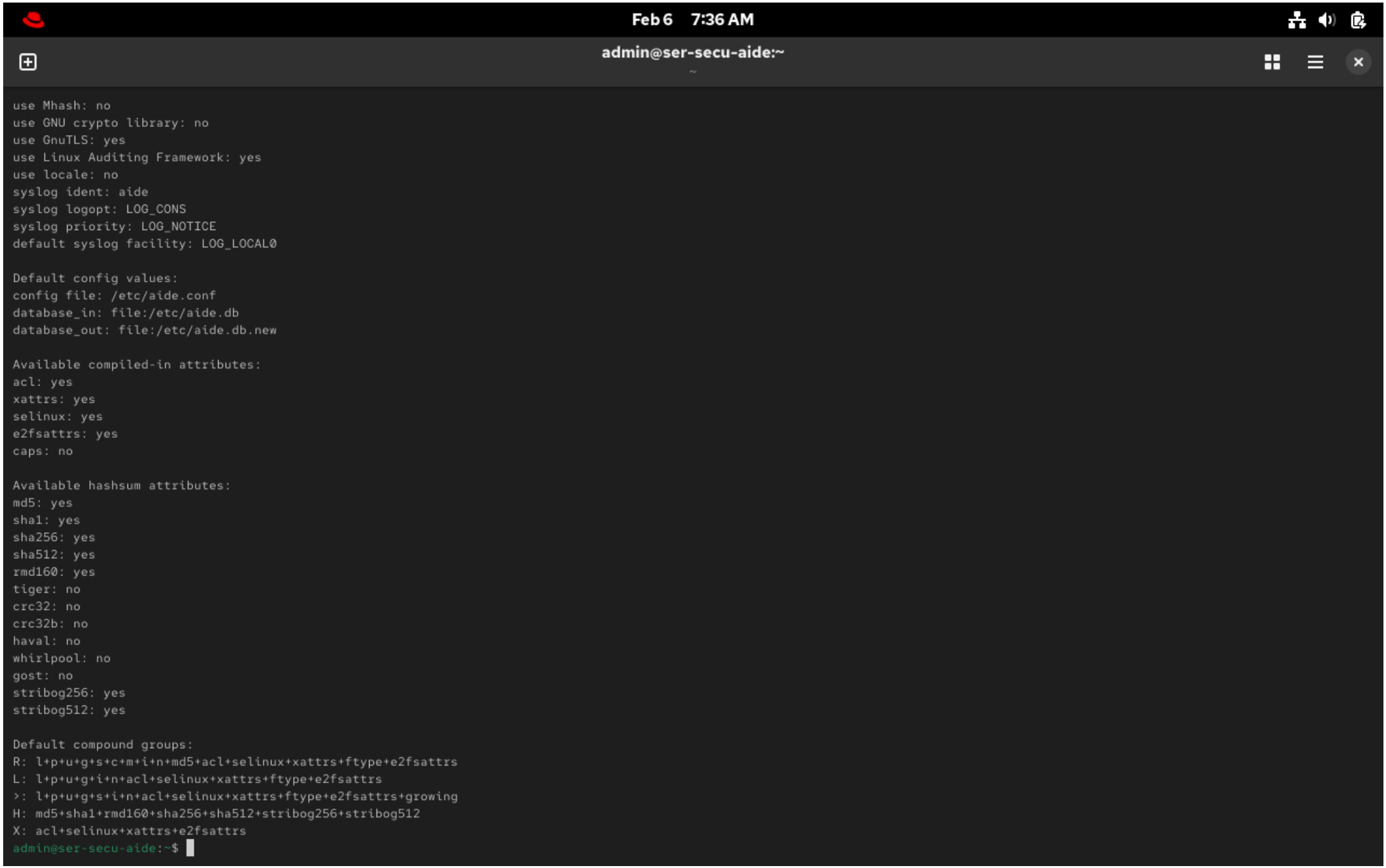

Feb 6 7:52 AM
admin@ser-secu-aide:~
chrony.conf environment insights-client mime.types profile.d ssh wpa_supplicant
cifs-utils ethertypes ipp-usb mke2fs.conf protocols ssl X11
cockpit exports iscsi modprobe.d pulse sssd xattr.conf
colord favicon.png issue modules-load.d qemu-ga statetab.d xdg
containers filesystems issue.d motd ras subgid xml
credstore firefox issue.net motd.d rc.d subgid- yggdrasil
credstore.encrypted firewalld kdump mtab rc.local subuid yggdrasil-worker-package-manager
cron.d flatpak kdump.conf multipath reader.conf.d subuid- yum
cron.daily fonts kernel nanorc redhat-release sudo.conf yum.conf
cron.deny foomatic keys netconfig request-key.conf sudoers yum.repos.d
cron.hourly fprintd.conf keyutils NetworkManager request-key.d sudoers.d
cron.monthly fstab krb5.conf networks resolv.conf sudo-ldap.conf
crontab fuse.conf krb5.conf.d nftables rhsm swid
cron.weekly fwupd ld.so.cache nsswitch.conf rpc sysconfig
crypto-policies gcrypt ld.so.conf nvme rpm sysctl.conf
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init
[sudo] password for admin:
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog256) failed for '/var/lib/aide/aide.db.new.gz'
WARNING: /var/lib/aide/aide.db.new.gz: gnutls_hash_init (stribog512) failed for '/var/lib/aide/aide.db.new.gz'
Start timestamp: 2026-02-06 07:48:20 -0500 (AIDE 0.18.6)
AIDE successfully initialized database.
New AIDE database written to /var/lib/aide/aide.db.new.gz
Number of entries: 121318
The attributes of the (uncompressed) database(s):
/var/lib/aide/aide.db.new.gz
MD5 : 3PkkXxmQwmuNSsM40DZOtg==
SHA1 : iXozIk20zHNnIeEO/7CA8nQhQyk=
SHA256 : B+wCm8vflKfFb4di0IWa8XGKSiY3NT8D
x1fSSbeOOpM=
SHA512 : y/RJRbcmVw2xziTuiFyTSyuBXP/JuMFw
3RdFHkpF4DpeIe2QqZLaCz05yrPD9Z54
6U2kK4DMdhiatP9XLO24Og==
RMD160 : gbHsFeCO1mvzYxlTvu6l1IPKtsU=
End timestamp: 2026-02-06 07:49:19 -0500 (run time: 0m 59s)
admin@ser-secu-aide:~$

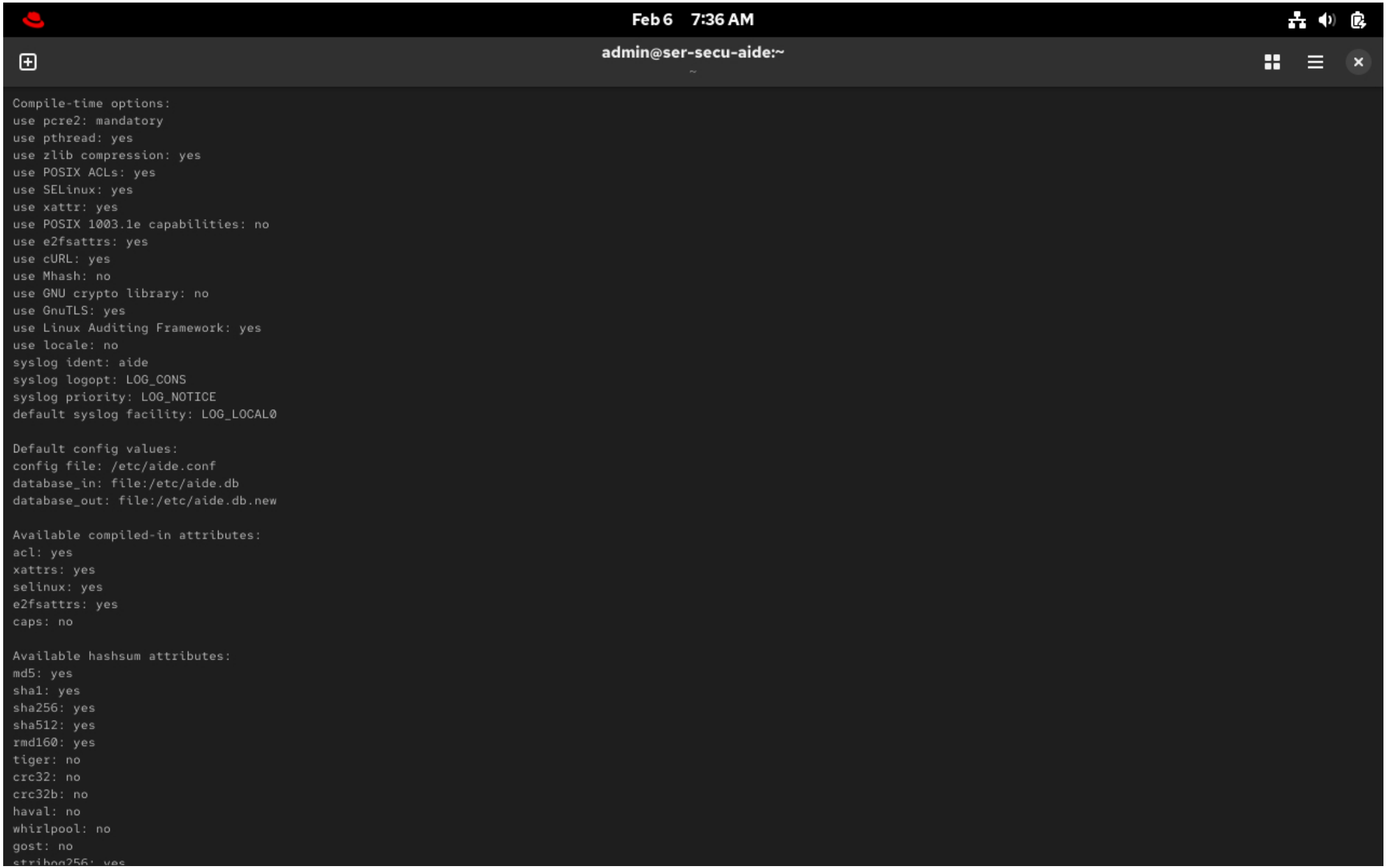

Feb 6 7:47 AM
admin@ser-secu-aide:~
R: l+p+u+g+s+c+m+i+n+md5+acl+selinux+xattrs+ftype+e2fsattrs
L: l+p+u+g+i+n+acl+selinux+xattrs+ftype+e2fsattrs
>: l+p+u+g+s+i+n+acl+selinux+xattrs+ftype+e2fsattrs+growing
H: md5+sha1+rmd160+sha256+sha512+stribog256+stribog512
X: acl+selinux+xattrs+e2fsattrs
admin@ser-secu-aide:~$ ls /etc
adjtime
aide.conf
aliases
alsa
alternatives
anacrontab
asound.conf
at.deny
audit
authselect
avahi
bash_completion.d
bashrc
bindresvport.blacklist
binfmt.d
bluetooth
brlapi.key
brltty
brltty.conf
chromium
chrony.conf
cifs-utils
cockpit
colord
containers
credstore
credstore.encrypted
cron.d
cron.daily
cron.deny
cron.hourly
cron.monthly
crontab
cron.weekly
crypto-policies
crypttab
csh.cshrc
csh.login
cups
cupshelpers
dbus-1
dconf
debuginfod
default
depmod.d
dhcp
DIR_COLORS
DIR_COLORS.lightbgcolor
dnf
dnsmasq.conf
dnsmasq.d
dracut.conf
dracut.conf.d
egl
enscript.cfg
environment
ethertypes
exports
favicon.png
filesystems
firefox
firewalld
flatpak
fonts
foomatic
fprintd.conf
fstab
fuse.conf
fwupd
gcrypt
gdm
geoclue
glvnd
gnome-remote-desktop
gnupg
GREP_COLORS
groff
group
group-
grub2.cfg
grub.d
gshadow
gshadow-
gss
host.conf
hostname
hosts
hp
inittab
inputrc
insights-client
ipp-usb
iscsi
issue
issue.d
issue.net
kdump
kdump.conf
kernel
keys
keyutils
krb5.conf
krb5.conf.d
ld.so.cache
ld.so.conf
ld.so.conf.d
libaudit.conf
libblockdev
libibverbs.d
libnl
libssh
locale.conf
localtime
login.defs
logrotate.conf
logrotate.d
lsm
lvm
machine-id
magic
mailcap
makedumpfile.conf.sample
man_db.conf
mcelog
microcode_ctl
mime.types
mke2fs.conf
modprobe.d
modules-load.d
motd
motd.d
mtab
multipath
nanorc
netconfig
NetworkManager
networks
nftables
nsswitch.conf
nvme
openldap
opt
os-release
ostree
PackageKit
pam.d
paperspecs
passwd
passwd-
pbm2ppa.conf
pkcs11
pkgconfig
pki
plymouth
pm
pnm2ppa.conf
polkit-1
popt.d
printcap
profile
profile.d
protocols
pulse
qemu-ga
ras
rc.d
rc.local
reader.conf.d
redhat-release
request-key.conf
request-key.d
resolv.conf
rhsm
rpc
rpm
rsyncd.conf
rsyslog.conf
rsyslog.d
rwtab.d
samba
sane.d
sasl2
security
selinux
services
sestatus.conf
setroubleshoot
sgml
shadow
shadow-
shells
skel
smartmontools
sos
speech-dispatcher
ssh
ssl
sssd
statetab.d
subgid
subgid-
subuid
subuid-
sudo.conf
sudoers
sudoers.d
sudo-ldap.conf
swid
sysconfig
sysctl.conf
sysctl.d
systemd
system-release
system-release-cpe
terminfo
tmpfiles.d
tpm2-tss
trusted-key.key
tuned
udev
udisks2
updatedb.conf
UPower
vconsole.conf
vimrc
virc
vmware-tools
vulkan
wgetrc
wireplumber
wpa_supplicant
X11
xattr.conf
xdg
xml
yggdrasil
yggdrasil-worker-package-manager
yum
yum.conf
yum.repos.d
admin@ser-secu-aide:~$ sudo nano /etc/aide.conf
[sudo] password for admin:
admin@ser-secu-aide:~$ sudo aide --init

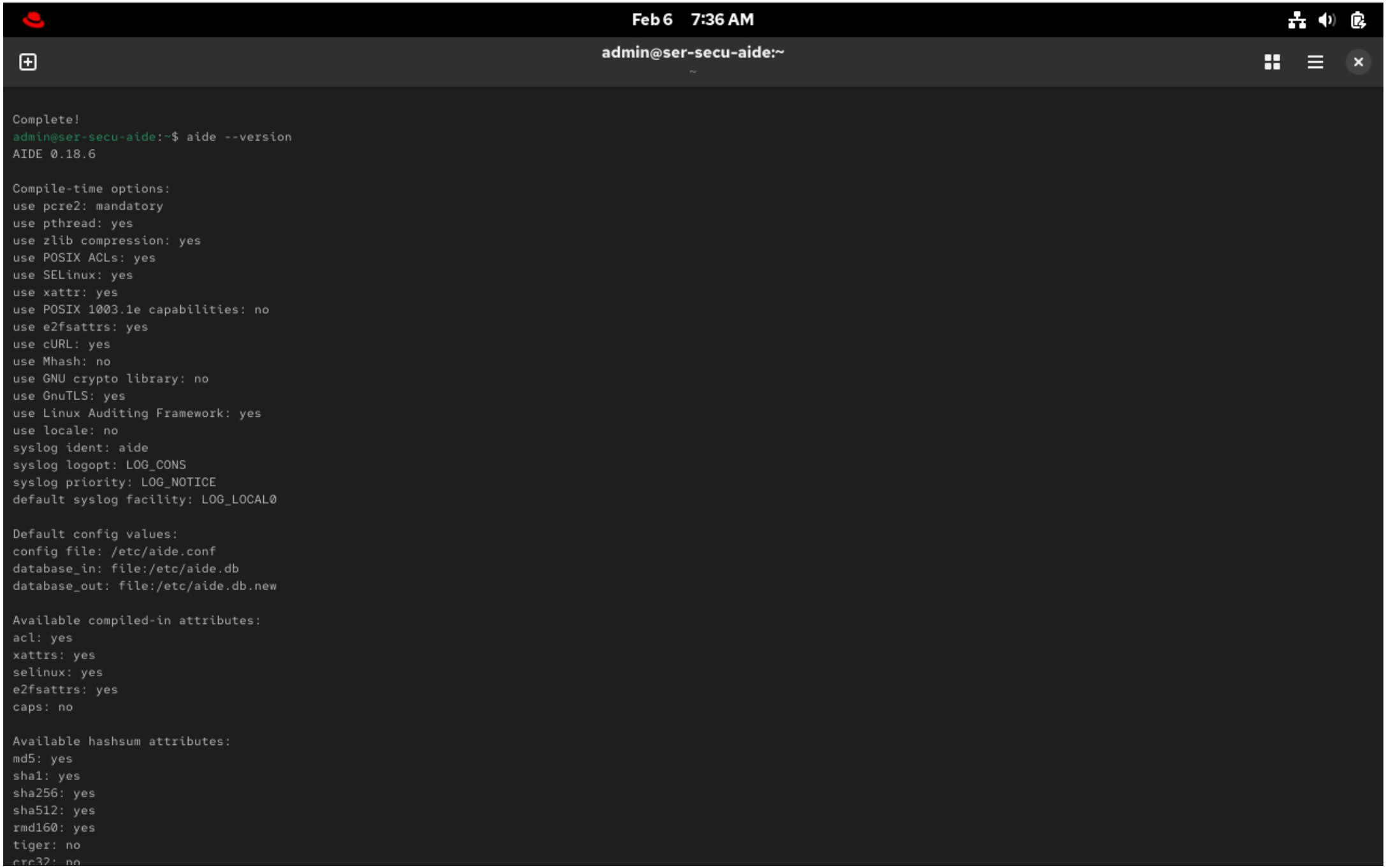

Feb 6 7:43 AM
admin@ser-secu-aide:~ – sudo nano /etc/aide.conf
GNU nano 8.1 /etc/aide.conf Modified
ALLXTRAHASHES = sha1+rmd160+sha256+sha512+tiger
# Everything but access time (Ie. all changes)
EVERYTHING = R+ALLXTRAHASHES
# Sane, with multiple hashes
# NORMAL = R+rmd160+sha256+whirlpool
#NORMAL = FIPSR+sha512
NORMAL=p+i+n+u+g+s+m+c+acl+xattrs+sha256
# For directories, don't bother doing hashes
DIR = p+i+n+u+g+acl+selinux+xattrs
# Access control only
PERMS = p+i+u+g+acl+selinux
# Logfile are special, in that they often change
LOG = >
# Just do sha256 and sha512 hashes
LSPP = FIPSR+sha512
# Some files get updated automatically, so the inode/ctime/mtime change
# but we want to know when the data inside them changes
DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256
# Next decide what directories/files you want in the database.
/boot NORMAL
/bin NORMAL
/sbin NORMAL
/lib NORMAL
/lib64 NORMAL
/opt NORMAL
/usr NORMAL
/root NORMAL
These are too volatile
!/usr/src
!/usr/tmp
Check only permissions, inode, user and group for /etc, but
cover some important files closely.
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ◂ Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next ▸ Forward

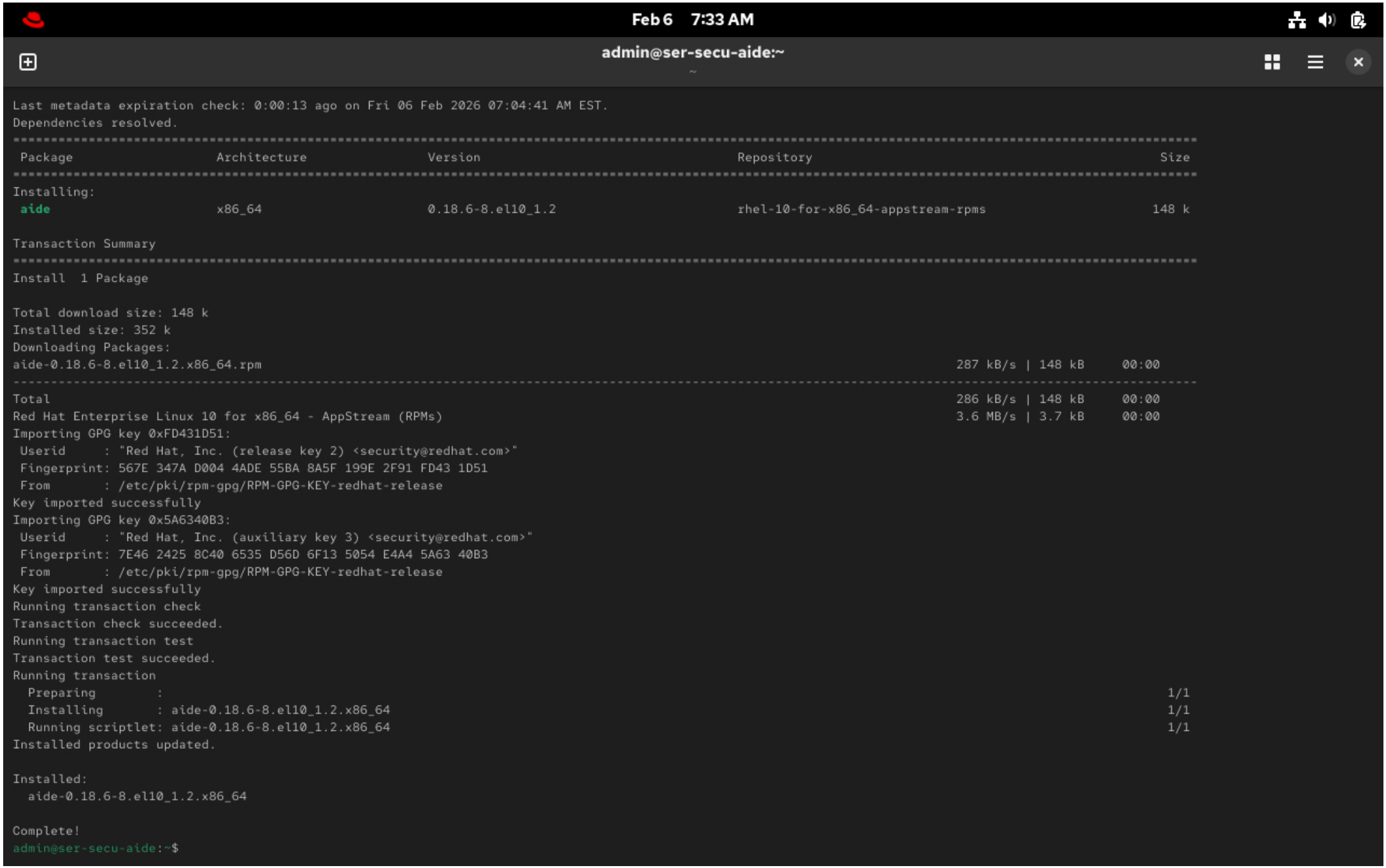

Feb 6 7:41 AM
admin@ser-secu-aide:~ – sudo nano /etc/aide.conf
GNU nano 8.1 /etc/aide.conf Modified
#R: p+i+n+u+g+s+m+c+acl+selinux+xattrs+md5
#L: p+i+n+u+g+acl+selinux+xattrs
#E: Empty group
#>: Growing logfile p+u+g+i+n+S+acl+selinux+xattrs
# You can create custom rules like this.
# With MHASH...
# ALLXTRAHASHES = sha1+rmd160+sha256+sha512+whirlpool+tiger+haval+gost+crc32
ALLXTRAHASHES = sha1+rmd160+sha256+sha512+tiger
# Everything but access time (Ie. all changes)
EVERYTHING = R+ALLXTRAHASHES
# Sane, with multiple hashes
# NORMAL = R+rmd160+sha256+whirlpool
#NORMAL = FIPSR+sha512
NORMAL=p+i+n+u+g+s+m+c+acl+xattrs+sha256
# For directories, don't bother doing hashes
DIR = p+i+n+u+g+acl+selinux+xattrs
# Access control only
PERMS = p+i+u+g+acl+selinux
# Logfile are special, in that they often change
LOG = >
# Just do sha256 and sha512 hashes
LSPP = FIPSR+sha512
# Some files get updated automatically, so the inode/ctime/mtime change
# but we want to know when the data inside them changes
DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256
# Next decide what directories/files you want in the database.
/boot NORMAL
/bin NORMAL
/sbin NORMAL
/lib NORMAL
/lib64 NORMAL
/opt NORMAL
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ◂ Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next ▸ Forward

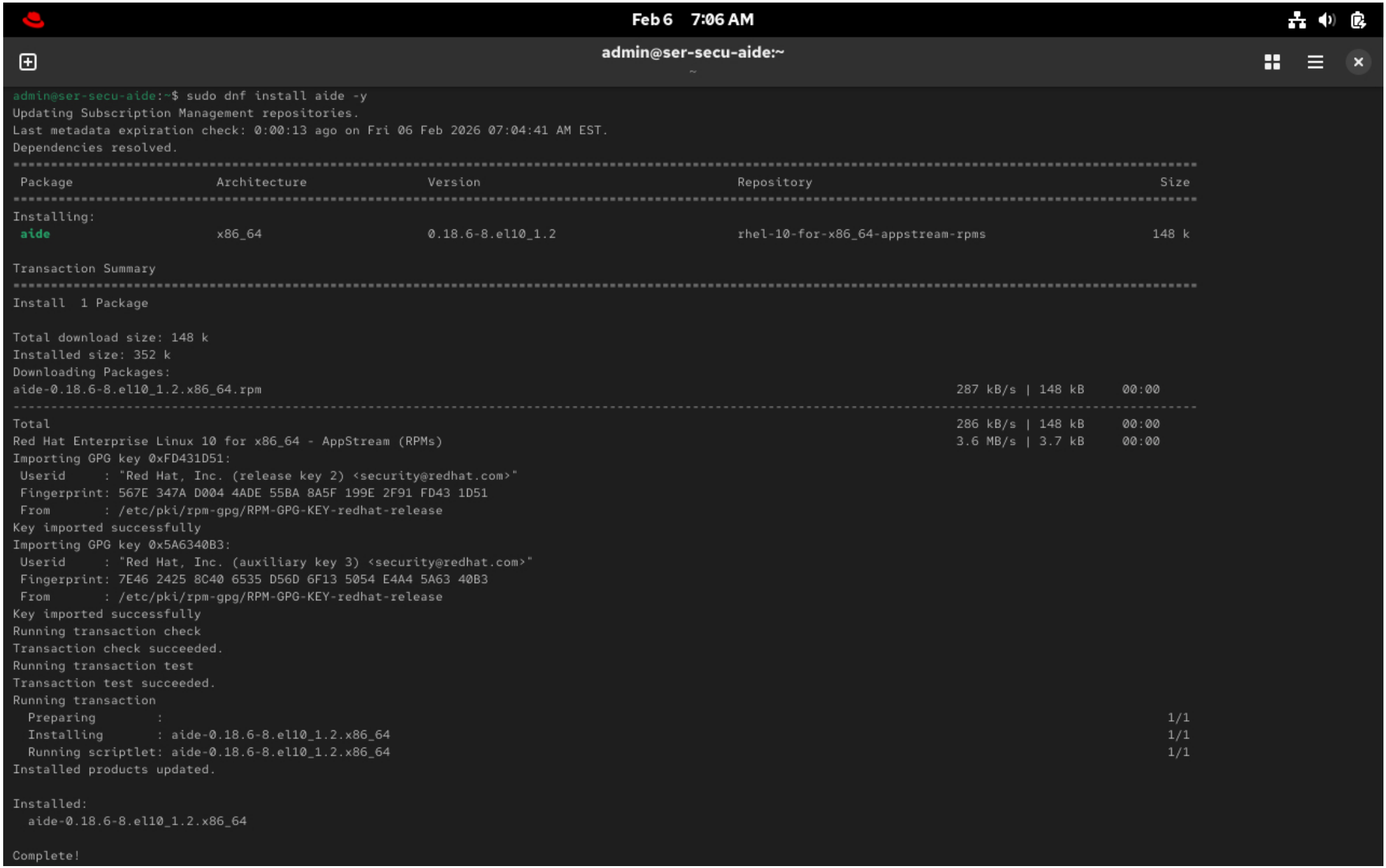

Feb 6 7:40 AM
admin@ser-secu-aide:~ – sudo nano /etc/aide.conf
GNU nano 8.1 /etc/aide.conf Modified
#R: p+i+n+u+g+s+m+c+acl+selinux+xattrs+md5
#L: p+i+n+u+g+acl+selinux+xattrs
#E: Empty group
#>: Growing logfile p+u+g+i+n+S+acl+selinux+xattrs
# You can create custom rules like this.
# With MHASH...
# ALLXTRAHASHES = sha1+rmd160+sha256+sha512+whirlpool+tiger+haval+gost+crc32
ALLXTRAHASHES = sha1+rmd160+sha256+sha512+tiger
# Everything but access time (Ie. all changes)
EVERYTHING = R+ALLXTRAHASHES
# Sane, with multiple hashes
# NORMAL = R+rmd160+sha256+whirlpool
NORMAL = FIPSR+sha512
# For directories, don't bother doing hashes
DIR = p+i+n+u+g+acl+selinux+xattrs
# Access control only
PERMS = p+i+u+g+acl+selinux
# Logfile are special, in that they often change
LOG = >
# Just do sha256 and sha512 hashes
LSPP = FIPSR+sha512
# Some files get updated automatically, so the inode/ctime/mtime change
# but we want to know when the data inside them changes
DATAONLY = p+n+u+g+s+acl+selinux+xattrs+sha256
# Next decide what directories/files you want in the database.
/boot NORMAL
/bin NORMAL
/sbin NORMAL
/lib NORMAL
/lib64 NORMAL
/opt NORMAL
^G Help ^O Write Out ^F Where Is ^K Cut ^T Execute ^C Location M-U Undo M-A Set Mark M-] To Bracket M-B Previous ◂ Back
^X Exit ^R Read File ^\ Replace ^U Paste ^J Justify ^/ Go To Line M-E Redo M-6 Copy ^B Where Was M-F Next ▸ Forward

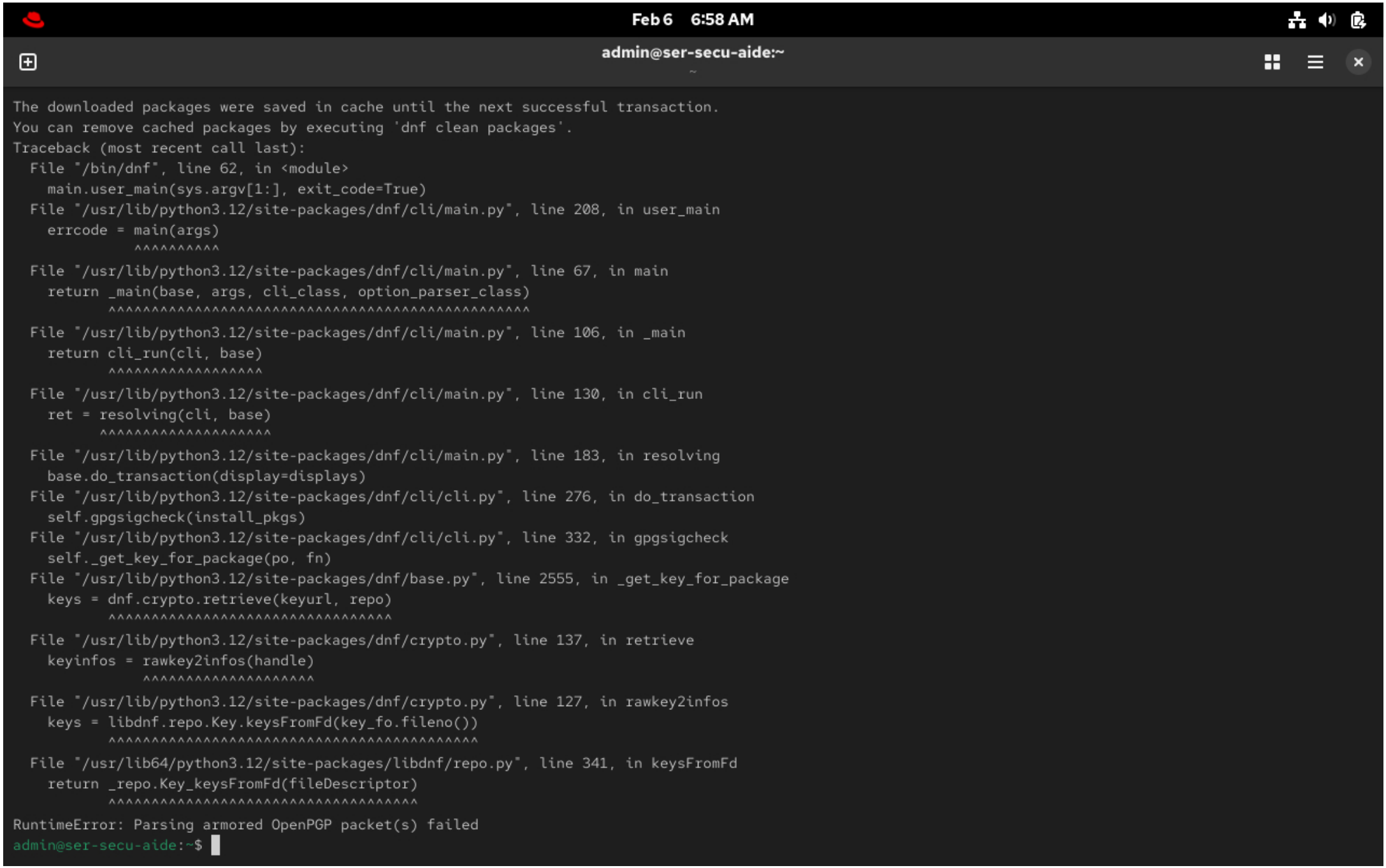

Feb 6 7:36 AM
admin@ser-secu-aide:~
use Mhash: no
use GNU crypto library: no
use GnuTLS: yes
use Linux Auditing Framework: yes
use locale: no
syslog ident: aide
syslog logopt: LOG_CONS
syslog priority: LOG_NOTICE
default syslog facility: LOG_LOCAL0
Default config values:
config file: /etc/aide.conf
database_in: file:/etc/aide.db
database_out: file:/etc/aide.db.new
Available compiled-in attributes:
acl: yes
xattrs: yes
selinux: yes
e2fsattrs: yes
caps: no
Available hashsum attributes:
md5: yes
sha1: yes
sha256: yes
sha512: yes
rmd160: yes
tiger: no
crc32: no
crc32b: no
haval: no
whirlpool: no
gost: no
stribog256: yes
stribog512: yes
Default compound groups:
R: l+p+u+g+s+c+m+i+n+md5+acl+selinux+xattrs+ftype+e2fsattrs
L: l+p+u+g+i+n+acl+selinux+xattrs+ftype+e2fsattrs
>: l+p+u+g+s+i+n+acl+selinux+xattrs+ftype+e2fsattrs+growing
H: md5+sha1+rmd160+sha256+sha512+stribog256+stribog512
X: acl+selinux+xattrs+e2fsattrs
admin@ser-secu-aide:~$

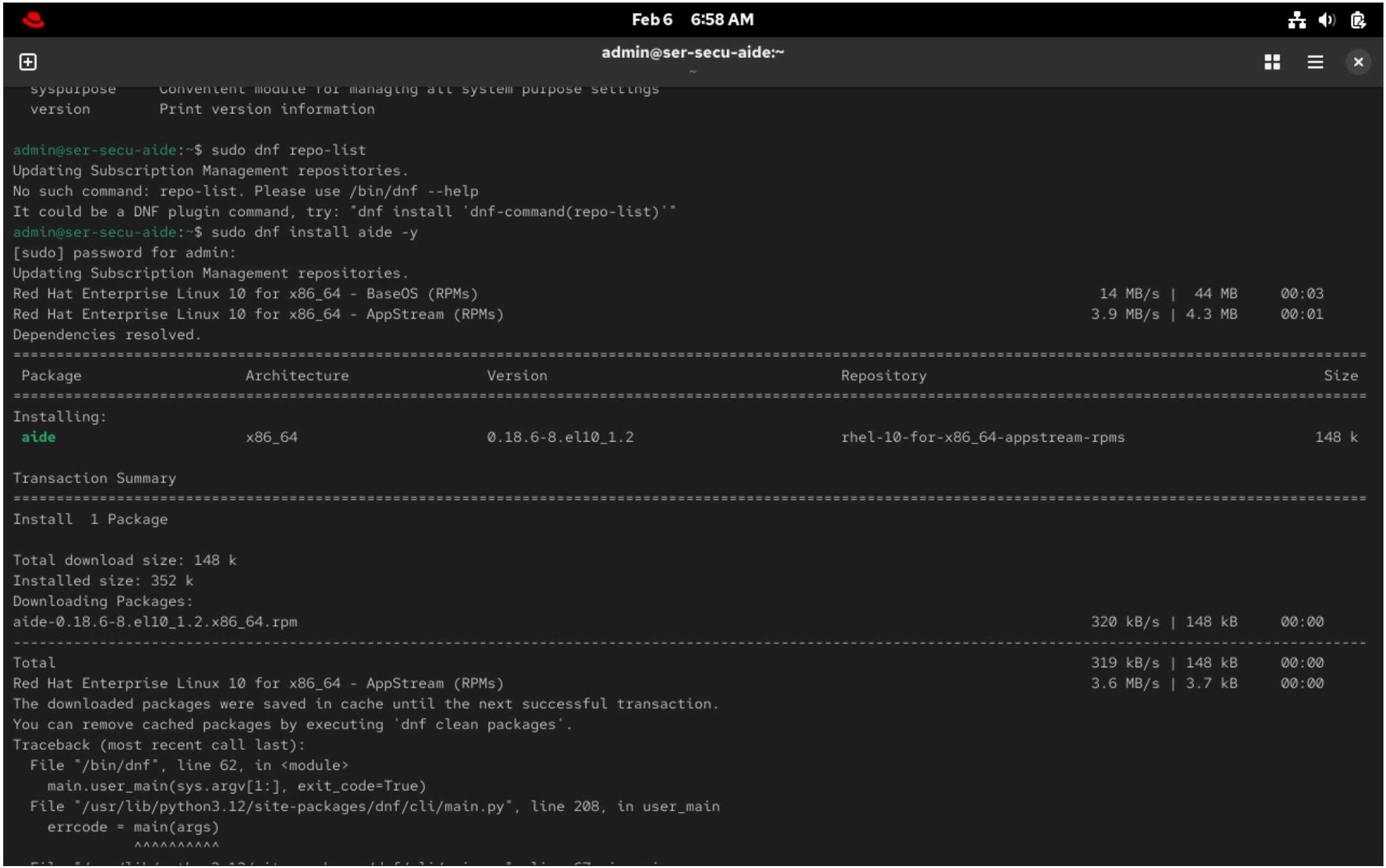

Feb 6 7:36 AM
admin@ser-secu-aide:~
Compile-time options:
use pcre2: mandatory
use pthread: yes
use zlib compression: yes
use POSIX ACLs: yes
use SELinux: yes
use xattr: yes
use POSIX 1003.1e capabilities: no
use e2fsattrs: yes
use cURL: yes
use Mhash: no
use GNU crypto library: no
use GnuTLS: yes
use Linux Auditing Framework: yes
use locale: no
syslog ident: aide
syslog logopt: LOG_CONS
syslog priority: LOG_NOTICE
default syslog facility: LOG_LOCAL0
Default config values:
config file: /etc/aide.conf
database_in: file:/etc/aide.db
database_out: file:/etc/aide.db.new
Available compiled-in attributes:
acl: yes
xattrs: yes
selinux: yes
e2fsattrs: yes
caps: no
Available hashsum attributes:
md5: yes
sha1: yes
sha256: yes
sha512: yes
rmd160: yes
tiger: no
crc32: no
crc32b: no
haval: no
whirlpool: no
gost: no

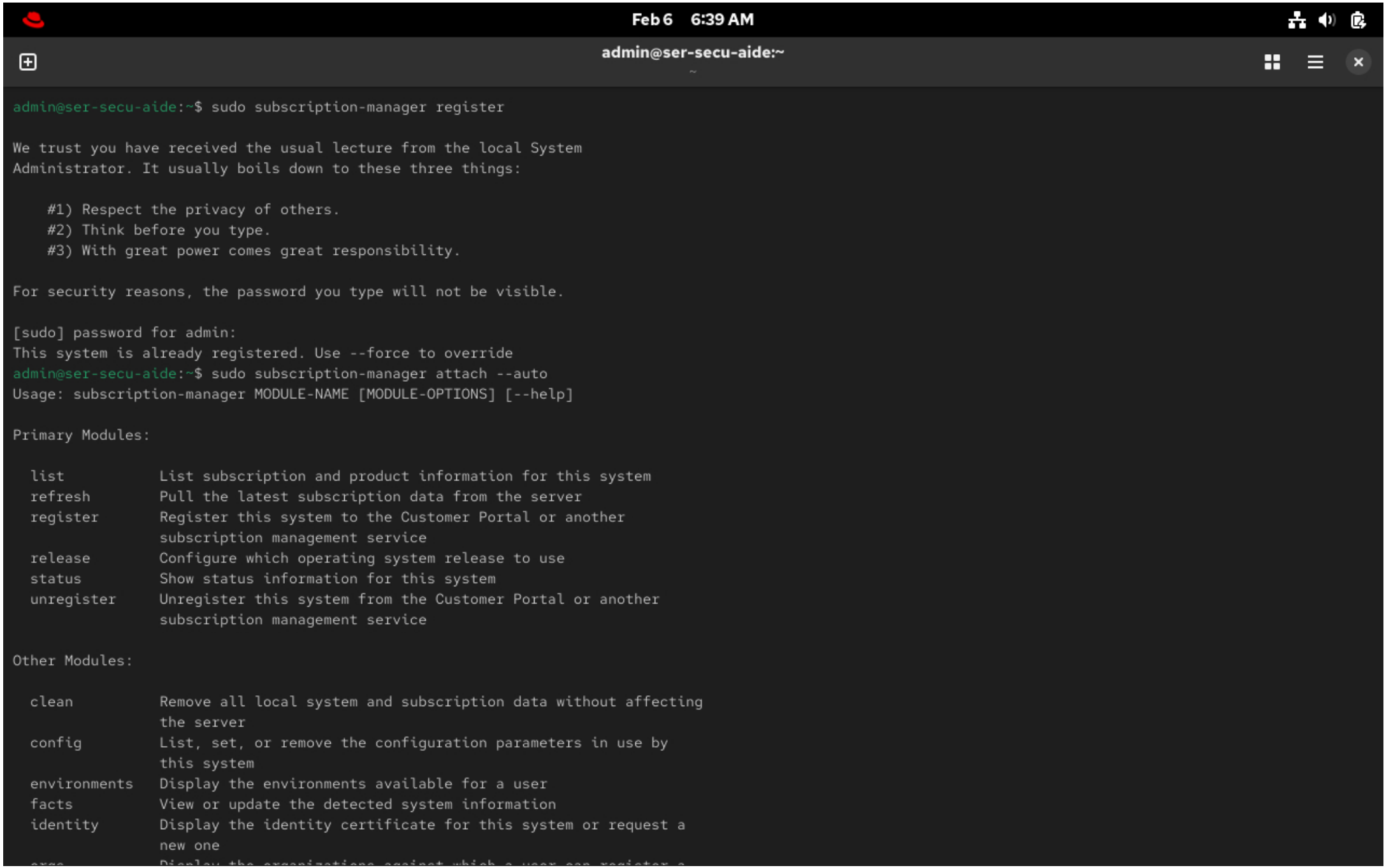

Feb 6 7:36 AM
admin@ser-secu-aide:~
~
Complete!
admin@ser-secu-aide:~$ aide --version
AIDE 0.18.6
Compile-time options:
use pcre2: mandatory
use pthread: yes
use zlib compression: yes
use POSIX ACLs: yes
use SELinux: yes
use xattr: yes
use POSIX 1003.1e capabilities: no
use e2fsattrs: yes
use cURL: yes
use Mhash: no
use GNU crypto library: no
use GnuTLS: yes
use Linux Auditing Framework: yes
use locale: no
syslog ident: aide
syslog logopt: LOG_CONS
syslog priority: LOG_NOTICE
default syslog facility: LOG_LOCAL0
Default config values:
config file: /etc/aide.conf
database_in: file:/etc/aide.db
database_out: file:/etc/aide.db.new
Available compiled-in attributes:
acl: yes
xattrs: yes
selinux: yes
e2fsattrs: yes
caps: no
Available hashsum attributes:
md5: yes
sha1: yes
sha256: yes
sha512: yes
rmd160: yes
tiger: no
crc32: no

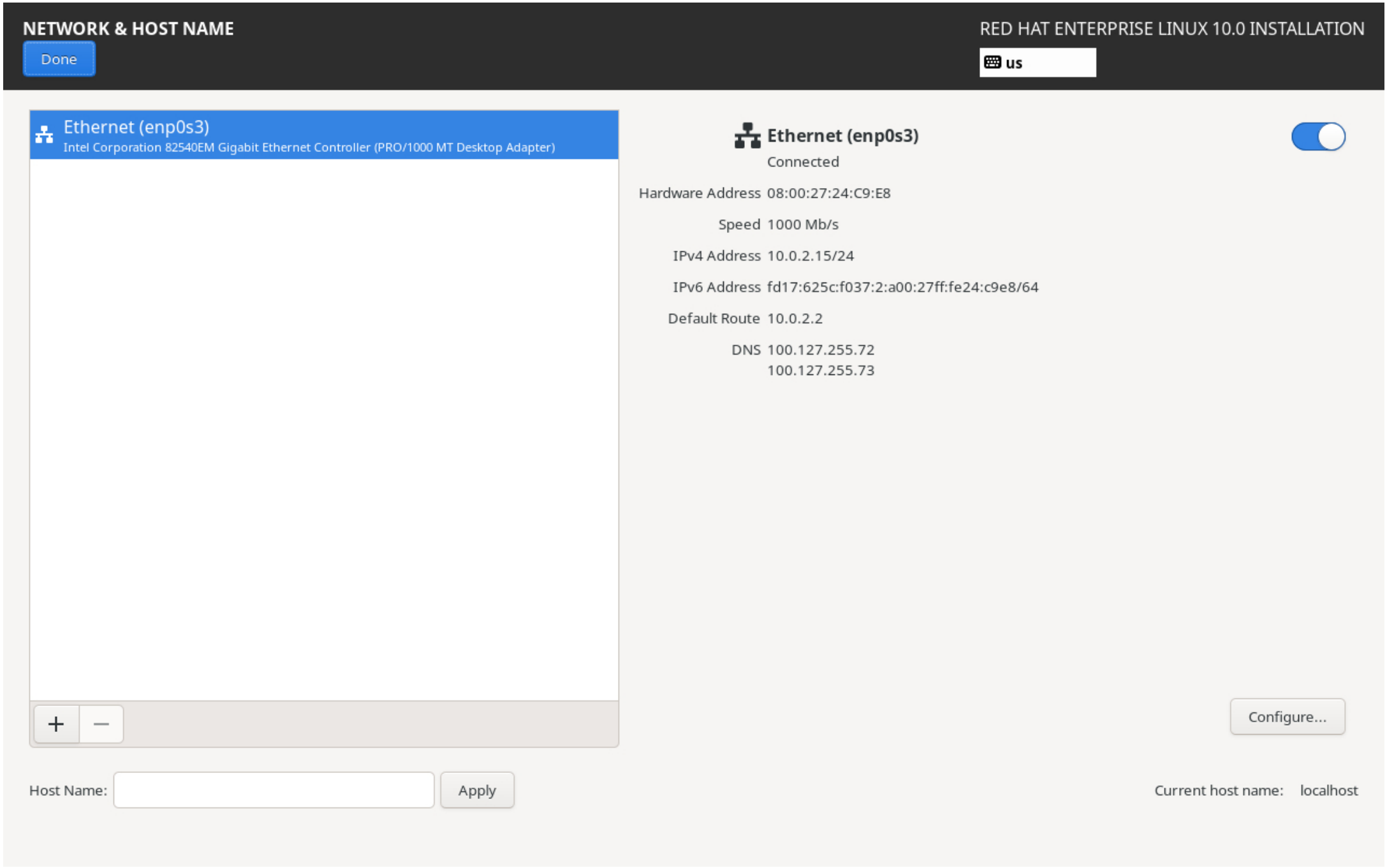

Feb 6 7:33 AM
admin@ser-secu-aide:~
Last metadata expiration check: 0:00:13 ago on Fri 06 Feb 2026 07:04:41 AM EST.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
aide x86_64 0.18.6-8.el10_1.2 rhel-10-for-x86_64-appstream-rpms 148 k
Transaction Summary
Install 1 Package
Total download size: 148 k
Installed size: 352 k
Downloading Packages:
aide-0.18.6-8.el10_1.2.x86_64.rpm 287 kB/s | 148 kB 00:00
Total 286 kB/s | 148 kB 00:00
Red Hat Enterprise Linux 10 for x86_64 - AppStream (RPMs) 3.6 MB/s | 3.7 kB 00:00
Importing GPG key 0xFD431D51:
Userid : "Red Hat, Inc. (release key 2) <security@redhat.com>"
Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
Userid : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : aide-0.18.6-8.el10_1.2.x86_64 1/1
Running scriptlet: aide-0.18.6-8.el10_1.2.x86_64 1/1
Installed products updated.
Installed:
aide-0.18.6-8.el10_1.2.x86_64
Complete!
admin@ser-secu-aide:~$

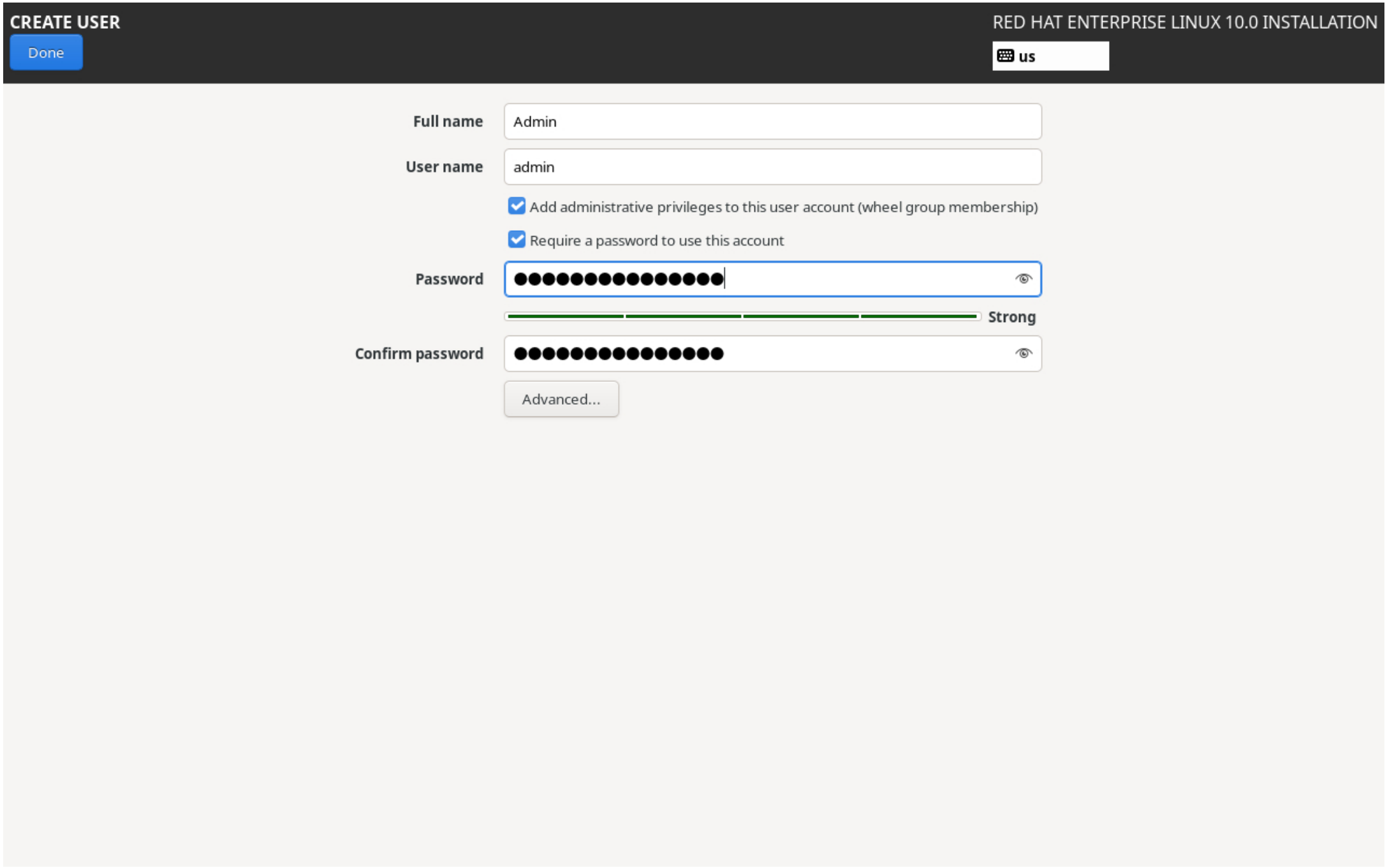

Feb 6 7:06 AM
admin@ser-secu-aide:~
admin@ser-secu-aide:~$ sudo dnf install aide -y
Updating Subscription Management repositories.
Last metadata expiration check: 0:00:13 ago on Fri 06 Feb 2026 07:04:41 AM EST.
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
aide x86_64 0.18.6-8.el10_1.2 rhel-10-for-x86_64-appstream-rpms 148 k
Transaction Summary
Install 1 Package
Total download size: 148 k
Installed size: 352 k
Downloading Packages:
aide-0.18.6-8.el10_1.2.x86_64.rpm 287 kB/s | 148 kB 00:00
Total 286 kB/s | 148 kB 00:00
Red Hat Enterprise Linux 10 for x86_64 - AppStream (RPMs) 3.6 MB/s | 3.7 kB 00:00
Importing GPG key 0xFD431D51:
Userid : "Red Hat, Inc. (release key 2) <security@redhat.com>"
Fingerprint: 567E 347A D004 4ADE 55BA 8A5F 199E 2F91 FD43 1D51
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Importing GPG key 0x5A6340B3:
Userid : "Red Hat, Inc. (auxiliary key 3) <security@redhat.com>"
Fingerprint: 7E46 2425 8C40 6535 D56D 6F13 5054 E4A4 5A63 40B3
From : /etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Key imported successfully
Running transaction check
Transaction check succeeded.
Running transaction test
Transaction test succeeded.
Running transaction
Preparing : 1/1
Installing : aide-0.18.6-8.el10_1.2.x86_64 1/1
Running scriptlet: aide-0.18.6-8.el10_1.2.x86_64 1/1
Installed products updated.
Installed:
aide-0.18.6-8.el10_1.2.x86_64
Complete!

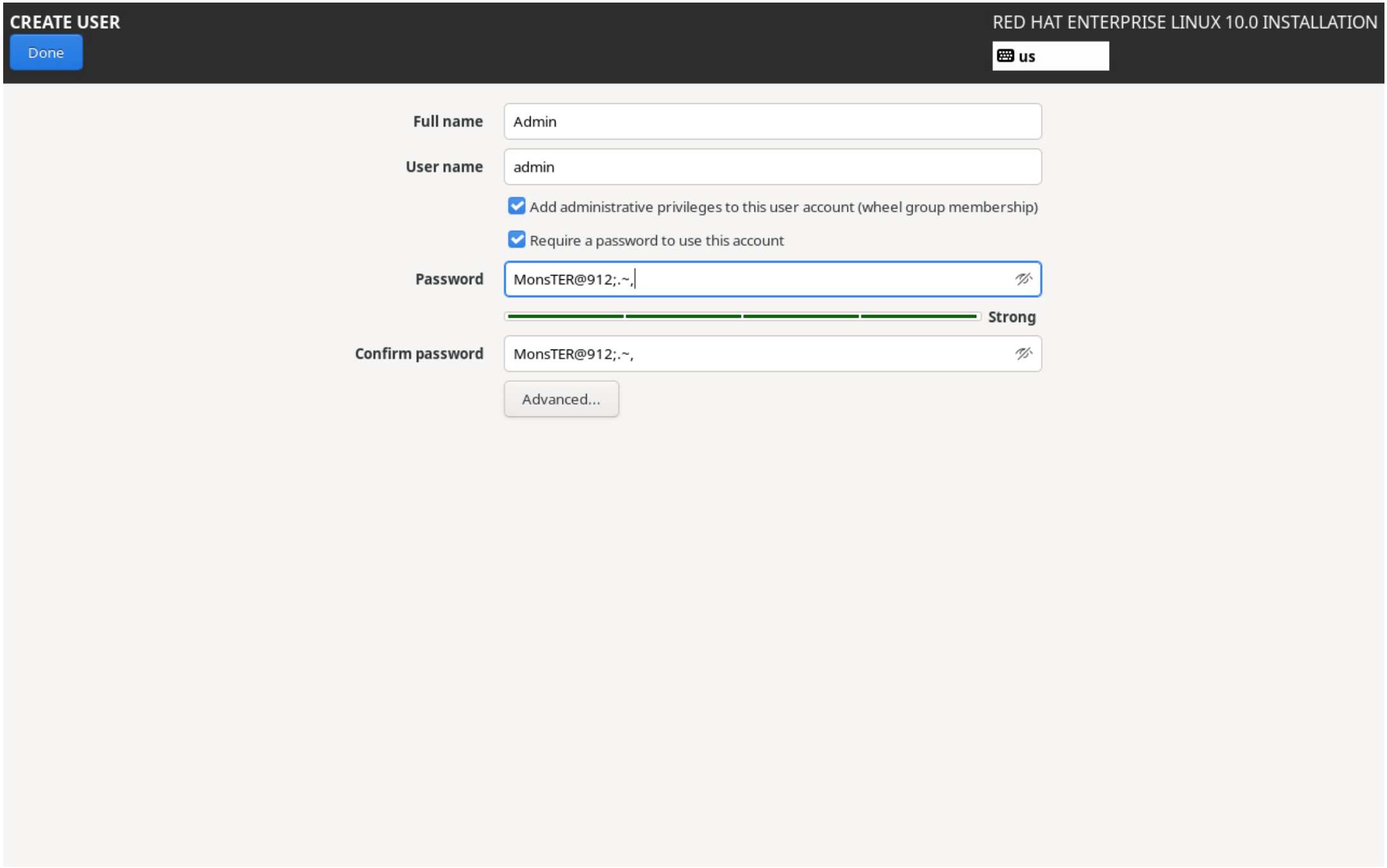

Feb 6 6:58 AM
admin@ser-secu-aide:~
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'dnf clean packages'.
Traceback (most recent call last):
File "/bin/dnf", line 62, in <module>
main.user_main(sys.argv[1:], exit_code=True)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 208, in user_main
errcode = main(args)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 67, in main
return _main(base, args, cli_class, option_parser_class)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 106, in _main
return cli_run(cli, base)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 130, in cli_run
ret = resolving(cli, base)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 183, in resolving
base.do_transaction(display=displays)
File "/usr/lib/python3.12/site-packages/dnf/cli/cli.py", line 276, in do_transaction
self.gpgsigcheck(install_pkgs)
File "/usr/lib/python3.12/site-packages/dnf/cli/cli.py", line 332, in gpgsigcheck
self._get_key_for_package(po, fn)
File "/usr/lib/python3.12/site-packages/dnf/base.py", line 2555, in _get_key_for_package
keys = dnf.crypto.retrieve(keyurl, repo)
File "/usr/lib/python3.12/site-packages/dnf/crypto.py", line 137, in retrieve
keyinfos = rawkey2infos(handle)
File "/usr/lib/python3.12/site-packages/dnf/crypto.py", line 127, in rawkey2infos
keys = libdnf.repo.Key.keysFromFd(key_fo.fileno())
File "/usr/lib64/python3.12/site-packages/libdnf/repo.py", line 341, in keysFromFd
return _repo.Key_keysFromFd(fileDescriptor)
RuntimeError: Parsing armored OpenPGP packet(s) failed
admin@ser-secu-aide:~$


Feb 6 6:58 AM
admin@ser-secu-aide:~
syspurpose Convenient module for managing all system purpose settings
version Print version information
admin@ser-secu-aide:~$ sudo dnf repo-list
Updating Subscription Management repositories.
No such command: repo-list. Please use /bin/dnf --help
It could be a DNF plugin command, try: "dnf install 'dnf-command(repo-list)'"
admin@ser-secu-aide:~$ sudo dnf install aide -y
[sudo] password for admin:
Updating Subscription Management repositories.
Red Hat Enterprise Linux 10 for x86_64 - BaseOS (RPMs) 14 MB/s | 44 MB 00:03
Red Hat Enterprise Linux 10 for x86_64 - AppStream (RPMs) 3.9 MB/s | 4.3 MB 00:01
Dependencies resolved.
Package Architecture Version Repository Size
Installing:
aide x86_64 0.18.6-8.el10_1.2 rhel-10-for-x86_64-appstream-rpms 148 k
Transaction Summary
Install 1 Package
Total download size: 148 k
Installed size: 352 k
Downloading Packages:
aide-0.18.6-8.el10_1.2.x86_64.rpm 320 kB/s | 148 kB 00:00
Total 319 kB/s | 148 kB 00:00
Red Hat Enterprise Linux 10 for x86_64 - AppStream (RPMs) 3.6 MB/s | 3.7 kB 00:00
The downloaded packages were saved in cache until the next successful transaction.
You can remove cached packages by executing 'dnf clean packages'.
Traceback (most recent call last):
File "/bin/dnf", line 62, in <module>
main.user_main(sys.argv[1:], exit_code=True)
File "/usr/lib/python3.12/site-packages/dnf/cli/main.py", line 208, in user_main
errcode = main(args)
^^^^^^^^^^


Feb 6 6:39 AM
admin@ser-secu-aide:~
admin@ser-secu-aide:~$ sudo subscription-manager register
We trust you have received the usual lecture from the local System
Administrator. It usually boils down to these three things:
#1) Respect the privacy of others.
#2) Think before you type.
#3) With great power comes great responsibility.
For security reasons, the password you type will not be visible.
[sudo] password for admin:
This system is already registered. Use --force to override
admin@ser-secu-aide:~$ sudo subscription-manager attach --auto
Usage: subscription-manager MODULE-NAME [MODULE-OPTIONS] [--help]
Primary Modules:
list List subscription and product information for this system
refresh Pull the latest subscription data from the server
register Register this system to the Customer Portal or another
subscription management service
release Configure which operating system release to use
status Show status information for this system
unregister Unregister this system from the Customer Portal or another
subscription management service
Other Modules:
clean Remove all local system and subscription data without affecting
the server
config List, set, or remove the configuration parameters in use by
this system
environments Display the environments available for a user
facts View or update the detected system information
identity Display the identity certificate for this system or request a
new one


NETWORK & HOST NAME
Done
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
Ethernet (enp0s3)
Intel Corporation 82540EM Gigabit Ethernet Controller (PRO/1000 MT Desktop Adapter)
Ethernet (enp0s3)
Connected
Hardware Address 08:00:27:24:C9:E8
Speed 1000 Mb/s
IPv4 Address 10.0.2.15/24
IPv6 Address fd17:625c:f037:2:a00:27ff:fe24:c9e8/64
Default Route 10.0.2.2
DNS 100.127.255.72
100.127.255.73
Configure...
Host Name:
Apply
Current host name: localhost


CREATE USER
Done
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
Full name
Admin
User name
admin
Add administrative privileges to this user account (wheel group membership)
Require a password to use this account
Password
Strong
Confirm password
Advanced...


CREATE USER
Done
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
Full name
Admin
User name
admin
Add administrative privileges to this user account (wheel group membership)
Require a password to use this account
Password
MonsTER@912;.~,
Strong
Confirm password
MonsTER@912;.~,
Advanced...

The root account is used for administering the system.

The root user (also known as super user) has complete access to the entire system. For this reason, logging into this system as the root user is best done only to perform system maintenance or administration.

Disable root account

Disabling the root account will lock the account and disable remote access with root account. This will prevent unintended administrative access to the system.

Enable root account

Enabling the root account will allow you to set a root password and optionally enable remote access to root account on this system.

Root Password: ●●●●●●●●●●●

Strong

Confirm: ●●●●●●●●●●●

Allow root SSH login with password

The root account is used for administering the system.

The root user (also known as super user) has complete access to the entire system. For this reason, logging into this system as the root user is best done only to perform system maintenance or administration.

Disable root account

Disabling the root account will lock the account and disable remote access with root account. This will prevent unintended administrative access to the system.

Enable root account

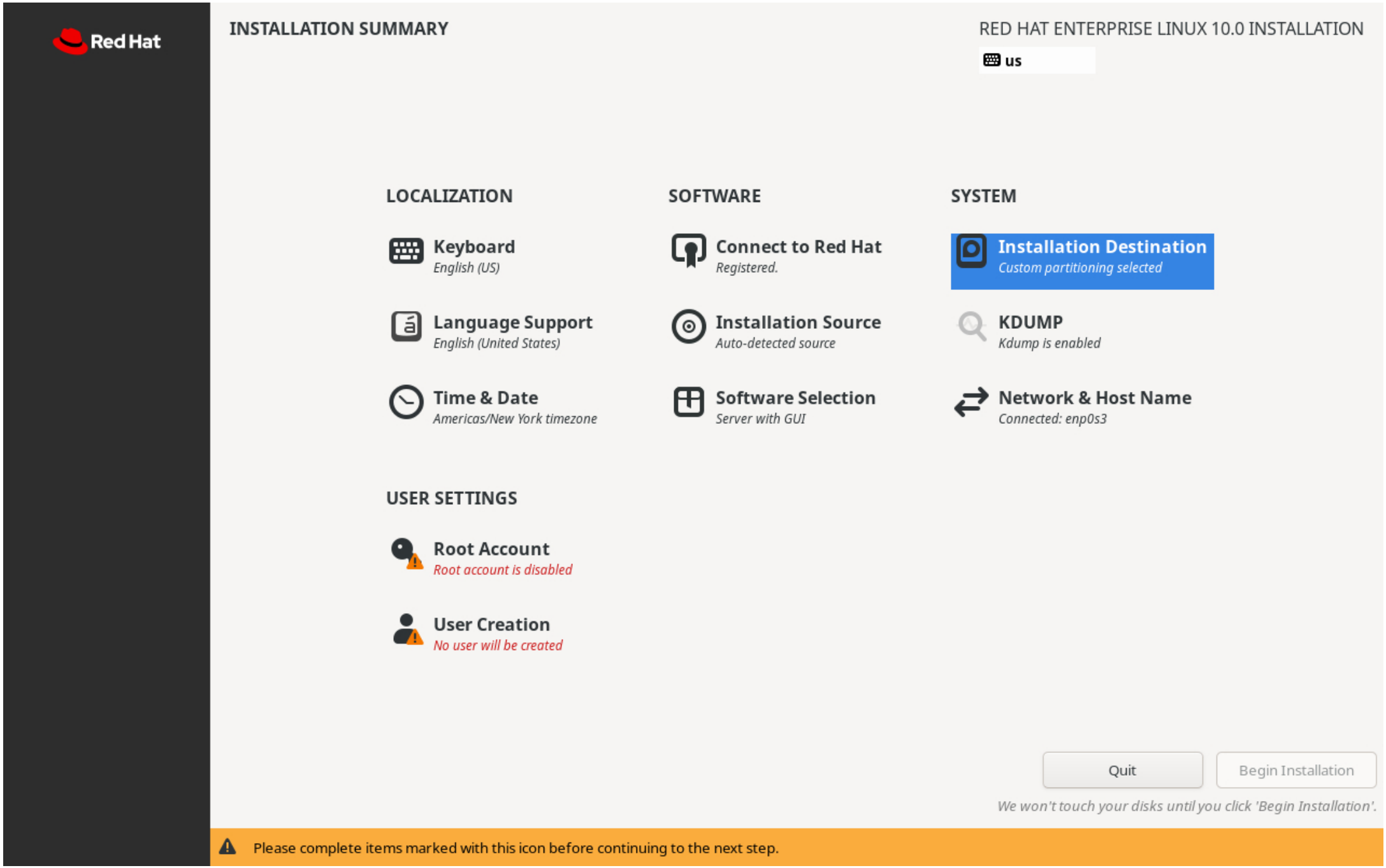
Enabling the root account will allow you to set a root password and optionally enable remote access to root account on this system.

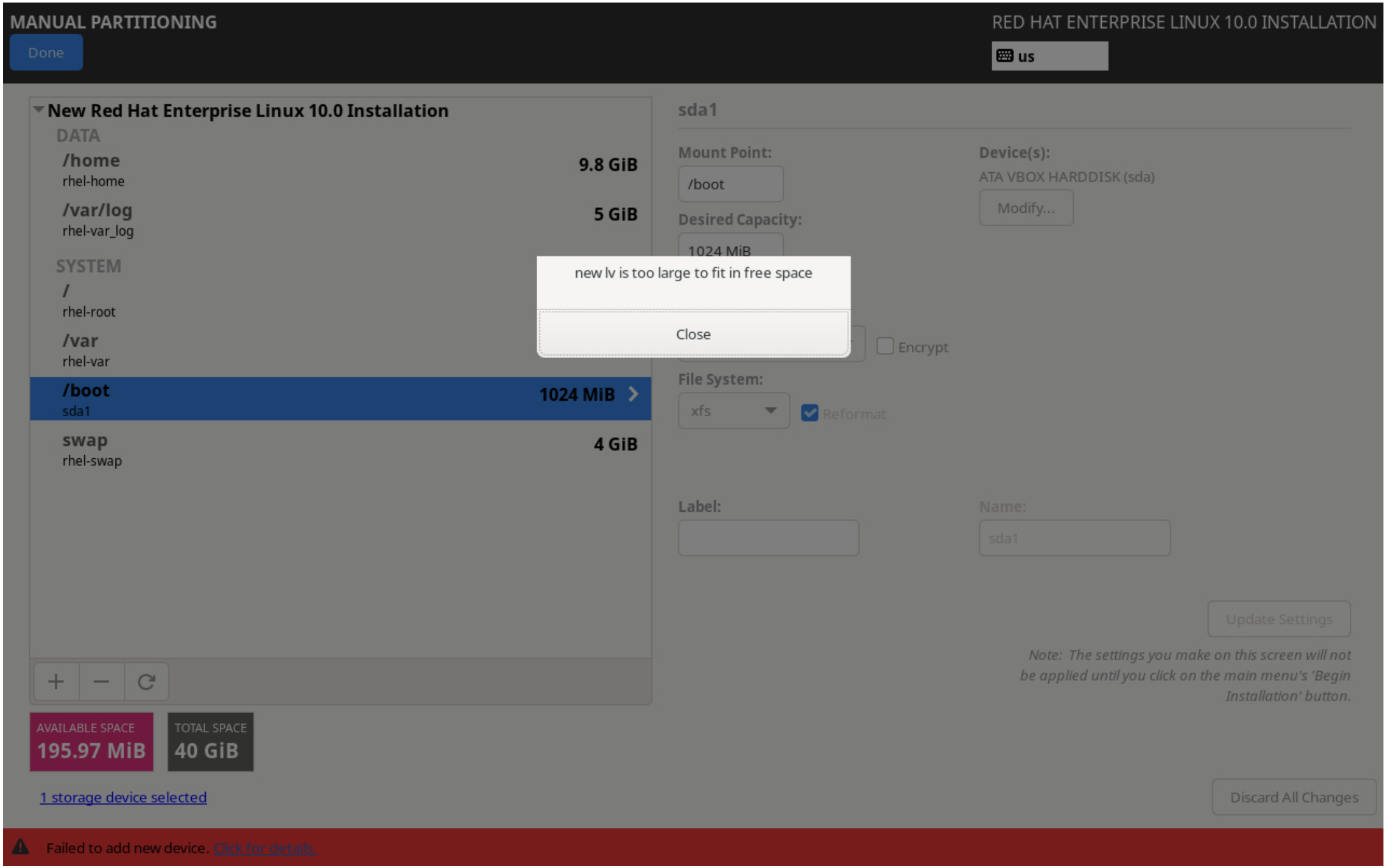
Root Password: AdmIN@99;.~,

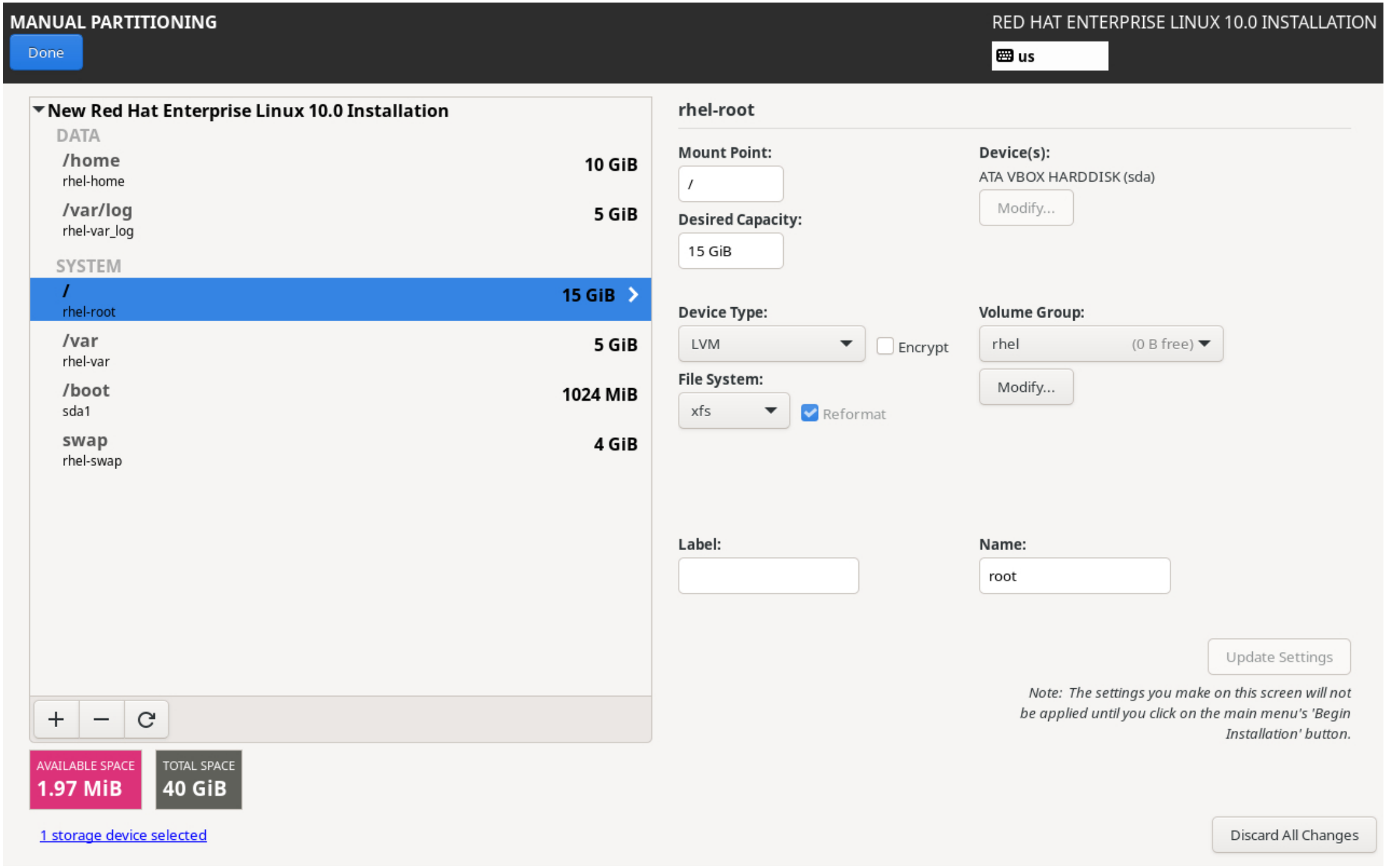
Strong

Confirm: AdmIN@99;.~,

Allow root SSH login with password


Red Hat
INSTALLATION SUMMARY
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
LOCALIZATION
Keyboard
English (US)
Language Support
English (United States)
Time & Date
Americas/New York timezone
SOFTWARE
Connect to Red Hat
Registered.
Installation Source
Auto-detected source
Software Selection
Server with GUI
SYSTEM
Installation Destination
Custom partitioning selected
KDUMP
Kdump is enabled
Network & Host Name
Connected: enp0s3
USER SETTINGS
Root Account
Root account is disabled
User Creation
No user will be created
Quit
Begin Installation
We won't touch your disks until you click 'Begin Installation'.
Please complete items marked with this icon before continuing to the next step.


MANUAL PARTITIONING
Done
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
New Red Hat Enterprise Linux 10.0 Installation
DATA
/home
rhel-home
9.8 GiB
/var/log
rhel-var_log
5 GiB
SYSTEM
/
rhel-root
/var
rhel-var
/boot
sda1
1024 MiB
swap
rhel-swap
4 GiB
AVAILABLE SPACE
195.97 MiB
TOTAL SPACE
40 GiB
1 storage device selected
sda1
Mount Point:
/boot
Device(s):
ATA VBOX HARDDISK (sda)
Modify...
Desired Capacity:
1024 MiB
new lv is too large to fit in free space
Close
Encrypt
File System:
xfs
Reformat
Label:
Name:
sda1
Update Settings
Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.
Discard All Changes
Failed to add new device. Click for details.


MANUAL PARTITIONING
Done
RED HAT ENTERPRISE LINUX 10.0 INSTALLATION
us
New Red Hat Enterprise Linux 10.0 Installation
DATA
/home
rhel-home
10 GiB
/var/log
rhel-var_log
5 GiB
SYSTEM
/
rhel-root
15 GiB
/var
rhel-var
5 GiB
/boot
sda1
1024 MiB
swap
rhel-swap
4 GiB
AVAILABLE SPACE
1.97 MiB
TOTAL SPACE
40 GiB
1 storage device selected
rhel-root
Mount Point:
/
Desired Capacity:
15 GiB
Device(s):
ATA VBOX HARDDISK (sda)
Modify...
Device Type:
LVM
Encrypt
File System:
xfs
Reformat
Volume Group:
rhel
(0 B free)
Modify...
Label:
Name:
root
Update Settings
Note: The settings you make on this screen will not be applied until you click on the main menu's 'Begin Installation' button.
Discard All Changes