, FreeIPA

-
- FreeIPA
- FreeIPA
- FreeIPA
  -
  -
-
  - web- FreeIPA
- FreeIPA

:

- Astra Linux Special Edition .10015-01 (1.7), .10015-10
- Astra Linux Special Edition .10015-17
- Astra Linux Special Edition .10015-37 (7.7)
- Astra Linux Special Edition .10015-03 (7.6)
- Astra Linux Special Edition .10152-02 (4.7)
- Astra Linux Special Edition .10015-01 (1.6)
- Astra Linux Special Edition .10015-16 . 1
- Astra Linux Special Edition .10015-16 . 2
- Astra Linux Special Edition .10265-01 (8.1)
- Astra Linux Common Edition 2.12

. , .

, , , . .

DogTag:

- - p12 ;
- , /etc/ssl/freeipa . .

FreeIPA

(-) FreeIPA ipa-backup (freeipa-server). ipa-backup:

- :
  - . FreeIPA ( );
  - . FreeIPA;
- GPG- root . ;
- /var/lib/ipa/backup:
  - ipa-full-YEAR-MM-DD-HH-MM-SS (GMT);
  - ipa-data-YEAR-MM-DD-HH-MM-SS (GMT);
- header. :

```
[ipa]
type = FULL
time = 2021-09-22T14:03:50
host = ipa0.ipadomain0.ru
ipa_version = 4.6.4
version = 1
services = NTP,KDC,KPASSWD,KEYS,OTPD,HTTP,DNS,DNSKeySync,ADTRUST,EXTID
```

header :

  - ( );
  - ;
  - ;
  - FreeIPA;
  - ;
  - , .
- , , ;
- FreeIPA.

:

```
sudo ipa-backup
```

```
Preparing backup on ipa0.ipadomain0.ru
Stopping IPA services
```

```
Backing up userRoot in IPADOMAIN0-RU to LDIF
Backing up IPADOMAIN0-RU
Backing up files
Backed up to /var/lib/ipa/backup/ipa-full-2021-09-22-17-04-02
Starting IPA service
The ipa-backup command was successful
```

FreeIPA

. , :

- 10.0.20.0/24;
- ipa0.ipadomain0.ru ipa1.ipadomain0.ru (IP- 10.0.2.22);
- ipa1.ipadomain0.ru .

- DogTag: p12 . . , ;
- DogTag , , , , .

- ipa0.ipadomain0.ru:
  - :

    ```
    sudo ipa-replica-manage del ipa1.ipadomain0.ru
    ```

  - , DNS- . "SRV record", "A record", "NS record":

    ```
    ipa dnsrecord-find ipadomain0.ru | egrep "(SRV|A|NS) record:"
    ```

    - , - web- FreeIPA;

  - "PTR" :

    ```
    ipa dnsrecord-add 20.0.10.in-addr.arpa. 22 --ptr-rec ipa1.
    ipadomain0.ru.
    ```

    22 - ;

- :
  - ;
  - (Astra Linux Special Edition -);
  - (FQDN) , ;
  - , ;
  - ;
  - ;
  - ;
  - (DogTag - p12 . . FreeIPA:). :
    - DogTag:

      ```
      sudo astra-freeipa-replica -a ipa1.ipadomain0.ru-200305-
      142302.p12 --pin 12345678
      ```

    - DogTag:

      ```
      sudo astra-freeipa-replica --dogtag
      ```

FreeIPA

, , . :

```
sudo ipa-restore ipa-full-2021-09-22-17-04-02/
```

```
Directory Manager (existing master) password:

Preparing restore from /var/lib/ipa/backup/ipa-full-2021-09-22-17-04-02/ on
ipa0.ipadomain0.ru
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data.
Continue to restore? [no]: yes
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Stopping IPA services
Configuring certmonger to stop tracking system certificates for CA
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in IPADOMAIN0-RU
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

, :

```
sudo ipa-restore /var/lib/ipa/backup/ipa-full-2021-09-22-17-04-02/
```

FreeIPA :

- ;
- (Astra Linux Special Edition -);
- (FQDN) , ;
- , ;
- FreeIPA FreeIPA Astra Linux;
- ;
- (Astra Linux Special Edition -);

  .

- . - ;
- . FreeIPA :

  ```
  sudo ipa-restore /var/lib/ipa/backup/ipa-full-2021-09-22-17-04-02/
  ```

  ```
  Directory Manager (existing master) password:
  ```

```
Preparing restore from /var/lib/ipa/backup/ipa-full-2021-09-22-17-04-
02/ on ipa0.ipadomain0.ru
Performing FULL restore from FULL backup
Temporary setting umask to 022
Restoring data will overwrite existing live data.
Continue to restore? [no]: yes
Each master will individually need to be re-initialized or
re-created from this one. The replication agreements on
masters running IPA 3.1 or earlier will need to be manually
re-enabled. See the man page for details.
Disabling all replication.
Stopping IPA services
Configuring certmonger to stop tracking system certificates for CA
Systemwide CA database updated.
Restoring files
Systemwide CA database updated.
Restoring from userRoot in IPADOMAIN0-RU
Restarting GSS-proxy
Starting IPA services
Restarting SSSD
Restarting oddjobd
Restoring umask to 18
The ipa-restore command was successful
```

- ;
- , ;

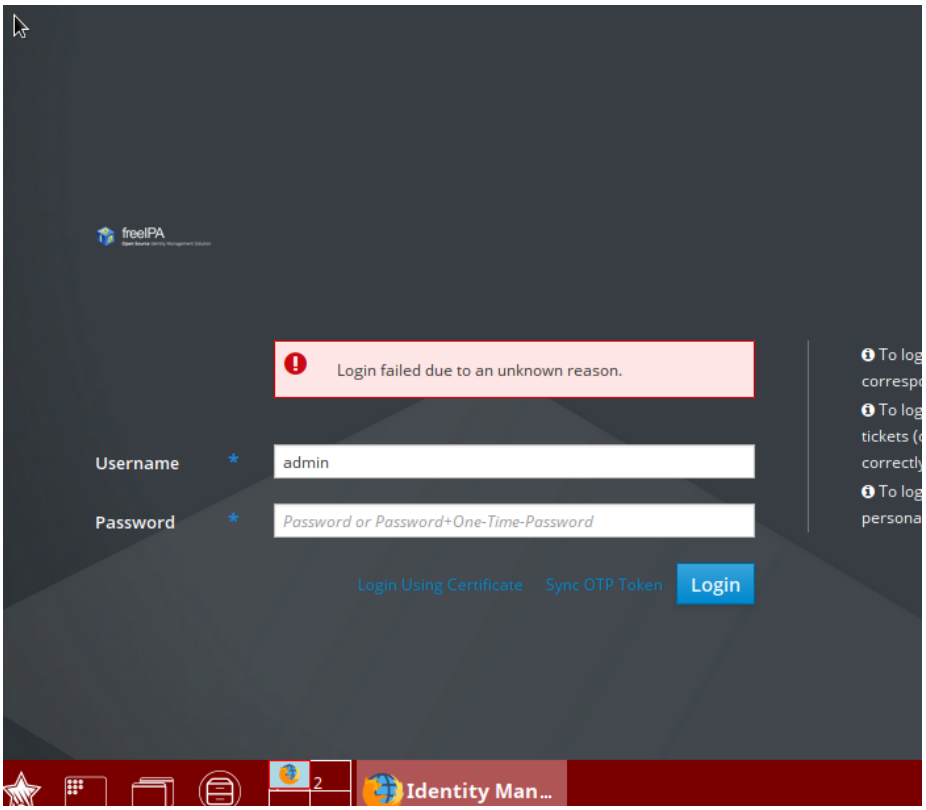
- .
.

, , :

```
kinit admin
ipa user-find
ipa host-find
ipa server-find
```

web- FreeIPA

web- FreeIPA "Login failed due to an unknown reason":



/var/log/syslog :

```
... named-pkcs11[929]: LDAP error: Can't contact LDAP server: bind to LDAP server failed
```

(/etc/resolv.conf) , IP- .

FreeIPA

FreeIPA :

- Astra Linux Common Edition:

  ```
  sudo apt dist-upgrade
  ```

- Astra Linux Special Edition . , . astra-update (fly-astra-update).

ipa-server-upgrade .