

HBAC FreeIPA

- [HBAC](#)
-
-
-



:

- 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

HBAC (Host-based access control) — . :

- ssh ;
- .



. .



FreeIPA allow_all, .



FreeIPA gidNumber. , HBAC , .

HBAC

, HBAC, web- FreeIPA Policy — Host-Based Access Control — HBAC Services. , ftp, sshd, su, login.



fly-dm fly-wm.

HBAC Services

Search

Q

Refresh

Delete

+ Add

☐	Service name	Description
☐	crond	crond
☐	ftp	ftp
☐	gdm	gdm
☐	gdm-password	gdm-password
☐	gssftp	gssftp
☐	kdm	kdm
☐	login	login
☐	proftpd	proftpd
☐	pure-ftpd	pure-ftpd
☐	sshd	sshd
☐	su	su
☐	su-l	su with login shell
☐	sudo	sudo
☐	sudo-i	sudo-i
☐	vsftpd	vsftpd

Showing 1 to 15 of 15 entries.

Policy — Host-Based Access Control — HBAC Rules Add, , Add and Edit. :

1. / , .
2. / , .
3. / , .

Who

User category the rule applies to: ☐ Anyone ☒ Specified Users and Groups

☐ Users

Delete Add

☐ User Groups

Delete Add

☐ admins

Accessing

Host category the rule applies to: ☐ Any Host ☒ Specified Hosts and Groups

☐ Hosts

Delete Add

☐ Host Groups

Delete Add

☐ ipaservers

Via Service

Service category the rule applies to: ☒ Any Service ☐ Specified Services and Groups

☐ Services

Delete Add

☐ Service Groups

Delete Add

, , , , , .
 , .

Policy — Host-Based Access Control — HBAC Test:

1. FreeIPA, , Next.

Who

Accessing

Via Service

Rules

Run Test

WHO

User login	First name	Last name	Status
☐ admin	admin	admin	✓ Enabled
☒ admin	admin	admin	✓ Enabled
☐ admin	admin	admin	✓ Enabled
☐ admin	admin	admin	✓ Enabled
☐ admin	admin	admin	✓ Enabled
☐ admin	admin	admin	✓ Enabled

Showing 1 to 6 of 6 entries.

☐ Specify external User:

Next

2. FreeIPA, , Next.

Who

Accessing

Via Service

Rules

Run Test

ACCESSING

Host name	Description	Enrolled
☒ 192.168.1.100		True

Showing 1 to 1 of 1 entries.

☐ Specify external Host:

PrevNext

3. , , Next.

Via Service

Who

Accessing

Via Service

Rules

Run Test

VIA SERVICE

Service name	Description
☐ crond	crond
☐ ftp	ftp
☐ gdm	gdm
☐ gdm-password	gdm-password
☐ gssftp	gssftp
☐ kdm	kdm
☐ login	login
☐ postfixd	postfixd
☐ pure-ftpd	pure-ftpd
☒ sshd	sshd
☐ su	su
☐ sudo	su with login shell
☐ sudo-i	sudo-i
☐ vsftpd	vsftpd

Showing 1 to 15 of 15 entries.

☐ Specify external HBAC Service:

PrevNext

4. , , Next.

Rules

Who

Accessing

Via Service

Rules

Run Test

RULES

☐ Include Enabled ☐ Include Disabled

Rule name	Status	Description
☐ allow_admins_to_servers	✔ Enabled	Allow members of a group admins to access any server via any service.
☐ allow_all	✔ Enabled	Allow all users to access any host from any host
☐ allow_freeipa_admins_to_freeipa_servers	✔ Enabled	Allow members of a group freeipa_admins to access any freeipa server via any service.
☐ allow_users_to_workstations	✔ Enabled	Allow members of a group ipausers to access any workstation via any service.

Showing 1 to 4 of 4 entries.

< Prev

> Next

5. (). Run Test.

Run Test

Who

Accessing

Via Service

Rules

Run Test

Run Test

RULES

☒ Matched ☒ Unmatched

Rule name	Matched	Status	Description
-----------	---------	--------	-------------

< Prev New Test >

6. , (,) . .

Run Test

Who

Accessing

Via Service

Rules

Run Test

Run Test

ACCESS GRANTED

RULES

☒ Matched ☒ Unmatched

Rule name	Matched	Status	Description
allow_admins_to_servers	True	✔ Enabled	Allow members of a group admins to access any server via any service.
allow_freeipa_admins_to_freeipa_servers	True	✔ Enabled	Allow members of a group freeipa_admins to access any freeipa server via any service.
allow_users_to_workstations		✔ Enabled	Allow members of a group ipausers to access any workstation via any service.

Showing 1 to 3 of 3 entries.

< Prev

New Test

Disable, — Delete:

HBAC Rules

Search

Q

Refresh

Delete

+ Add

— Disable

✔ Enable

☐	Rule name	Status	Description
☒	allow_admins_to_servers	✔ Enabled	Allow members of a group server-administrators to access to host group server via any service.
☐	allow_all	— Disabled	Allow all users to access any host from any host
☐	allow_freeipa_admins_to_freeipa_servers	✔ Enabled	Allow members of a group freeipa_admins to access any freeipa server via any service.
☐	allow_kdobrinin_to_003	— Disabled	
☐	allow_users_to_workstations	✔ Enabled	Allow members of a group ipausers to access any workstation via any service.
☐	allow_zimbra_backup_group_to_mail01	✔ Enabled	Allow group zimbra_editors access to rbta-msk-vsrv-mail01 via ssh

Showing 1 to 6 of 6 entries.