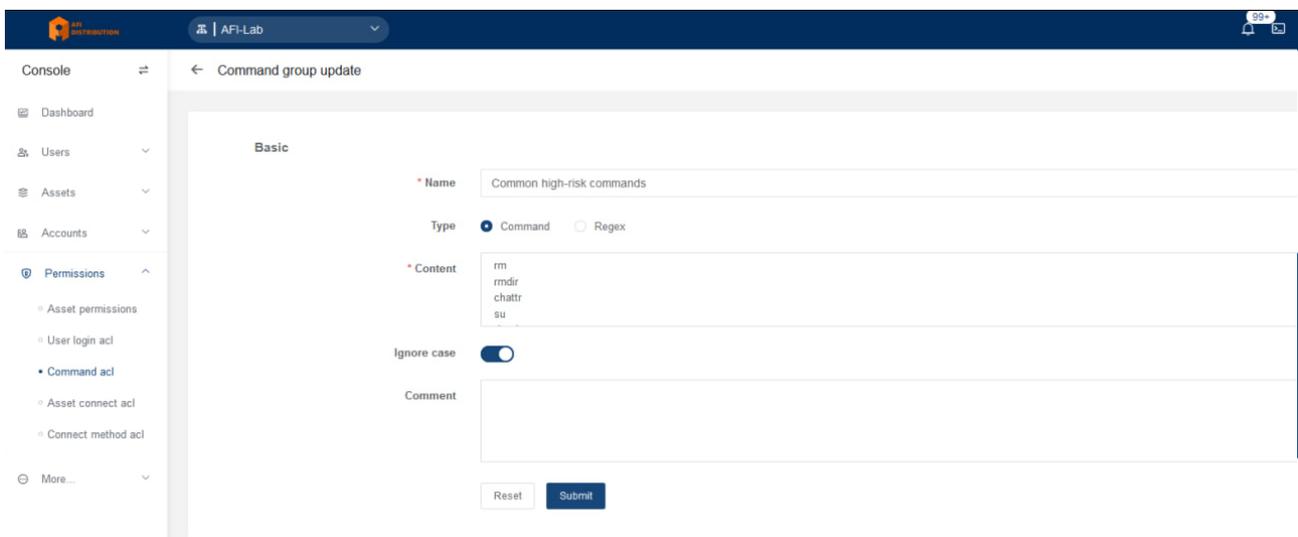


Command filter configuration for SSH and database queries

Command ACL Configuration

1. Go to the "**Console - Policies - ACLs - Command filter**" section and open the "**Command Group**" tab.
2. Click the "**Create**" button, enter a name for the list, such as "**Common high-risk commands**", and fill in the list with the required commands or regular expressions (see the screenshot). Save it by clicking the "**Submit**" button.



The screenshot shows the 'Command group update' configuration page in the JumpServer web interface. The page is titled 'Basic' and contains the following fields:

- Name:** Common high-risk commands
- Type:** Command Regex
- Content:** rm, rmdir, chmod, su
- Ignore case:**
- Comment:** (empty)

At the bottom of the form, there are two buttons: 'Reset' and 'Submit'.

3. Open the "**Command filter**" tab and click "**Create**" to create a filter.
4. The filter configuration includes the following parameters:
 - **Priority:** the filter priority. The action of the filter with the highest priority will always be executed.
 - **User:** JumpServer users for whom the filter will apply.
 - **Asset:** target systems where the filter will control connections.
 - **Account:** accounts on target systems that will be controlled by the filter.
 - **Command Group:** groups of commands that will be blocked.
 - **Action:** the filter action: **Reject** - block the command, **Accept** - execute the command, **Review** - send the command for approval by a specified employee, **Warning** - warn the specified employee about executing the command.

Console

- Dashboard
- Users
- Assets
- Accounts
- Permissions
 - Asset permissions
 - User login acl
 - Command acl
 - Asset connect acl
 - Connect method acl
 - More...

AFI-Lab

Basic

* Name: Common high-risk commands

Priority: 50
1-100, the lower the value will be match first

User

* User: AllUsers SpecificUsers Select By Attribute

Попцов Сергей(sergey) x Наталия Орлова(nlo) x

Asset

* Asset: AllAsset SpecificAsset Select By Attribute

JumpServer22(10.10.53.22) x

Account

* Account: All accounts Specify account

Command group

Command group: Common high-risk commands x

Action

Action: Reject Accept Review Warning

5. Click **"Submit"** to save the settings.

Версия #1

Сергей Попцов создал 21 января 2025 11:43:14

Сергей Попцов обновил 21 января 2025 11:47:46