New issue

Can add custom ports without permission #443



Fabrimat commented on Apr 24, 2021 • edited ▼

Bug Report

System Information

- Operating System 4.19.0-16-amd64 SMP Debian 4.19.181-1 (2021-03-19) x86_64 GNU/Linux
- AMP version and build date v2.1.0.14, built 08/04/2021 18:11
- Which AMP release stream you're using Mainline

I confirm:

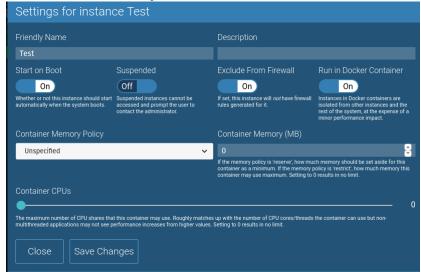
- that I have searched for an existing bug report for this issue.
- $\ensuremath{{\ensuremath{\square}}}$ that I am using the latest available version of AMP.
- that my operating system is up-to-date.

Symptoms

- What are you trying to do?
 Editing ports of an istance without having the proper permission
- What are you expecting to happen?
 That it gives me an error
- What is actually happening? ('Nothing' is not an acceptable answer!)
 The port is added without saying anything

Reproduction

1. I created a Minecraft instance with those settings



Jump to bottom

2. Created a Test user with the following permissions (the user is not member of any group)

Permissions for Test
User specific permissions for Test
This role is shared across all instances.

B Settings
Which Settings users in this role have permission to change the value of

B AMP Instance Manager

B File Manager

B Local File Backup

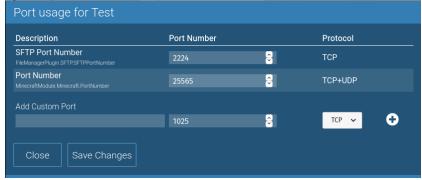
B AMPCore
Core functionality built into AMP itself

B All Instances

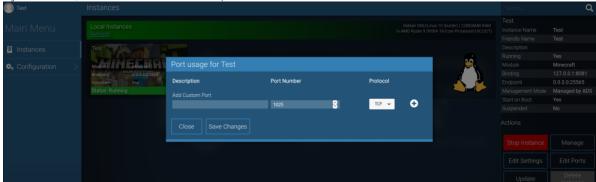
B All Instances

C Test

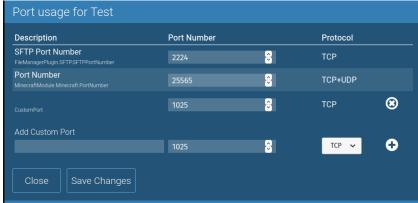
3. Login with a super admin and check the instance ports



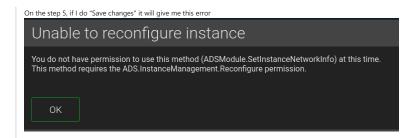
4. Login with the Test user, click on the Minecraft Instance and then "Edit ports"



- 5. Click on the "+" in the dialog and then "Close"
- 6. Check again the ports with the super admin



7. A new port has been added



PhonicUK commented on Apr 28, 2021 • edited ▼

Contributor

Clicking + doesn't actually add the port, the network changes aren't applied until you actually hit "Save". If you fully reload the page they won't be there.

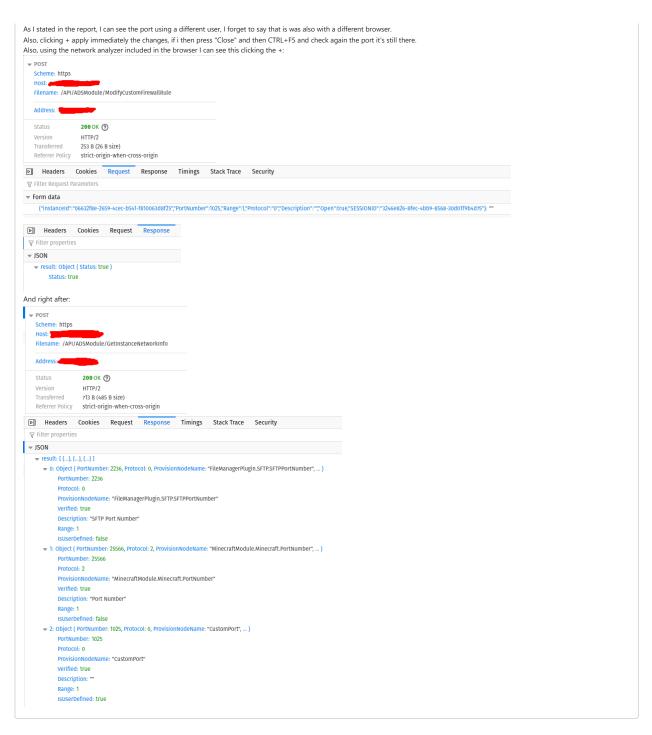
It might be incorrectly showing that they're in the list (and it shouldn't be showing the option to edit ports if you don't have permission) - but I can verify that the security model is operating correctly and the changes are not being applied when the user doesn't have permission. Indeed as it says, the API call to set the network information (the ports) requires the global Reconfigure permission for ADS.

So while it's a tad confusing that the user can even see that dialog when they won't be able to make any changes, the security model is operating as intended and there is no fault.

PhonicUK closed this as completed on Apr 28, 2021

Fabrimat commented on Apr 28, 2021 • edited ↓

Author



PhonicUK reopened this on Apr 30, 2021

PhonicUK commented on Apr 30, 2021

Contributor

Aah, there was a change at one point where the + and - didn't actually make the changes, indeed you're right and at the moment they do. Different API calls in that situation. Turns out,

ModifyCustomFirewallRule was missing the metadata for it's permissions because originally it wasn't exposed to the web. Not a huge issue since you'd have to at least be logged in, but this will be
patched immediately.

PhonicUK closed this as completed on Apr 30, 2021

- PhonicUK added core promoted security labels on Apr 30, 2021
- PhonicUK added this to Needs triage in AMP Core via automation on Apr 30, 2021
- PhonicUK moved this from Needs triage to High priority in AMP Core on Apr 30, 2021
- PhonicUK moved this from High priority to Closed in AMP Core on Apr 30, 2021

PhonicUK commented on Apr 30, 2021

Contributor

We are assigning a CVE for this issue. Details to follow.

PhonicUK commented on May 4, 2021 • edited ▼

Contributor

This issue was assigned CVE-2021-31926 - The issue was fixed as part of the 2.1.1.2 update.

Assignees

PhonicUK

Labels

core **promoted** security

Projects

III AMP Core

Closed

Milestone

No milestone

Development

No branches or pull requests

2 participants

