Troubleshoot Prime Collaboration Assurance (PCA) "RequestError" Message

Contents

Introduction

This document describes how to identify and resolve the **"RequestError: Unable to load j_spring_security_check status: 500"** Error at PCA log in.

Prerequisites

Requirements

Root access will be required, if root access is not already enabled, please refer to the section Obtaining Root Access

Components Used

This document is not restricted to hardware or software versions

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

Background Information

This issue occurs because invalid values are found in the file /opt/emms/emsam/conf/LdapSettings.properties file.

These values are not expected when Lightweight Directory Access Protocol (LDAP) is disabled.

Additionally this may occur if you enabled Ldap settings, and disabled them prior to an upgrade.

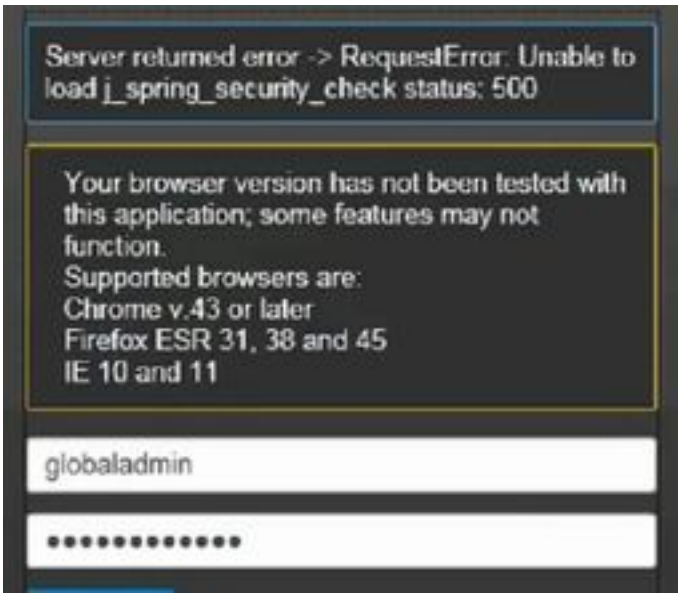
```
[root@PU1ICCGPCA01 ~]# cat /opt/bkp_files/LdapSettings.properties
#Ldap Settings File
#Wed Jul 19 15:24:59 IST 2017
ldap_backup_server_port=\
ldap_ssl=false
ldap_server=\
ldap_admin_dn=\
ldap_searchbase=\
ldap_backup_server=\
ldap_server_port=\
ldap_360_searchbase=\
ldap_password=Invalid Run...
```

Problem

When logging into the graphical user interface (GUI) you will receive an error message stating:

> "RequestError: Unable to load j_spring_security_check status: 500"

This sometimes occurs after an upgrade regardless of the browser.



> Note: PCA 12.1 SP3 introduces "pgbouncer" if you are running this version or above please first perform the below
> Step 1. In root execute "**ps -ef | grep pgbouncer**"
> Step 2. If this does not return as the below, please restart the PCA services before proceeding

```
[root@pca121 ~]# ps -ef | grep pgbouncer
root     10340 10266  0 19:53 pts/0    00:00:00 grep --color=auto pgbouncer
pgbounc+ 12031     1  0 Aug31 ?        01:54:48 /usr/bin/pgbouncer -d -q /etc/pg
bouncer/pgbouncer.ini
[root@pca121 ~]#
```

Solution

Step 1. Log in to the PCA Command Line Interface (CLI) as root

Step 2. Input **cd /opt/emms/emsam/conf/**

Step 3. Input **vi LdapSettings.properties**

Step 4. Input **I** to edit this file and delete all of the entries.

Step 5. Input **:wq!** to save the file

Step 6. Input **/opt/emms/emsam/bin/cpcmcontrol.sh restart**

> **Note** The full restart of services can take up to 20 - 30 minutes.

Obtaining Root Access

This section describes how to obtain Root Access for PCA

Step 1. Log in through Secure Shell Host (SSH) to PCA and use port 26 as the Admin User

Step 2. Input.**root_enable**

Type in the root password you want

Step 3. Input**root**and type in the root password

Step 4. Once logged in as root Input.**/opt/emms/emsam/bin/enableRoot.sh**

Step 5. Input**passwd**and re-enter in your root password

You now should be able to close the SSH session and re-log in directly as root