

Prime Collaboration Assurance(PCA)の「RequestError」メッセージのトラブルシューティング

内容

[概要](#)

[前提条件](#)

[背景説明](#)

[問題](#)

[解決方法](#)

[ルートアクセスの取得](#)

概要

このドキュメントでは、「RequestError:j_spring_security_checkステータスをロードできません : 500" Error at PCA log in.

前提条件

要件

ルートアクセスが必要です。ルートアクセスがまだ有効になっていない場合は、「ルートアクセスの取得」の項を参照してください。

使用するコンポーネント

このドキュメントは、ハードウェアまたはソフトウェアのバージョンに限定されるものではありません

このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、初期（デフォルト）設定の状態から起動しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

背景説明

この問題は、無効な値が/opt/emms/emsam/conf/LdapSettings.propertiesファイルで見つかるために発生します。

これらの値は、Lightweight Directory Access Protocol(LDAP)が無効になっている場合は予期されません。

また、アップグレード前にLDAP設定を有効にし、無効にした場合にも発生する可能性があります。

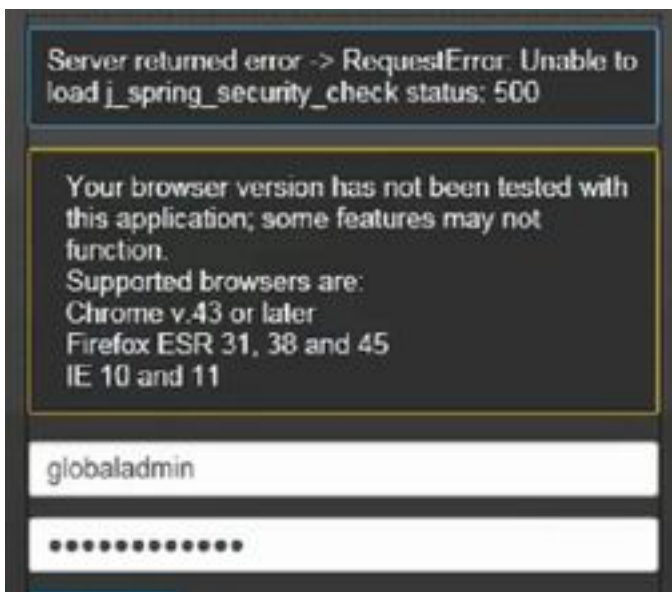
```
[root@PU1ICGPCA01 ~]# cat /opt/bkp_files/LdapSettings.properties
#Ldap Settings File
#Wed Jul 19 15:24:59 IST 2017
ldap_backup_server_port=\
ldap_ssl=false
ldap_server=\
ldap_admin_dn=\
ldap_searchbase=\
ldap_backup_server=\
ldap_server_port=\
ldap_360_searchbase=\
ldap_password=Invalid Run...
```

問題

Graphical User Interface (GUI ; グラフィカルユーザインターフェイス) にログインすると、次のようなエラーメッセージが表示されます。

「RequestError:j_spring_security_checkステータスをロードできません : 500"」

これは、ブラウザに関係なく、アップグレード後に発生することがあります。



注 : PCA 12.1 SP3では「pgbouncer」が導入されています。このバージョン以上を実行している場合は、まず次の手順を実行してください
ステップ1:rootで「ps -ef | grep pgbouncer"
ステップ2 :これが次のように戻らない場合は、続行する前にPCAサービスを再起動してください

```
[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 ~]#
```

解決方法

ステップ1:PCAコマンドラインインターフェイス(CLI)にrootとしてログインします。

ステップ2:`cd /opt/emms/emsam/conf/`

ステップ3:`vi LdapSettings.properties`

ステップ4:`!`と入力してこのファイルを編集し、すべてのエントリを削除します。

ステップ5 : 入力 : `wq!` ファイルを保存するには

ステップ6:`/opt/emms/emsam/bin/cpcmcontrol.sh restart`

注サービスの完全な再起動には、最大20 ~ 30分かかります。

ルートアクセスの取得

ここでは、PCAのルートアクセスを取得する方法について説明します

ステップ1 : セキュアシェルホスト(SSH)を介してPCAにログインし、ポート26を管理ユーザとして使用します

ステップ2:`Input.root_enable`

ルートパスワードを入力します

ステップ3:rootパスワードを入力します。

ステップ4: root `Input./opt/emms/emsam/bin/enableRoot.sh`としてログインした後

ステップ5:パスワードを入力し、ルートパスワードを再入力します

これで、SSHセッションを閉じて、rootとして直接ログインし直せるようになります

翻訳について

シスコは世界中のユーザにそれぞれの言語でサポート コンテンツを提供するために、機械と人による翻訳を組み合わせて、本ドキュメントを翻訳しています。ただし、最高度の機械翻訳であっても、専門家による翻訳のような正確性は確保されません。シスコは、これら翻訳の正確性について法的責任を負いません。原典である英語版（リンクからアクセス可能）もあわせて参照することを推奨します。