PCA(Prime Collaboration Assurance) "RequestError" 메시지 트러블슈팅

목차

[소개](#)
[사전 요구 사항](#)
[배경 정보](#)
[문제](#)
[솔루션](#)
[루트 액세스 얻기](#)

소개

이 문서에서는 **"RequestError: j_spring_security_check 상태를 로드할 수 없습니다. 500"** PCA 로그인 시 오류가 발생했습니다.

사전 요구 사항

요구 사항

루트 액세스가 필요합니다. 루트 액세스가 아직 활성화되지 않은 경우 루트 액세스 얻기 섹션을 참조하십시오

사용되는 구성 요소

이 문서는 하드웨어 또는 소프트웨어 버전으로 제한되지 않습니다

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우, 모든 명령어의 잠재적인 영향을 미리 숙지하시기 바랍니다.

배경 정보

이 문제는 /opt/emms/emsam/conf/LdapSettings.properties 파일에 잘못된 값이 있기 때문에 발생합니다.

LDAP(Lightweight Directory Access Protocol)가 비활성화된 경우 이러한 값은 필요하지 않습니다.

또한 이는 업그레이드 전에 Ldap 설정을 활성화했다가 비활성화한 경우에 발생할 수 있습니다.

```
[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...
```

문제

GUI에 로그인하면 다음과 같은 오류 메시지가 표시됩니다.

> "요청 오류: j_spring_security_check 상태를 로드할 수 없습니다. 500"

이는 브라우저와 상관없이 업그레이드 후에 발생하는 경우가 있습니다.

> 참고: 이 버전 이상을 실행 중인 경우 PCA 12.1 SP3에 "pgbouncer"가 도입되었습니다. 먼저 다음을 수행하십시오
> 1단계. 루트 실행 **"ps -ef | grep pgbouncer"**
> 2단계. 이 결과가 아래와 같이 반환되지 않으면 계속하기 전에 PCA 서비스를 다시 시작하십시오

```
[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 ~]#
```

솔루션

1단계. PCA CLI(Command Line Interface)에 루트로 로그인합니다.

2단계. **cd /opt/emms/emsam/conf/ 입력**

3단계. LdapSettings**.properties를 통해 입력**

4단계. 이 **파일**을 수정하고 모든 항목을 삭제하려면 I를 입력합니다.

5단계. 입력 **:wq!** 파일을 저장하려면

6단계. /opt/emms/emsam/bin/cpcmcontrol.sh restart를 **입력합니다.**

참고 서비스를 완전히 다시 시작하는 데 최대 20~30분이 걸릴 수 있습니다.

루트 액세스 얻기

이 섹션에서는 PCA에 대한 루트 액세스를 얻는 방법에 대해 설명합니다

1단계. SSH(Secure Shell Host)를 통해 PCA에 로그인하고 포트 26을 관리자 사용자로 사용합니다

2단계. Input.**root_enable**

원하는 루트 비밀번호를 입력합니다

3단계. Inputrootand를 입력하고 루트 암호를 입력합니다.

4단계. 루트 Input./opt/emms/emsam/bin/enableRoot.sh으로 로그인한 **경우**

5단계. Inputpasswdand를 입력하고 루트 암호를 다시 입력합니다.

이제 SSH 세션을 종료하고 루트로 직접 다시 로그인할 수 있습니다

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.