O SOAR não pode iniciar o PostgreSQL

Aplicabilidade

Splunk SOAR

Descrição

Problema ao iniciar o banco de dados:

```
[root@hostname db]# systemctl restart postgresql-9.4
Failed to restart postgresql-9.4.service: Unit is not loaded properly: Invalid argument.
See system logs and 'systemctl status postgresql-9.4.service' for details.
```

Investigação

Observação: Dependendo do tipo de instalação (Privilegiado ou Não privilegiado) - os caminhos e os usuários necessários para executar as etapas a seguir variarão. Tome cuidado ao executar essas etapas e verifique se o usuário correto está executando os comandos.

Para instalações Privilegiadas, você pode encontrar o usuário como "root" ou um nome de usuário em relação ao serviço em execução (por exemplo: postgres, pgbouncer, phantom, etc.). Para instalações não privilegiadas você provavelmente verá "phantom" ou outra conta nomeada especificamente usada durante a instalação do SOAR.

Executando systemctl status postgresql-9.4.service:

```
[root@hostname db]# systemctl status postgresql-9.4.service
● postgresql-9.4.service
Loaded: error (Reason: Invalid argument)
Active: inactive (dead) Aug 01 10:27:21 fqdn systemd[1]: postgresql-9.4.service lacks both ExecSt
Aug 01 10:27:21  fqdn systemd[1]: Cannot add dependency job for unit postgresql-9.4.service, ignc
Aug 01 10:27:51  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
Aug 01 10:27:51  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
```

```
Aug 01 10:27:52  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
Aug 01 10:27:53  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
Aug 01 10:27:53  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
Aug 01 10:27:58  fqdn systemd[1]: postgresql-9.4.service lacks both ExecStart= and ExecStop= set
Hint: Some lines were ellipsized, use -l to show in full.
```

Tentou o serviço Stop-Start Phantom, mas obteve este erro ao iniciar:

```
[root@hostname db]# /<phantom_home>/bin/start_phantom.sh
Starting all Phantom services
psql: could not connect to server: No such file or directory
Is the server running locally and accepting
connections on Unix domain socket "/tmp/.s.PGSQL.6432"?
psql: could not connect to server: No such file or directory
Is the server running locally and accepting
connections on Unix domain socket "/tmp/.s.PGSQL.6432"?
psql: could not connect to server: No such file or directory
Is the server running locally and accepting
connections on Unix domain socket "/tmp/.s.PGSQL.6432"?
psql: could not connect to server: No such file or directory
```

Também é notado que postmaster.pid não existe em /<phantom_home>/data/db.

Resolução

Observação: Dependendo do tipo de instalação (Privilegiado ou Não privilegiado) - os caminhos e os usuários necessários para executar as etapas a seguir variarão. Tome cuidado ao executar essas etapas e verifique se o usuário correto está executando os comandos.

Para instalações Privilegiadas, você pode encontrar o usuário como "root" ou um nome de usuário em relação ao serviço em execução (por exemplo: postgres, pgbouncer, phantom, etc.). Para instalações não privilegiadas você provavelmente verá "phantom" ou outra conta nomeada especificamente usada durante a instalação do SOAR.

Executando a Solução Alternativa, fazendo o seguinte:

a. Para iniciar o serviço Postgres

```
sudo -su postgres
/usr/pgsql-9.4/bin/pg_ctl start -D /opt/phantom/data/db/ -s -w -t 300
```

b. Para inicializar o serviço Pgbouncer

```
sudo -su postgres
/usr/bin/pgbouncer -d -q /etc/pgbouncer/pgbouncer.ini
```

c. Iniciar Fantasma

```
/<phantom_home>/bin/start_phantom.sh
```

3. Assim que o Fantasma for iniciado, verificamos as informações de login e GUI. Todos estão bem.

4. Executar os comandos stop_phantom.sh e start_phantom.sh funciona bem.

Sobre esta tradução
A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.