ナレッジベース記事：000532499

Isilon OneFS：強化されたクラスターがsshdの開始に失敗する（000532499）

プライマリ製品：Isilon OneFS

製品：Isilon OneFS

バージョン：6	記事タイプ：不具合修正	対象読者：レベル30 = お客様	最終発行日：2019年7月25日木曜日18:51:15（GMT）

サマリー：　ノードに割り当てられたIPが16を超えている場合、強化されたクラスターがsshの開始に失敗することがあります

問題：

強化されたクラスターでは、OneFSは外部インターフェイスへのssh接続を制限します。これを行うために、各IPが「ListenAddress」として/etc/ssh/sshd_configにリストされます。 OpenSSHは最大ソケット制限（MAX_LISTEN_SOCKS）値を16に設定します。この数を超えると、sshdは開始されず、/var/log/messagesに次のようなエラーが表示されます。

2019-04-17T14:28:24-04:00 <4.2> <CLUSTER>-1(id1) sshd[56211]: fatal: Too many listen sockets. Enlarge MAX_LISTEN_SOCKS

これは、ノードに障害が発生して、動的IP割り当てがより多くのIPをノードに追加し、16リスナー制限を超えた後に、またはより多くのIPを割り当てるようにネットワーク プールが変更された後に表示されます。

原因：

OpenSSHには16のMAX_LISTEN_SOCKS制限があり、16より多く追加すると、これを超過し、sshdは開始されません。

STIGハードニング要件の1つであるUNIX SRGの項目GEN005504では、SSHデーモンは指定された特定のネットワーク アドレスのみをリスンする必要があります。それに応じて、リスン ディレクティブが必要です。
したがって、ハードニングの一環として、sshd_configでは各ノードの外部IPアドレスごとにListenAddressディレクティブが追加されます。

解決策:

この値を「拡大する」するように示すメッセージが表示されますが、実行できません。 OpenSSHのインストール中に設定された、コードの一部です。 これにより、解決方法は構成の操作にゆだねられます。 現在、3つの既知のテスト済み回避策があります。 残念ながら、それらには副次的な影響がないものはなく、障害が発生したノードが交換され、IPがこの制限内になるよう再バランシングされるまで、一時的なものとみなすべきです。

回避策1:
ノードから強化構成を削除します。
実行可能:これにより、ポート22のすべてのIP(フロントおよびバックエンド)についてリストした標準構成に戻ります。
実行不可能:これにより、セキュリティ構成が削除され、会社のポリシーに違反する場合があります。

回避策2:
各ノードのIPの数を最大15に制限するようにネットワーク構成を変更します。
実行可能:IPを減らすことで、制限要件が満たされ、sshdを開始できるようになります。
実行不可能: 起こり得るいくつかの問題の1つは、これにより、クライアントがデータ アクセスのために使用しているIPが削除され、クライアント構成を変更する必要がある場合があることです。

回避策3:
/etc/ssh/sshd_configファイルを編集し、超過したListenAddress行をコメントアウトまたは削除します。
実行可能:ListenAddress行の数を16未満に減らすと、sshdが開始されます。
実行不可能:このファイルは再起動時にリセットされ、sshの欠如が返されます。

これに対する最良の解決方法は、クラスターをノードの欠如の状態にしないネットワーク構成です。 この問題は、OneFSに固有のものではなく、OpenSSHの制限です。

注:

回避策1:

```
#isi hardening revert
```

回避策2:

これを実装するには、ノード上の外部インターフェイスに割り当てられたプールを編集し、IPの数を減らす必要があります。
ノードの数に15(15によって最大16に対して猶予できる)を乗算した数を計算

し、割り当てるIPの数をその数未満にしておきます

その後sshdを再開します。

```
# isi services -a sshd disable
The service 'sshd' has been disabled.
# isi services -a sshd enable
The service 'sshd' has been enabled.
```

回避策その3:

```
#vi /etc/ssh/sshd_config
```

sshに使用する必要がないすべてのIPの前に「#」を追加して、構成ファイルで15以下を残します。

例:

```
# cat /etc/ssh/sshd_config
# X: ----------------
# X: This file is automatically generated and should not
be
# X: edited directly.  If you must make changes to the
# X: contents of this file it should be done via the
# X: template file located at
/etc/mcp/templates/sshd_config
# X: ----------------

#
Port 22
#isi_GEN005504
ListenAddress x.x.x.1
ListenAddress x.x.x.2
ListenAddress x.x.x.3
ListenAddress x.x.x.4
ListenAddress x.x.x.5
ListenAddress x.x.x.6
ListenAddress x.x.x.7
ListenAddress x.x.x.8
ListenAddress x.x.x.9
ListenAddress x.x.x.10
ListenAddress x.x.x.11
ListenAddress x.x.x.12
ListenAddress x.x.x.13
ListenAddress x.x.x.14
ListenAddress x.x.x.15
#ListenAddress x.x.x.16
#ListenAddress x.x.x.17
#ListenAddress x.x.x.18
ServerKeyBits 768
LoginGraceTime 120
KeyRegenerationInterval 3600
#isi_GEN001120
PermitRootLogin no
```

```
<<<TRUNCATED>>>
```

その後、sshdを再開します。

```
# isi services -a sshd disable
The service 'sshd' has been disabled.
# isi services -a sshd enable
The service 'sshd' has been enabled.
```

プライマリ製品： Isilon OneFS

製品： Isilon OneFS