ESXi 6.7P04(빌드 17167734) 이상과 SSH 비호 환성

목차

소개 요구 사항 추가 정보 결함 소프트웨어 자문 영향 받는 영역 해결 방법 해결 방법 단계 해결 방법 1 해결 방법 2

소개

HXDP [3.5(x), 4.0(x)] 및 ESXi 6.7P04(빌드 17167734) 이상 간에는 소프트웨어 상호 운용성 문제가 있습니다. 고객은 이 소프트웨어 조합을 피해야 합니다.

참고:이 문제는 6.7P04 이상의 모든 6.7 ESXi 버전으로 확장됩니다.

호환성 문제는 HXDP **4.0(2e)**에서 **해결됩니다**. 이 문제는 HXDP 4.5(1a) 이상에는 영향을 미치지 않습니다.

요구 사항

ESXi 6.7P04(빌드 17167734) 이상

HXDP 버전 - 3.5(x), 4.0(x)

추가 정보

결함

관련 버그 ID는 <u>CSCvv88204</u> - HXDP와의 ESXi OpenSSH 상호 운용성 문제

이 문제는 ESXi 6.7P04에서 발생합니다. VMware가 openSSH 라이브러리를 OpenSSH_8.3p1로 업그레이드했기 때문입니다. 이 새로운 버전의 OpenSSH는 SSH를 통해 ESXi에 직접 통신할 때 HXDP에서 내부적으로 사용하는 키 교환 방법에 대한 지원을 제거합니다.다음은 해당 버전에서 변경된 내용을 설명하는 OpenSSH 변경 로그의 조각입니다.

ssh(1), sshd(8): this release removes diffie-hellman-group14-shal from the default key exchange proposal for both the client and server.

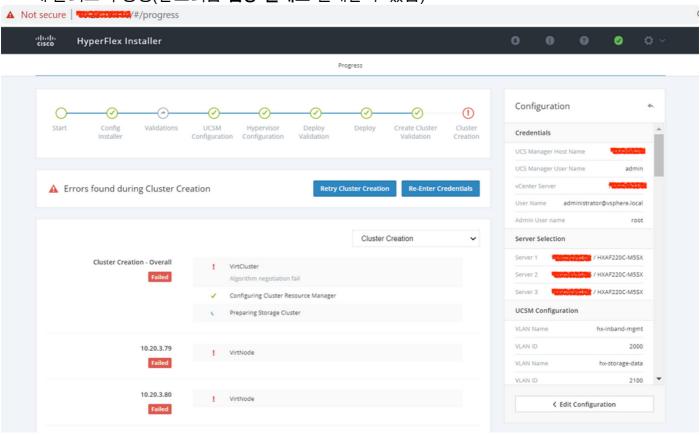
소프트웨어 자문

자세한 내용은 Software Advisory를 참조하십시오. - ESXi 6.7 P04용 Cisco Software Advisory

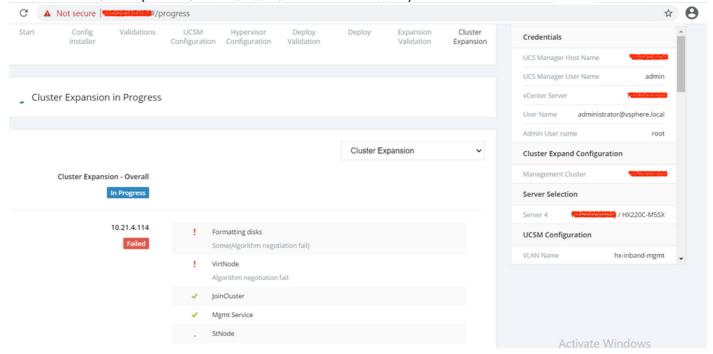
영향 받는 영역

HX의 일부 기능 영역은 다음과 같이 영향을 받습니다.

• 새 클러스터 생성(알고리즘 협상 실패로 실패할 수 있음)



• 클러스터 확장(알고리즘 협상 실패로 실패할 수 있음)



• 클러스터 재등록(stcli 클러스터 재등록이 "알고리즘 협상 실패"로 실패할 수 있음)

root@ucsblr1152-svcm:~# stcli cluster reregister --vcenter-url 10.33.16.117 --vcenter-user administrator@vsphere.local --vcenter-password Nbv@12345 --vcenter-datacenter ucsblr1149cip-dc --vcenter-cluster ucsblr1149cip-cluster

Reregister StorFS cluster with a new vCenter ...

Storage cluster reregistration with a new vCenter failed

Algorithm negotiation fail

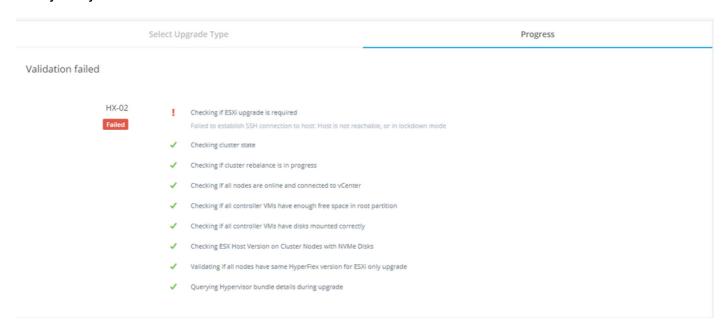
root@ucsblr1152-svcm:~#

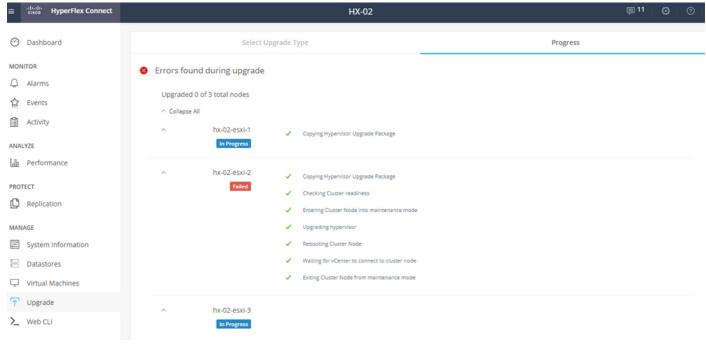
- HX Connect의 시스템 정보 페이지
- 업그레이드는 "호스트에 대한 SSH 연결을 설정하지 못했습니다." 또는 "업그레이드 중 오류가 발견됨"으로 실패할 수 있습니다.

ESXi 업그레이드가 ssh 예외로 인해 실패합니다.

2020-12-16-10:31:04.675 [] [vmware-upgrade-pool-9] 오류 c.s.sysmgmt.stMgr.SshScpUtilImpl - 호 스트에 대한 SSH 연결을 설정하지 못했습니다.호스트에 연결할 수 없거나 잠금 모드입니다.

com.jcraft.jsch.JSch예외:알고리즘 협상 실패





• 잠재적으로 다른 영역

해결 방법

HXDP 릴리스 노트는 3.5(x) 및 4.0(x) 릴리스에서 지원되지 않는 이 버전의 6.7을 구체적으로 발표하도록 업데이트되었습니다.이 문제는 HXDP 4.0 패치 - 4.0(2e) 및 모든 릴리스 4.5(1a) 이상에서 수정되었습니다.

- ESXi에 내장된 롤백 메커니즘을 사용하여 호환되는 ESXi 버전으로 롤백합니다.
- 또 다른 해결 방법은 각 ESXi 호스트에서 sshd_config를 업데이트하고 SSH 서비스를 다시 시작하여 제거된 키 교환 방법을 다시 활성화하는 것입니다. 이 해결 방법은 일시적으로 구현만하는 것이 좋습니다.

참고: 목표는 클러스터를 고정 HXDP 릴리스로 이동하고 가능한 한 빨리 이 해결 방법을 제거하는 것입니다.클러스터는 sshd_config에 추가된 이 추가 키 알고리즘 설정을 사용하여 이 상태를 장기 간 유지해서는 안 됩니다.

해결 방법 단계

HXDP를 고정 릴리스로 업그레이드할 수 없는 경우 다음 해결 방법을 사용하십시오.

해결 방법 1

• ESXi에 내장된 롤백 메커니즘을 사용하여 호환되는 ESXi 버전으로 롤백합니다.vmware KB 참조 - https://kb.vmware.com/s/article/1033604

해결 방법 2

각 ESXi 호스트에서 sshd_config를 업데이트하고 SSH 서비스를 다시 시작하여 제거된 키 교환 방법을 다시 활성화합니다.

• 각 ESXi 호스트의 /etc/ssh/sshd_config 아래의 KexAlgorithm에 +diffie-hellman-group14-sha1 추가

echo "KexAlgorithms +diffie-hellman-group14-shal" >> /etc/ssh/sshd_config

• KexAlgorithms **+diffie-hellman-group14-sha1이** /etc/ssh/sshd config에 표시되는지 확인합니다

```
Subsystem sftp /usr/lib/vmware/openssh/bin/sftp-server -f LOCAL5 -l INFO

AuthorizedKeysFile /etc/ssh/keys-%u/authorized_keys

# Timeout value of 10 mins. The default value of ClientAliveCountMax is 3.

# Hence, we get a 3 * 200 = 600 seconds timeout if the client has been

# unresponsive.

ClientAliveInterval 200

# sshd(8) will refuse connection attempts with a probability of "rate/100"

# (30%) if there are currently "start" (10) unauthenticated connections. The

# probability increases linearly and all connection attempts are refused if the

# number of unauthenticated connections reaches "full" (100)

MaxStartups 10:30:100

KexAlgorithms +diffie-hellman-group14-shal

I /etc/ssh/sshd_config [Modified] 54/54 100%
```

• ESXi SSH 프로세스 재시작

```
# /etc/init.d/SSH restart
[root@hx-02-esxi-2:/var/log]
[root@hx-02-esxi-2:/var/log] /etc/init.d/SSH restart
SSH login disabled
SSH login enabled
[root@hx-02-esxi-2:/var/log]
```

• 이전에 실패한 워크플로를 다시 시작하거나 다시 시작합니다.