DELL VxRail TPM and Secure Boot Technical Instructions

VxRail TPM and Secure Boot Technical Instructions

Dell VxRail TPM and Secure Boot
Technical note
May 2022

Abstract

This document describes how to resolve "Host Secure Boot was disabled" issues, by either enabling Secure Boot or disabling the TPM module.

Copyright

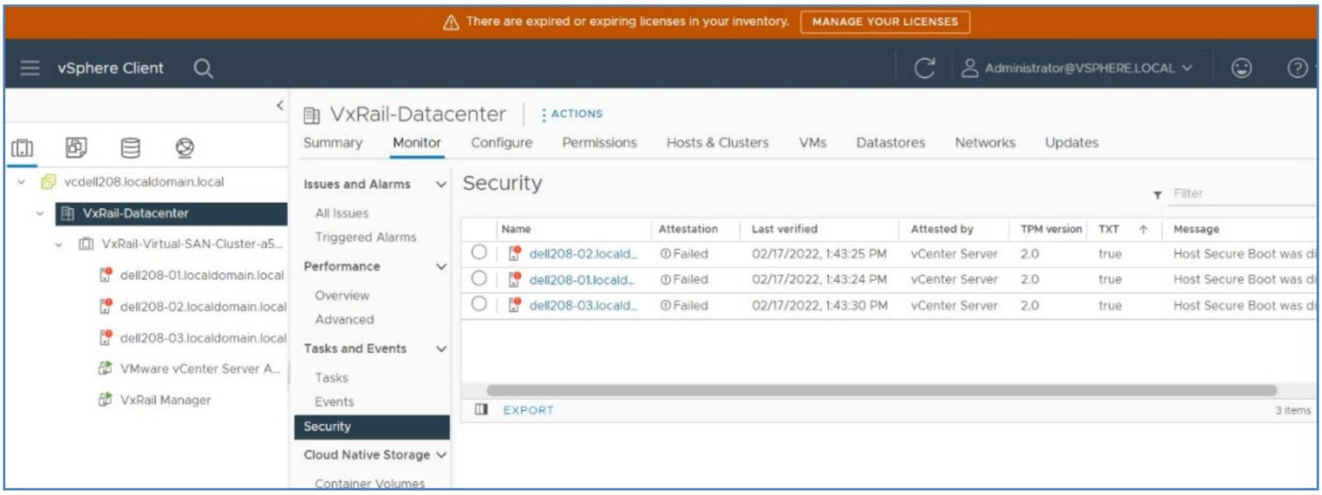
Contents

Procedure summary

By default, VxRail ships from the factory with TPM module enabled and Secure Boot disabled. After you receive the VxRail and complete VxRail Manager first run, the host
might not pass attestation. To resolve “Host Secure Boot was disabled” issues, either enable Secure Boot or disable the TPM module.
Note: VMware QuickBoot is not supported when Secure Boot is enabled.
To enable Secure Boot, see the ‘How to Enable Secure Boot” section of this document.
After enabling Secure Boot, if the TPM hierarchy is disabled by mistake, the host might not pass attestation. To resolve the “Unable to provision Endorsement Key on TPM 2.0 device: Endorsement Key creation failed on device.”/ “Internal failure” issue, see the ‘How to Enable Hierarchy’ section of this document.
To disable the TPM module, see the ‘How to Disable TPM” section of this document.
If after disabling the TPM, you want to enable Secure Boot, see the ‘How to Enable TPM and Secure Boot” section of this document. In this case, the host might show “N/A” message in attestation view until the TPM and Secure Boot are enabled.

How to Enable Secure Boot

1. View the ESXi host alarm status and accompanying error message.
2. Connect to vCenter Server by using the vSphere Client.
3. Select a data center and click the Monitor tab.
4. Click Security.
5. Review the host status in the Attestation column and read the accompanying message in the Message column.
6. If the error message is “Host Secure Boot was disabled”, you must enable Secure Boot to resolve the problem.

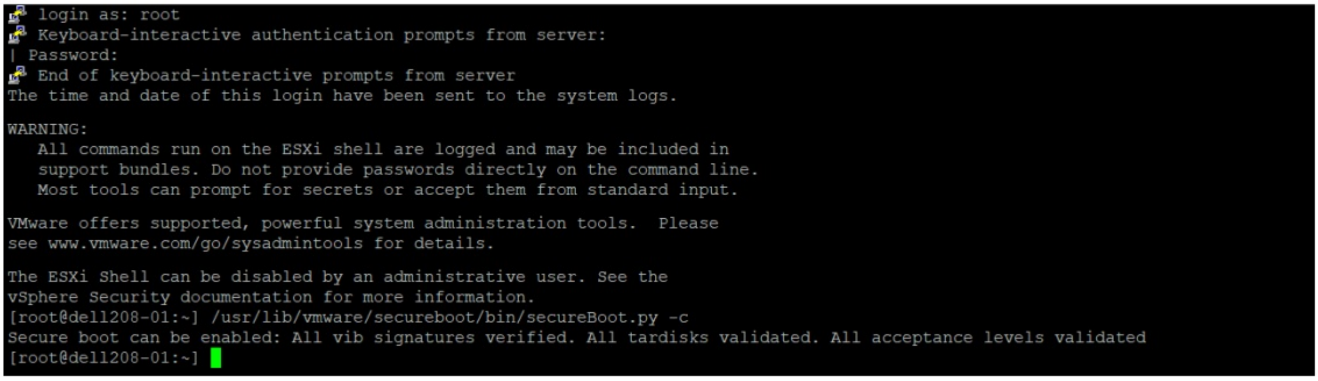


Security

	Name	Attestation	Last verified	Attested by	TPM version	TXT	Message
○	dell208-02.locald...	Failed	02/17/2022, 1:43:25 PM	vCenter Server	2.0	true	Host Secure Boot was di
○	dell208-01.locald...	Failed	02/17/2022, 1:43:24 PM	vCenter Server	2.0	true	Host Secure Boot was di
○	dell208-03.locald...	Failed	02/17/2022, 1:43:30 PM	vCenter Server	2.0	true	Host Secure Boot was di

Figure 1 Attestation failure

7. Verify whether Secure Boot can be enabled. If it cannot be enabled, contact Dell Tech Support.

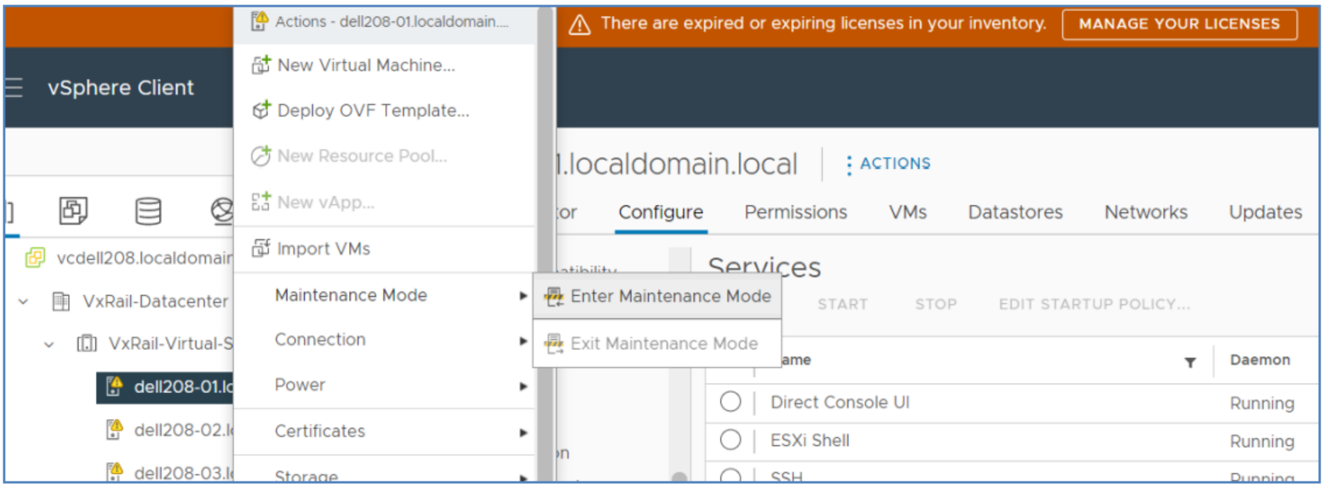


```
 login as: root
 Keyboard-interactive authentication prompts from server:
| Password:
 End of keyboard-interactive prompts from server
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@dell208-01:~] /usr/lib/vmware/secureboot/bin/secureBoot.py -c
Secure boot can be enabled: All vib signatures verified. All tardisks validated. All acceptance levels validated
[root@dell208-01:~]
```

Figure 2 Secure boot enablement verification

8. Enable Secure Boot:

   a. From the VMware vCenter vSphere Client, move one node to Enter Maintenance Mode.

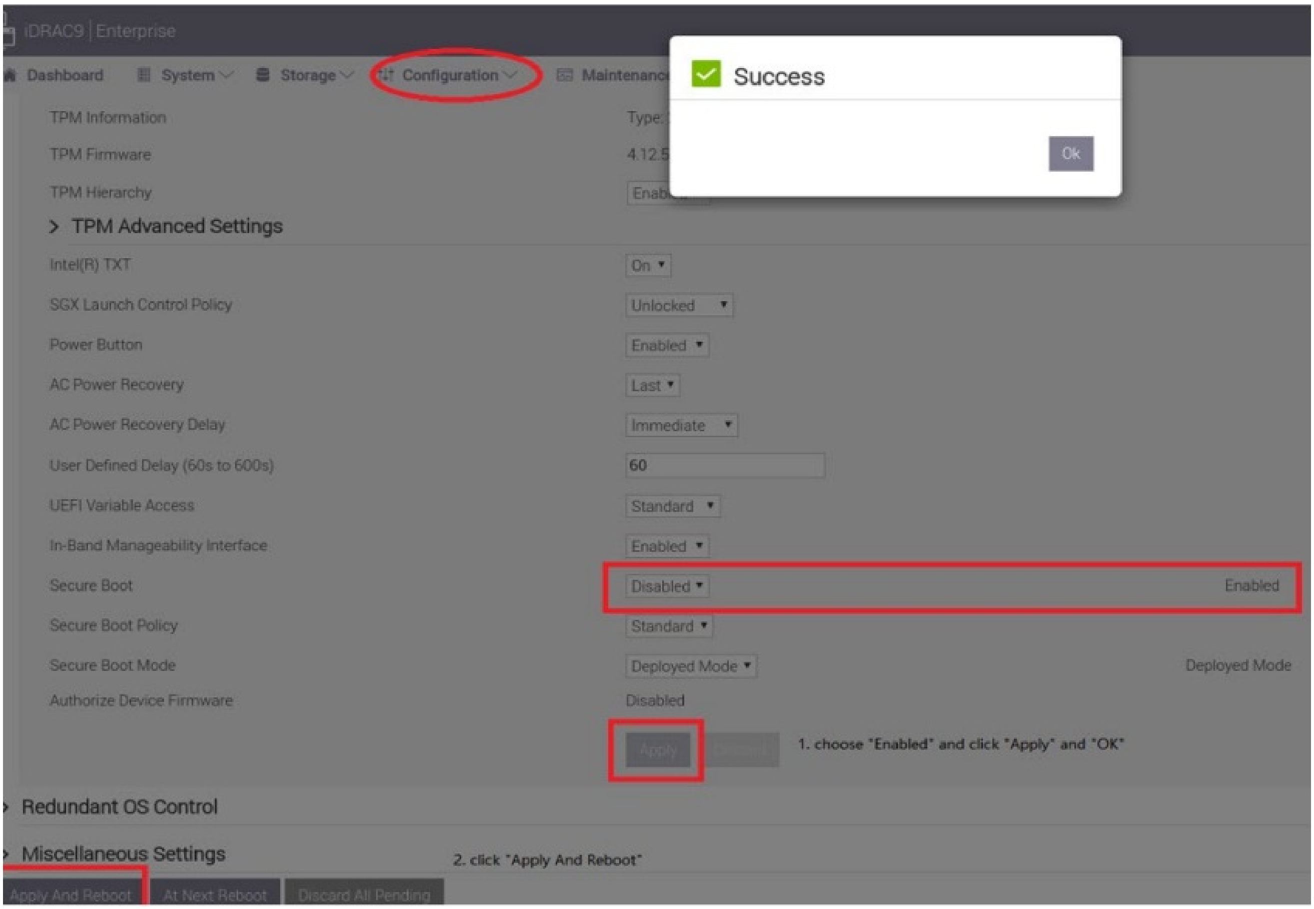


Name	Daemon
Direct Console UI	Running
ESXi Shell	Running
SSH	Running

Figure 3 Move node to Maintenance Mode.

b. Log in to iDRAC to configure Secure Boot, and select the Configure tab > BIOS Settings > System Security > TPM Advanced Settings.

c. Select Secure Boot enable and click Apply > OK > Apply and Reboot.



TPM Information Type:
TPM Firmware 4.12.5
TPM Hierarchy Enabled

TPM Advanced Settings

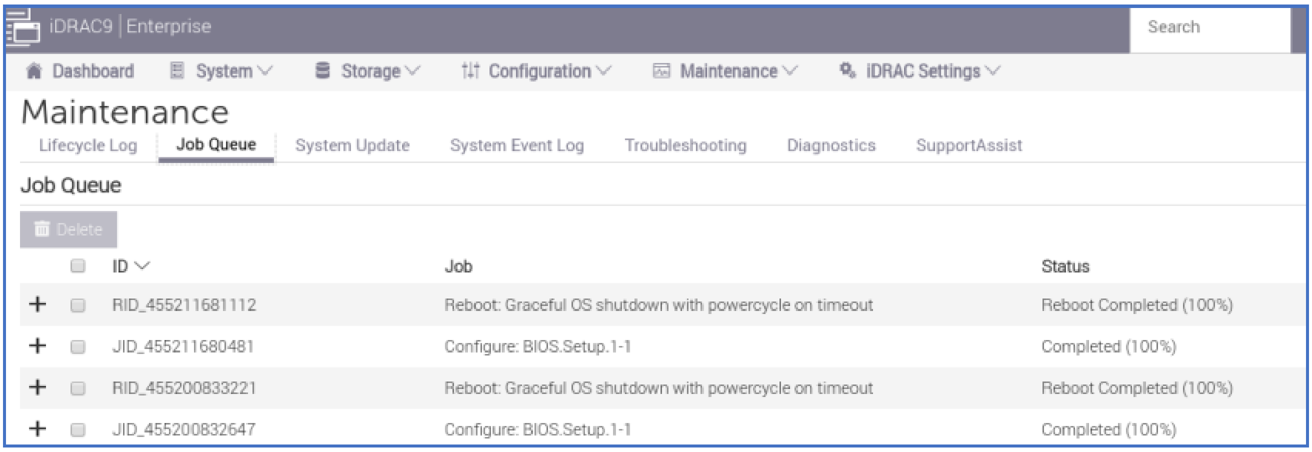
Intel(R) TXT	On	
SGX Launch Control Policy	Unlocked	
Power Button	Enabled	
AC Power Recovery	Last	
AC Power Recovery Delay	Immediate	
User Defined Delay (60s to 600s)	60	
UEFI Variable Access	Standard	
In-Band Manageability Interface	Enabled	
Secure Boot	Disabled	Enabled
Secure Boot Policy	Standard	
Secure Boot Mode	Deployed Mode	Deployed Mode
Authorize Device Firmware	Disabled	

1. choose "Enabled" and click "Apply" and "OK"

2. click "Apply And Reboot"

Figure 4 Enable Secure Boot.

d. Click Job queue. Wait for all jobs to complete 100%.



	☐	ID	Job	Status
+	☐	RID_455211681112	Reboot: Graceful OS shutdown with powercycle on timeout	Reboot Completed (100%)
+	☐	JID_455211680481	Configure: BIOS.Setup.1-1	Completed (100%)
+	☐	RID_455200833221	Reboot: Graceful OS shutdown with powercycle on timeout	Reboot Completed (100%)
+	☐	JID_455200832647	Configure: BIOS.Setup.1-1	Completed (100%)

Figure 5 Status reached 100% completion.

e. Log in to the VMware vCenter vSphere Client and set the node to Exit Maintenance Mode.

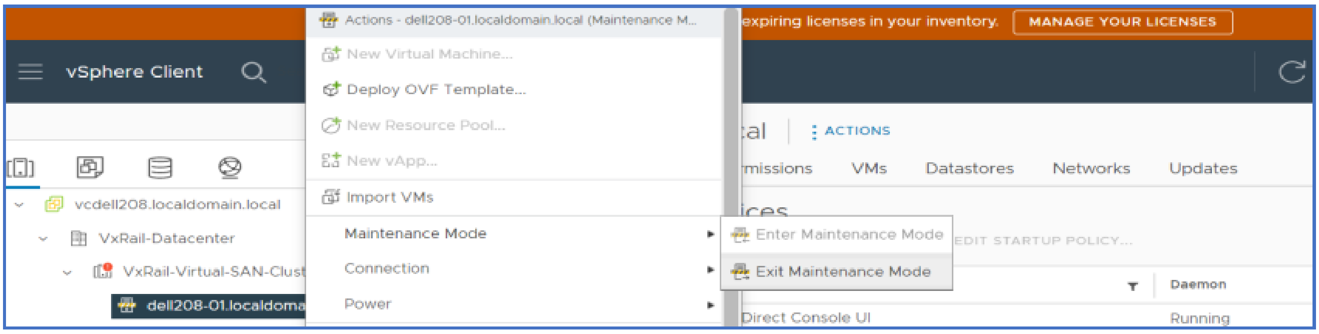
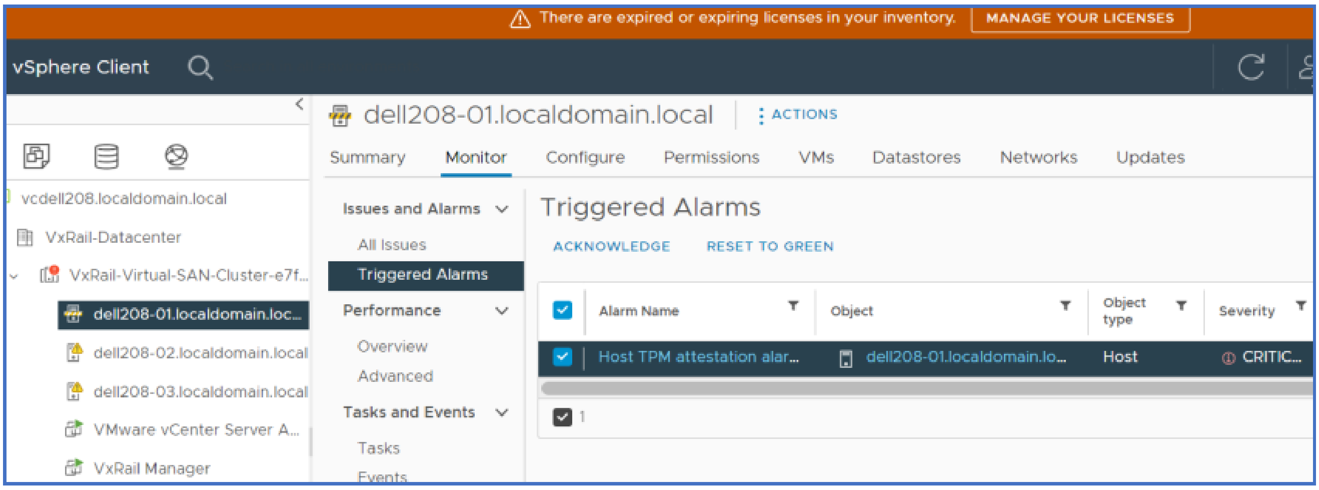


Figure 6 Set node to Exit Maintenance Mode.

9. Perform Step 8 on each node until all nodes have Secure Boot enabled from iDRAC.
10. Log in to VMware vCenter vSphere Client and select the data center.
11. Click the Monitor and Security tab to verify that the latest Attestation status shows “Passed”.
12. If you see the alarm with a red icon, select it and click RESET TO GREEN.



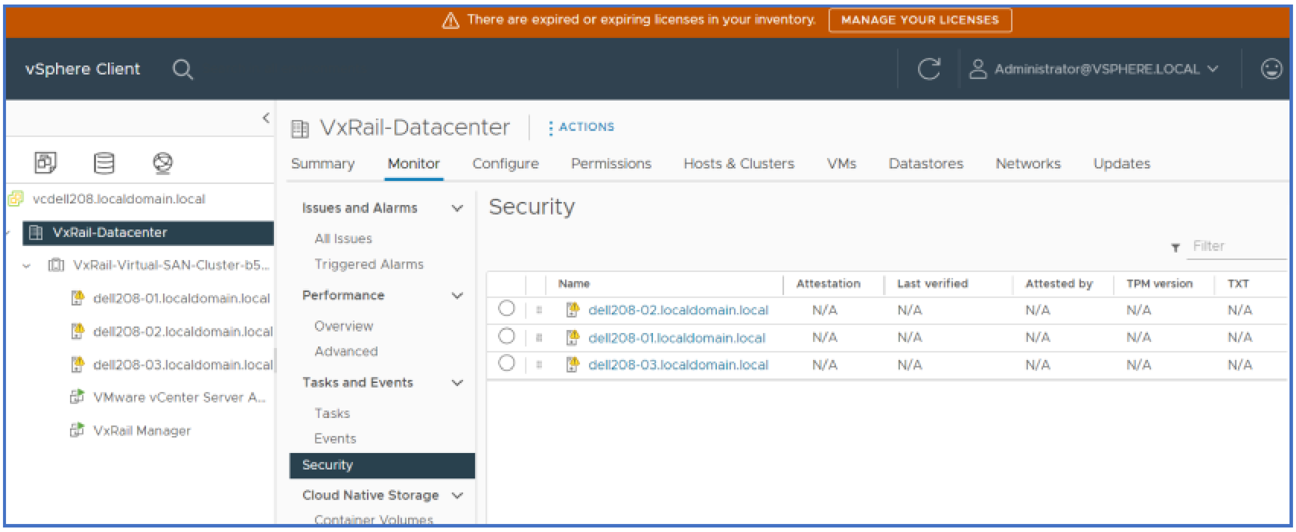
☑	Alarm Name	Object	Object type	Severity
☑	Host TPM attestation alar...	dell208-01.localdomain.lo...	Host	CRITIC...

☑ 1

Figure 7 Reset to Green.

How to Enable TPM and Secure Boot

1. View the ESXi host alarm status and accompanying error message.
2. Connect to VMware vCenter Server using the VMware vSphere Client.
3. Select a data center and click the Monitor tab.
4. Click Security.
5. Review the host status in the Attestation column and read the accompanying message in the Message column.
6. If the error message is “N/A”, enable TPM and Secure Boot to resolve the issue.

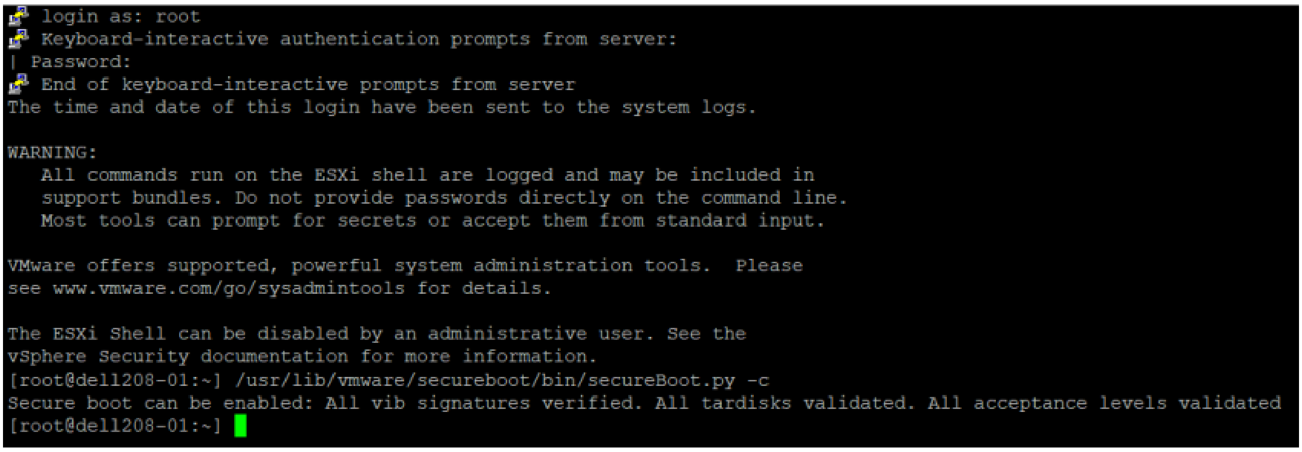


Security

Name	Attestation	Last verified	Attested by	TPM version	TXT
dell208-02.localdomain.local	N/A	N/A	N/A	N/A	N/A
dell208-01.localdomain.local	N/A	N/A	N/A	N/A	N/A
dell208-03.localdomain.local	N/A	N/A	N/A	N/A	N/A

Figure 8 Attestation status “N/A”

7. Verify whether Secure Boot can be enabled. If it cannot be enabled, contact Dell Tech Support.



```
 login as: root
 Keyboard-interactive authentication prompts from server:
| Password:
 End of keyboard-interactive prompts from server
The time and date of this login have been sent to the system logs.

WARNING:
   All commands run on the ESXi shell are logged and may be included in
   support bundles. Do not provide passwords directly on the command line.
   Most tools can prompt for secrets or accept them from standard input.

VMware offers supported, powerful system administration tools.  Please
see www.vmware.com/go/sysadmintools for details.

The ESXi Shell can be disabled by an administrative user. See the
vSphere Security documentation for more information.
[root@dell208-01:~] /usr/lib/vmware/secureboot/bin/secureBoot.py -c
Secure boot can be enabled: All vib signatures verified. All tardisks validated. All acceptance levels validated
[root@dell208-01:~]
```

Figure 9 Secure Boot enablement verification

8. Enable TPM and Secure Boot:

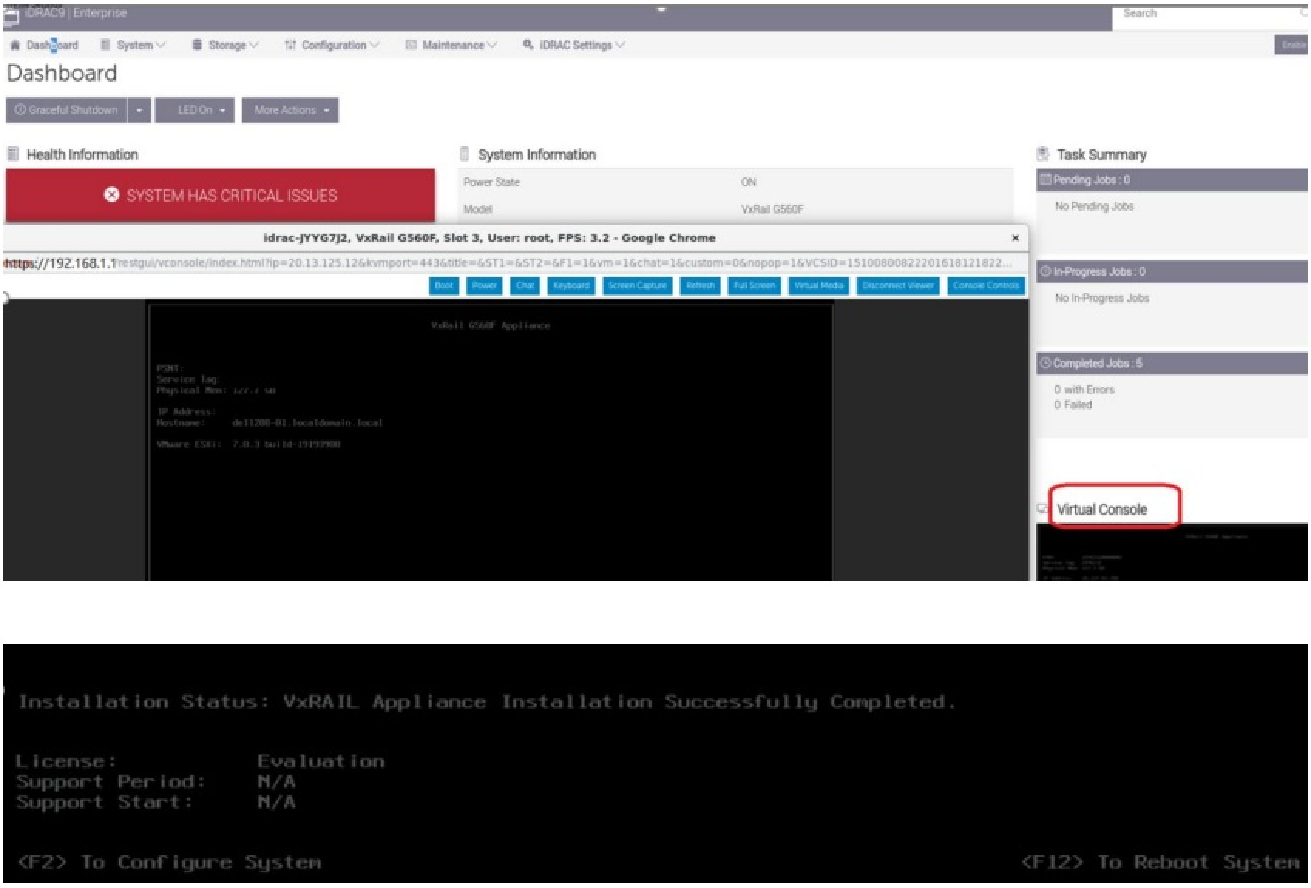
a. From the VMware vCenter vSphere Client, move one node to Enter Maintenance Mode.

b. Log in to iDRAC to configure Secure Boot, and select the Configure tab > BIOS Settings > System Security > TPM Security “On” > TPM Advanced Settings.

c. Select Secure Boot “enable” and click Apply > OK > Apply and Reboot.

d. Click Job queue. Wait for all jobs to complete 100%.

e. Go to Dashboard > Virtual Console to see if console shows “successfully completed”; if yes, continue.



idrac-JYYG7J2, VxRail G560F, Slot 3, User: root, FPS: 3.2 - Google Chrome

https://192.168.1.1/restgui/vconsole/index.html?ip=20.13.125.12&kvmport=443&title=&ST1=&ST2=&F1=1&vm=1&chat=1&custom=0&nopop=1&VCSID=1510080082220161812182...

```
                         VxRail G560F Appliance

PSNT:
Service Tag:
Physical Mem:  127.7 GB

IP Address:
Hostname:      dell208-01.localdomain.local

VMware ESXi:  7.0.3 build-19193900
```

```
Installation Status: VxRAIL Appliance Installation Successfully Completed.

License:            Evaluation
Support Period:     N/A
Support Start:      N/A

<F2> To Configure System                                                  <F12> To Reboot System
```

Figure 10 Installation successfully completed.

f. Log in to VMware vCenter vSphere Client and disconnect the node.

g. Reconnect the node, and then Exit Maintenance Mode.

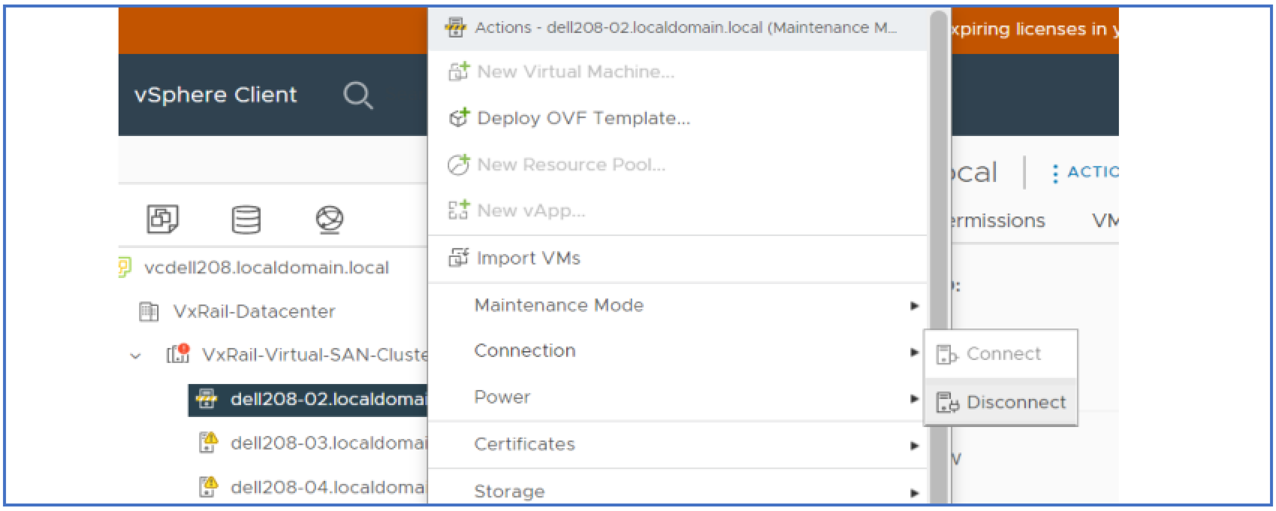
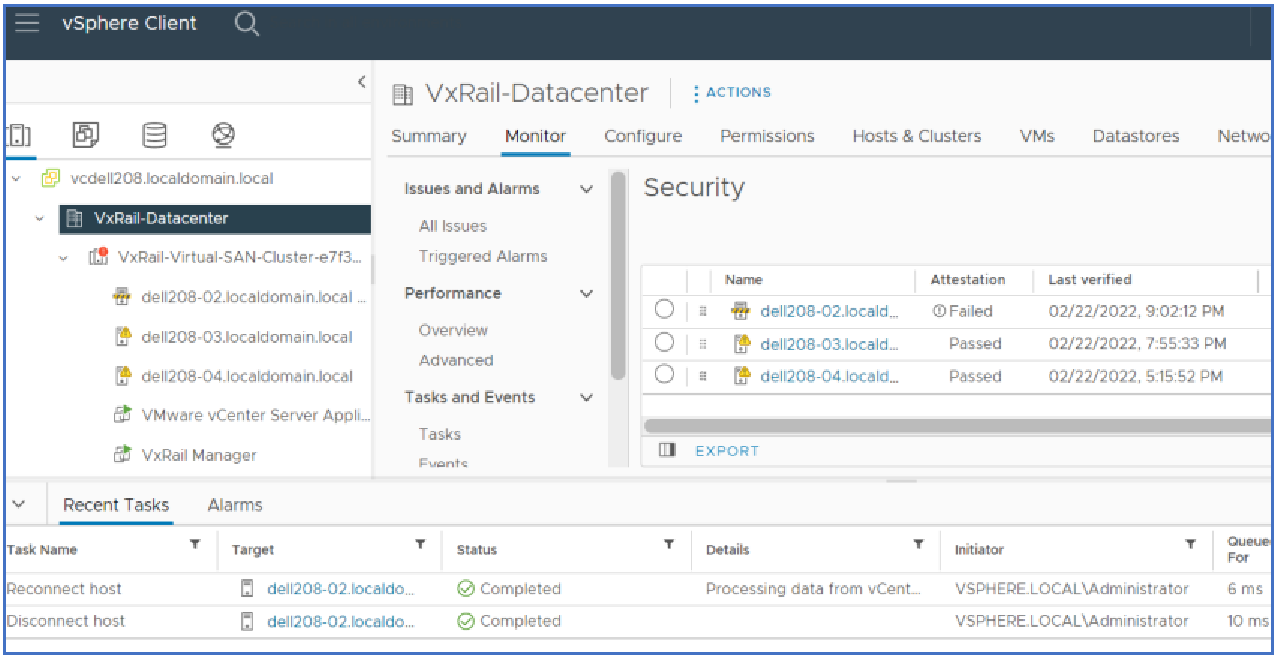


Figure 11 Disconnect and reconnect node.



Name	Attestation	Last verified
dell208-02.locald...	ⓘ Failed	02/22/2022, 9:02:12 PM
dell208-03.locald...	Passed	02/22/2022, 7:55:33 PM
dell208-04.locald...	Passed	02/22/2022, 5:15:52 PM

Task Name	Target	Status	Details	Initiator	Queued For
Reconnect host	dell208-02.localdo...	✓ Completed	Processing data from vCent...	VSPHERE.LOCAL\Administrator	6 ms
Disconnect host	dell208-02.localdo...	✓ Completed		VSPHERE.LOCAL\Administrator	10 ms

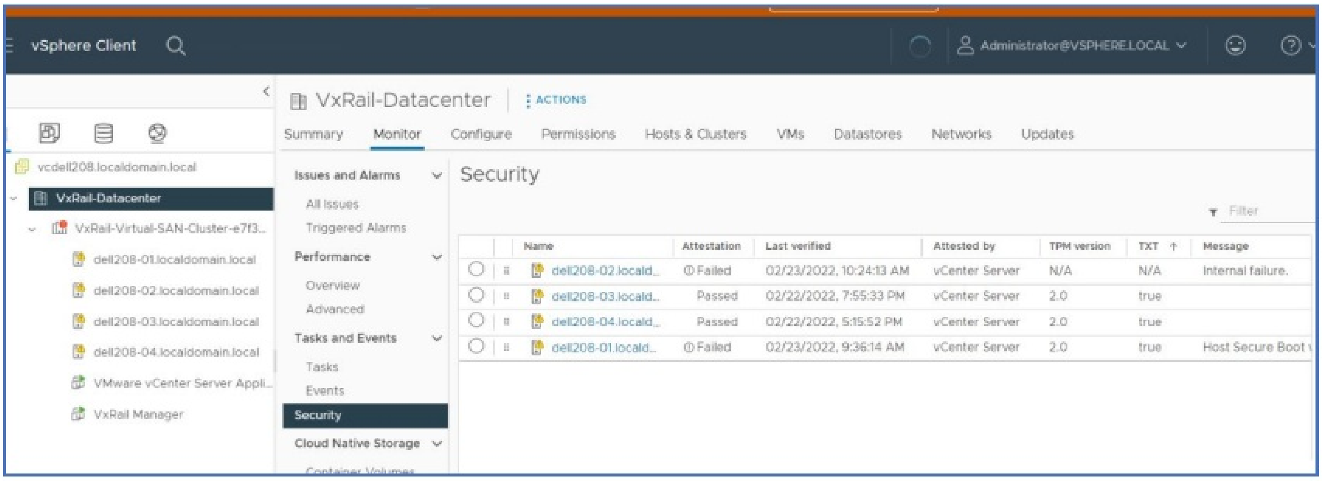
Figure 12 Recent tasks

9. Perform Steps 7 and 8 on each node until all nodes have TPM and Secure Boot enabled from iDRAC.
10. Log in to VMware vCenter vSphere Client and go to the data center.
11. Click the Monitor and Security tab to verify that the latest Attestation status is “Passed”. If you see an alarm with a red icon, select the specific Triggered Alarm and click RESET TO GREEN.

How to Disable TPM

Note: Before you disable TPM, ensure that Secure Boot has been enabled on the host.

1. View the ESXi host alarm status and accompanying error message.
2. Connect to VMware vCenter Server by using the VMware vSphere Client.
3. Select a data center and click the Monitor tab.
4. Click Security.
5. Review the host status in the Attestation column and read the accompanying message in the Message column.
6. If the error message is “Host Secure Boot was disabled”, you must disable TPM to resolve the problem if you do not want to enable Secure Boot.



Name	Attestation	Last verified	Attested by	TPM version	TXT ↑	Message
dell208-02.locald...	ⓘ Failed	02/23/2022, 10:24:13 AM	vCenter Server	N/A	N/A	Internal failure.
dell208-03.locald...	Passed	02/22/2022, 7:55:33 PM	vCenter Server	2.0	true	
dell208-04.locald...	Passed	02/22/2022, 5:15:52 PM	vCenter Server	2.0	true	
dell208-01.locald...	ⓘ Failed	02/23/2022, 9:36:14 AM	vCenter Server	2.0	true	Host Secure Boot v

Figure 13 Attestation host status.

7. If you see an alarm with a red icon, select the specific Triggered Alarm and click RESET TO GREEN.
8. Disable TPM:

a. From the VMware vCenter vSphere Client, move one node to Enter Maintenance Mode.

b. Log in to iDRAC to configure Secure Boot, and select the Configure tab > BIOS Settings > System Security > TPM Security “Off” > TPM Advanced Settings.

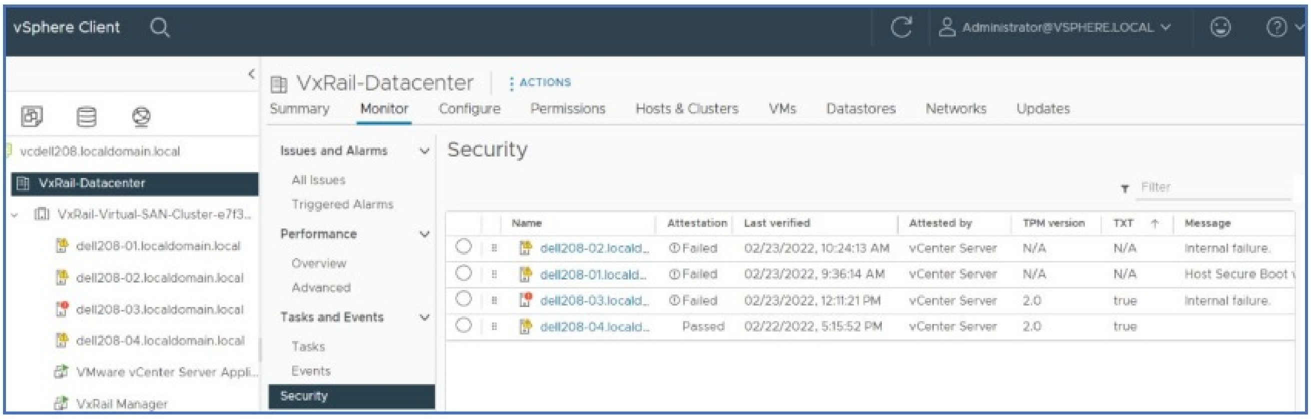
c. Select Secure Boot “disable” and click Apply > OK > Apply and Reboot.

d. Click Job queue. Wait for all jobs to complete 100%.

e. Go to Dashboard > Virtual Console to see if console shows “successfully completed”; if yes, continue.

f. Log in to the VMware vCenter vSphere Client and select Exit Maintenance Mode.

9. Perform Steps 7 and 8 on each node until all nodes have TPM disable from iDRAC.
10. Log in to VMware vCenter vSphere Client and select a data center.
11. Select the Monitor and Security tab to verify that the latest Attestation message failed. The TPM version and TXT show “N/A” and Message shows “Host Secure Boot was disabled”.



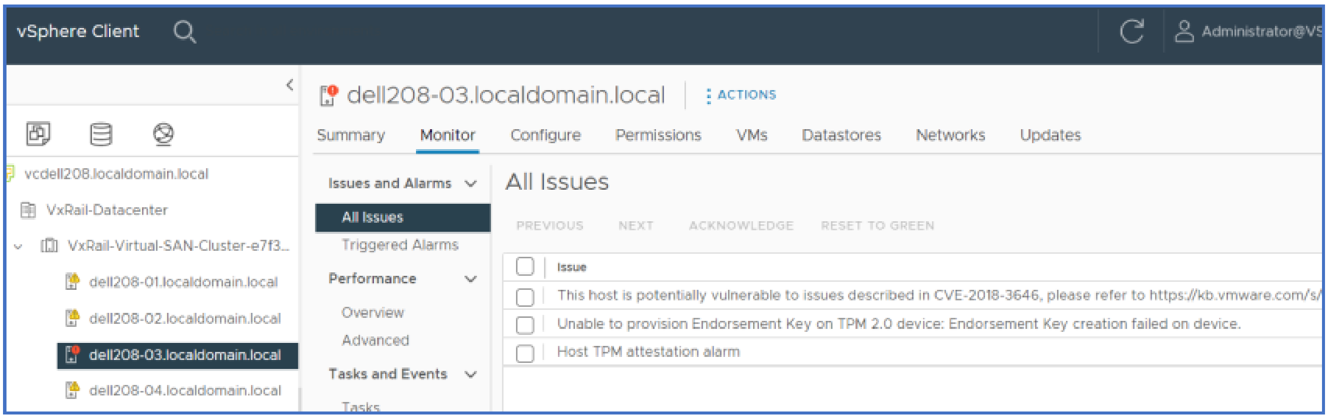
Security

Name	Attestation	Last verified	Attested by	TPM version	TXT	Message
dell208-02.locald...	Failed	02/23/2022, 10:24:13 AM	vCenter Server	N/A	N/A	Internal failure.
dell208-01.locald...	Failed	02/23/2022, 9:36:14 AM	vCenter Server	N/A	N/A	Host Secure Boot \
dell208-03.locald...	Failed	02/23/2022, 12:11:21 PM	vCenter Server	2.0	true	Internal failure.
dell208-04.locald...	Passed	02/22/2022, 5:15:52 PM	vCenter Server	2.0	true	

Figure 14 Attestation message failed.

How to Enable Hierarchy

1. View the ESXi host alarm status and accompanying error message.
2. Connect to VMware vCenter Server by using the VMware vSphere Client.
3. Select a data center and click the Monitor tab.
4. Click Security.
5. Review the host status in the Attestation column and read the accompanying message in the Message column.
6. If the error message is “Unable to provision Endorsement Key on TPM 2.0 device: Endorsement Key creation failed on device”, you must enable TPM Hierarchy
to resolve the issue.



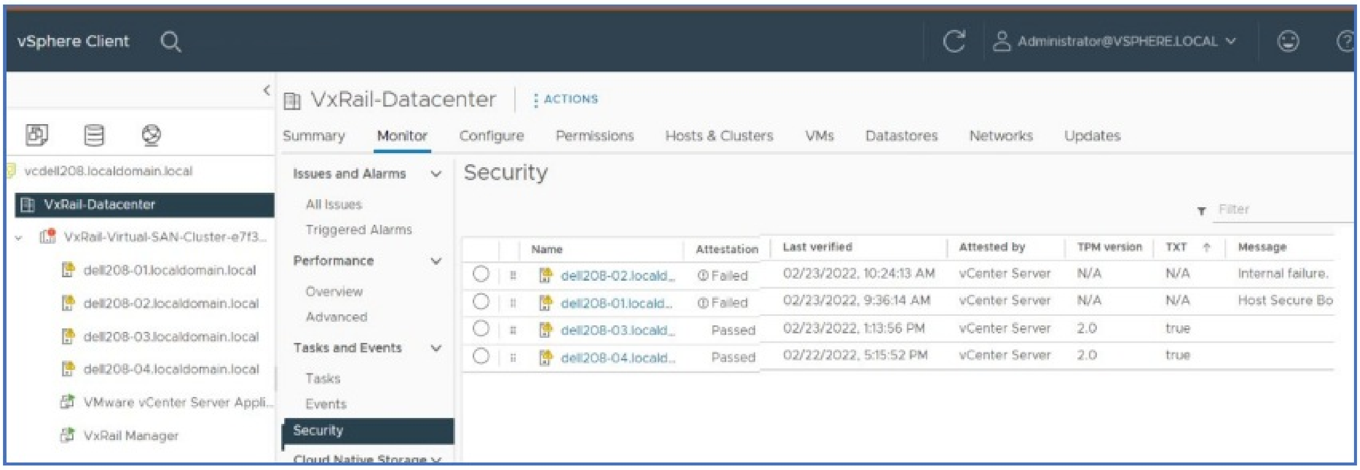
All Issues

Issue
This host is potentially vulnerable to issues described in CVE-2018-3646, please refer to https://kb.vmware.com/s/
Unable to provision Endorsement Key on TPM 2.0 device: Endorsement Key creation failed on device.
Host TPM attestation alarm

Figure 15 Endorsement key creation failed.

7. If you see an alarm with a red icon, select the specific Triggered Alarm and click RESET TO GREEN.

8. Enable TPM hierarchy:
   a. From the VMware vCenter vSphere Client, move one node to Enter Maintenance Mode.
   b. Log in to iDRAC to configure Secure Boot, and select the Configure tab > BIOS Settings > System Security > TPM >.
   c. Select TPM Hierarchy "Enable" and click Apply > OK > Apply and Reboot.
   d. Click Job queue. Wait for all jobs to complete 100%.
   e. Go to Dashboard > Virtual Console to see if console shows "successfully completed"; if yes, continue.
   f. Log in to the VMware vCenter vSphere Client and select Exit Maintenance Mode.
9. Perform Steps 7 and 8 on each node until all nodes have TPM hierarchy enabled from iDRAC.
10. Login VMware vCenter vSphere Client and select a data center.
11. Click the Monitor tab > Security to verify latest Attestation message as "Passed".



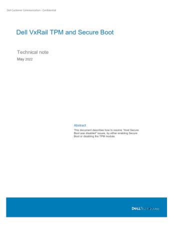
Security

Name	Attestation	Last verified	Attested by	TPM version	TXT	Message
dell208-02.locald...	Failed	02/23/2022, 10:24:13 AM	vCenter Server	N/A	N/A	Internal failure.
dell208-01.locald...	Failed	02/23/2022, 9:36:14 AM	vCenter Server	N/A	N/A	Host Secure Bo
dell208-03.locald...	Passed	02/23/2022, 1:13:56 PM	vCenter Server	2.0	true	
dell208-04.locald...	Passed	02/22/2022, 5:15:52 PM	vCenter Server	2.0	true	

Figure 16 Attestation passed.

Dell VxRail TPM and Secure Boot

Documents / Resources

	**DELL VxRail TPM and Secure Boot Technical** [pdf] Instructions VxRail TPM and Secure Boot, VxRail TPM, Secure Boot