

Durchführen von Hyperflex-Upgrades mit Best Practices

Inhalt

[Einleitung](#)

[Voraussetzungen](#)

[Anforderungen](#)

[Verwendete Komponenten](#)

[Schritte vor dem Upgrade](#)

[Versionsauswahl](#)

[Kompatibilität](#)

[Upgrade-Leitfäden](#)

[Überlegungen](#)

[Tools vor dem Upgrade](#)

[Hypercheck](#)

[Intersight-HealthCheck](#)

[Intersight HealthCheck-Demo](#)

[Kursvideos](#)

[Wichtige Prüfungen](#)

[Nicht verwendete Pakete in UCSM löschen](#)

[Überprüfen der Aktivierung von Spanning Tree Port \(STP\) PortFast auf Upstream-Switches](#)

[Physische Portfehler an Fabric Interconnect Ports oder Adaptern](#)

[Upstream konfiguriertes Speicherdaten-VLAN auf Standard- und gestreckten Clustern](#)

[MTU und Failover](#)

[Qualifizierung für Test-Upgrade](#)

[Validierung von Benutzern und Kennwörtern](#)

[Überprüfen des Eintritts in den Wartungsmodus](#)

[Überprüfen der vMotion-Konfiguration](#)

[Überprüfen Sie, ob EVC \(Enhanced VMotion Compatibility\) auf dem Cluster aktiviert ist.](#)

[Überprüfen der Affinitätsregeln auf virtuellen Systemen](#)

[ESXi Agent Manager \(EAM\)](#)

[SSH-Empfehlung](#)

[HXUSER-Sperre](#)

[Lockdown-Modus oder Beendet](#)

[Replikation](#)

[Laufwerksfehler](#)

[Austausch vorheriger Motherboards, Neubereitstellungen und Entfernen von Knoten](#)

[Diskrepanzen in HX und vCenter](#)

[HyperFlex vCenter - Registrierung](#)

[Zugehörige Informationen](#)

Einleitung

In diesem Dokument werden die Best Practices für ein erfolgreiches Upgrade des HyperFlex-Clusters beschrieben.

s

Voraussetzungen

Anforderungen

Cisco empfiehlt, sich mit folgenden Themen vertraut zu machen:

- Unified Computing System Manager (UCSM)
- Cisco Integrated Management Controller (CIMC)
- HyperFlex
- Elastic Sky X integriert (ESXi)
- vCenter
- Intersight

Verwendete Komponenten

- HyperFlex Connect 4.5(2e)
- UCSM 4.2(1f)
- Intersight
- vCenter 7.0 U3

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in Betrieb ist, stellen Sie sicher, dass Sie die möglichen Auswirkungen aller Befehle kennen.

Schritte vor dem Upgrade

Versionsauswahl

Die Entscheidung für die ausgewählte Zielversion richtet sich nach den Anforderungen der HyperFlex-Umgebung. Sein Zweck ist es, die neue Software von der alten zu verbessern, zu beheben und zu nutzen.

In den Versionshinweisen zu HyperFlex finden Sie Informationen wie neue Funktionen, neu unterstützte Hardware, Interoperabilität zwischen Komponenten, Richtlinien, Einschränkungen, Sicherheitskorrekturen und behobene Probleme.

Klicken Sie [hier](#), um die Versionshinweise zu überprüfen.

Kompatibilität

Bevor Sie das Hyperflex Cluster Upgrade ausführen, stellen Sie sicher, dass alle Versionen kompatibel sind. Cisco empfiehlt:

- Überprüfung der Interoperabilität der Versionen von HyperFlex, Unified Computing System (UCS) und ESXi/vCenter
- Überprüfen Sie alle Hardwaremodelle, die von der HyperFlex-Zielversion unterstützt werden.
- Die Anforderungen und Empfehlungen für die Cisco HyperFlex-Software finden Sie [hier](#).
- Alle dort aufgeführten UCS- und VMware-Versionen werden von Cisco vorgeschlagen und umfassend getestet.
- Cisco empfiehlt einige HyperFlex-Versionen, die zuverlässiger sind und intensiv getestet wurden.
- Die empfohlenen HyperFlex-Versionen können mit einem goldenen Stern gefunden werden, siehe [hier](#).

Upgrade-Leitfäden

Lesen Sie die Cisco HyperFlex-Upgrade-Leitfäden mit schrittweisen Anleitungen.

Die Leitfäden enthalten Informationen zu verschiedenen Szenarien, z. B.:

- Kombiniertes Upgrade. Upgrade aller HyperFlex-Cluster-Komponenten
- Individuelles Upgrade. Upgrade einer der HyperFlex Cluster-Komponenten
- Offline-Upgrade. Ist es erforderlich, dass der HyperFlex-Cluster heruntergefahren wird?
- Upgrade-Workflows abhängig vom Cluster-Typ (Standard, Strech, Edge)
- Upgrade-Leitfäden finden Sie [hier](#).
- Wenn der Cluster mit Cisco Intersight bereitgestellt wurde, verwenden Sie Intersight. Schauen Sie [hier](#) in den Leitfäden.

Überlegungen

- Cisco empfiehlt die Durchführung von Online-Upgrades zu Zeiten mit geringem Workflow-Datenverkehr oder Wartungszeitfenstern.
- Der Zeitaufwand für den Abschluss des Upgrades hängt von der Größe des Clusters ab.
- Ein Offline-Upgrade setzt voraus, dass alle virtuellen Gastsysteme offline sind.
- Cisco empfiehlt, die Versionshinweise für HyperFlex auf neu verfügbare Versionen zu überwachen, um zu verhindern, dass die aktuelle Version als End of Life (EOL) verwendet wird.
- Lesen Sie [hier](#) die Leitfäden zu den Cisco HyperFlex-Versionshinweisen.

Tools vor dem Upgrade

Führen Sie Health Checks durch, bevor das HyperFlex-Upgrade ausgeführt wird, um potenzielle Fehler zu beheben und unerwartete Verhaltensweisen während des Upgrades zu vermeiden.

Es gibt zwei verschiedene Methoden, mit denen diese Integritätsprüfungen durchgeführt werden können.

Hypercheck

Dieses Tool ist ein Dienstprogramm zur Durchführung proaktiver Selbstprüfungen bei HyperFlex-Systemen, um deren Stabilität und Ausfallsicherheit zu gewährleisten.

Hypercheck-Leitfäden finden Sie [hier](#).

Intersight-HealthCheck

Dies ist die empfohlene Methode für Vorabkontrollen. Es wird regelmäßig aktualisiert und enthält neue Fehlerbehebungsfunktionen, die potenzielle Fehlkonfigurationen leicht erkennen.

Es ist immer auf dem neuesten Stand, wenn es um neu entdeckte Vorbehalte geht, die während des Upgrade-Prozesses Unannehmlichkeiten darstellen. Informationen zum Intersight HealthCheck-Leitfaden finden Sie [hier](#).

Intersight HealthCheck-Demo

Schritt 1: Melden Sie sich bei Intersight an, und navigieren Sie zu Infrastructure Service. Wählen Sie dann HyperFlex Clusters und den Cluster aus.

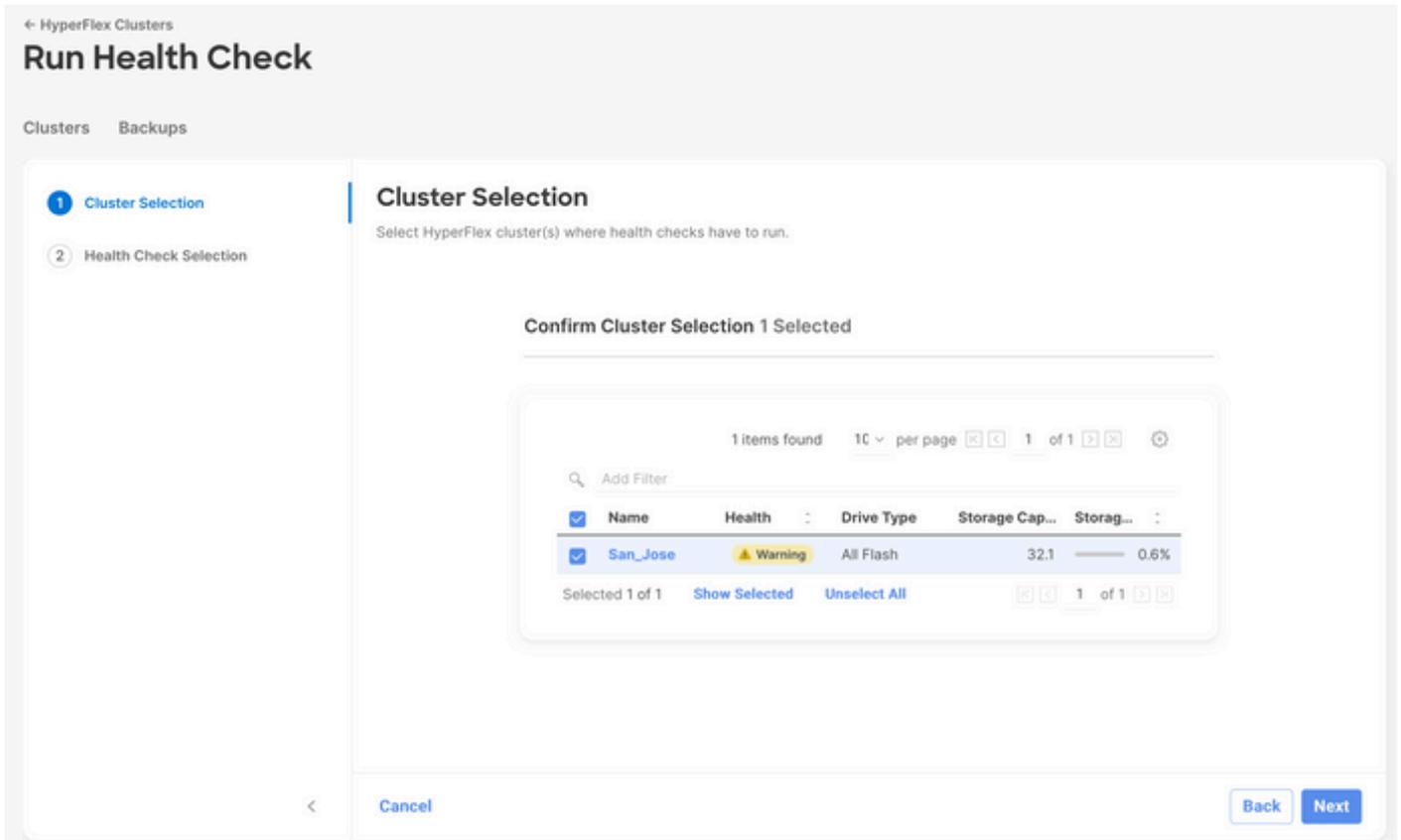
Beispiele zeigen einen Cluster mit dem Namen San_Jose. Wählen Sie im Dropdown-Menü Aktionen die Option Integritätsprüfung ausführen aus.

The screenshot displays the Intersight HyperFlex Clusters interface for a cluster named 'San_Jose'. The 'Health Check' tab is selected. The 'Details' section shows the overall health status as 'Warning' and the storage resiliency status as 'Healthy'. The 'General' section provides resource status, including storage utilization (32.1 TOTAL, 0.2 Used, 31.9 Free) and a capacity runway of 365+ days. An 'Actions' dropdown menu is open, listing various management actions, with 'Run Health Check' highlighted.



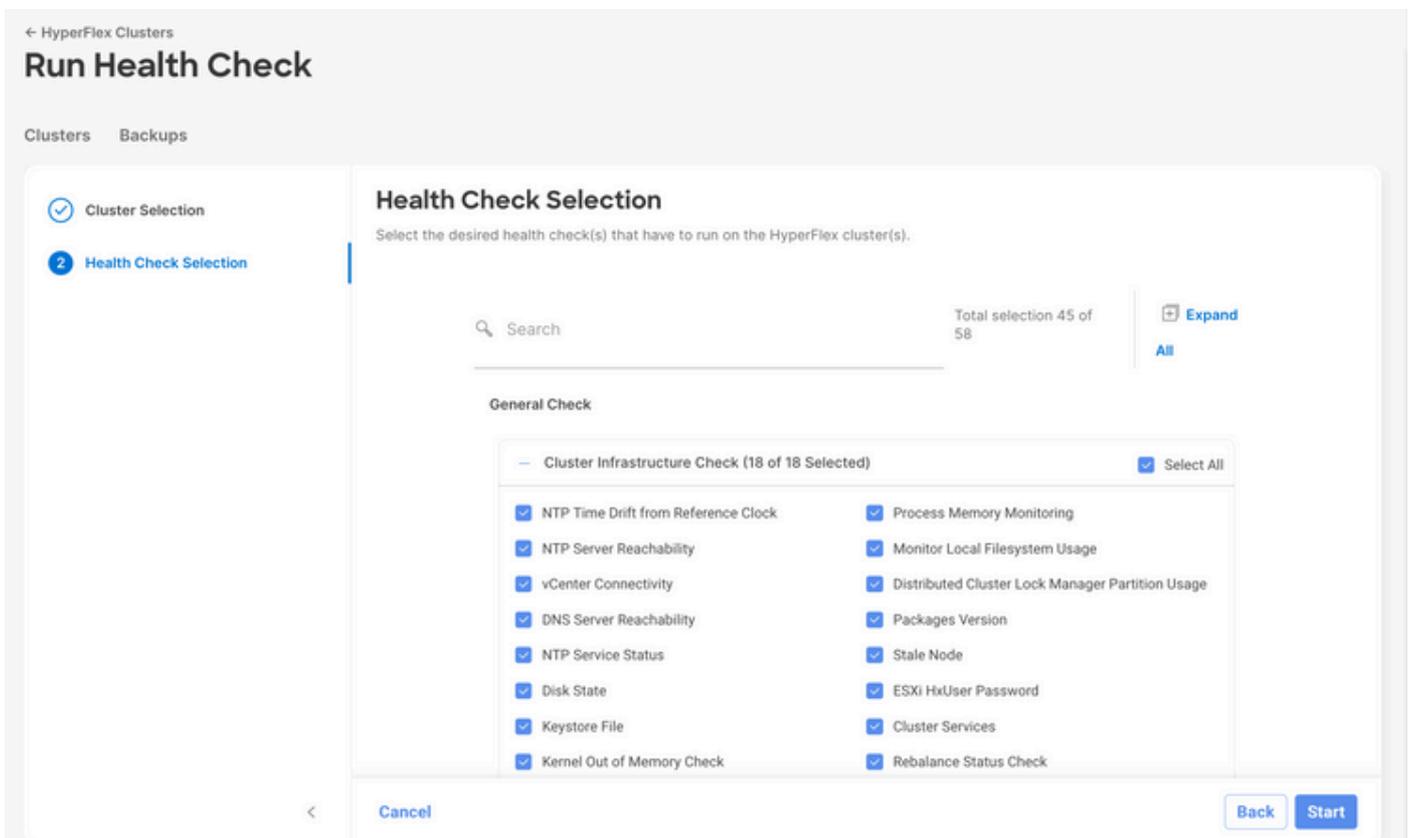
Hinweis: In diesem Beispiel werden Integritätsprüfungen für einen einzelnen Cluster gezeigt. Sie können die Integritätsprüfung für mehrere Cluster gleichzeitig auswählen und durchführen.

Bestätigen Sie den Cluster, und klicken Sie auf Weiter.



Mit dem Workflow können Sie bei Bedarf einige Prüfungen überspringen.

Schritt 2: Klicken Sie auf Start, um die Vorabprüfung zu starten.



Überprüfen Sie die Statusleiste, und warten Sie, bis die HealthCheck-Aufgabe abgeschlossen ist.

Requests



* All Requests +

Status In Progress Add Filter 1 items found 12 per page 1 of 1

Status
In Progress 1

Execution Type
Execute 1

<input type="checkbox"/>	Name	Status	Initiator	Target Type	Target Name	Start Time	Duration	ID	Execution Type	
<input type="checkbox"/>	Run Selected Hy...	In Progress 39%	@cisco...	HyperFlex Cluster	San_Jose	a minute ago	46 s	64b083b7696f6...	Execute	...

1 of 1

Schritt 3: Nach Abschluss der HealthCheck-Aufgabe können die Ergebnisse an verschiedenen Stellen überprüft werden.

Auf der Registerkarte "Integritätsprüfung" werden die allgemeinen Ergebnisse angezeigt. Das Beispiel wird so gefiltert, dass die Ergebnisse Passed und Not Run nicht angezeigt werden.

Overview Operate Profile Capacity Planning Performance **Health Check** Actions

Last Health Check Summary

General Check: 1 Failed, 42 Passed, 3 Unknown

Security Check

Test Run Time: Jul 13, 2023 5:09 PM

Reference: [Learn more at Help Center](#)

Results

Collapsed: Failed, Warning, Unknown, Passed, Not Run

Selected: General Check, Security Check

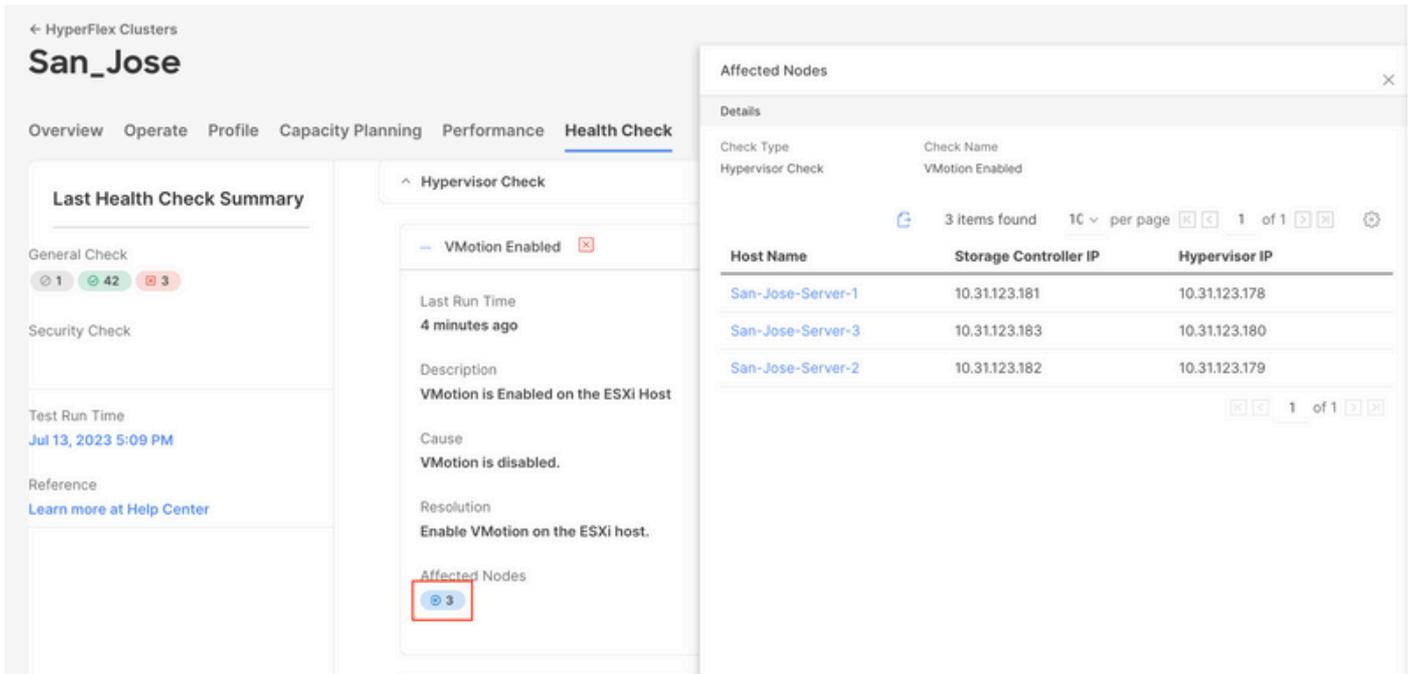
General Check

Hypervisor Check

- VMotion Enabled
- ESXi Cross Hosts Connectivity Check
- ESXi VIBs Check

Security Check

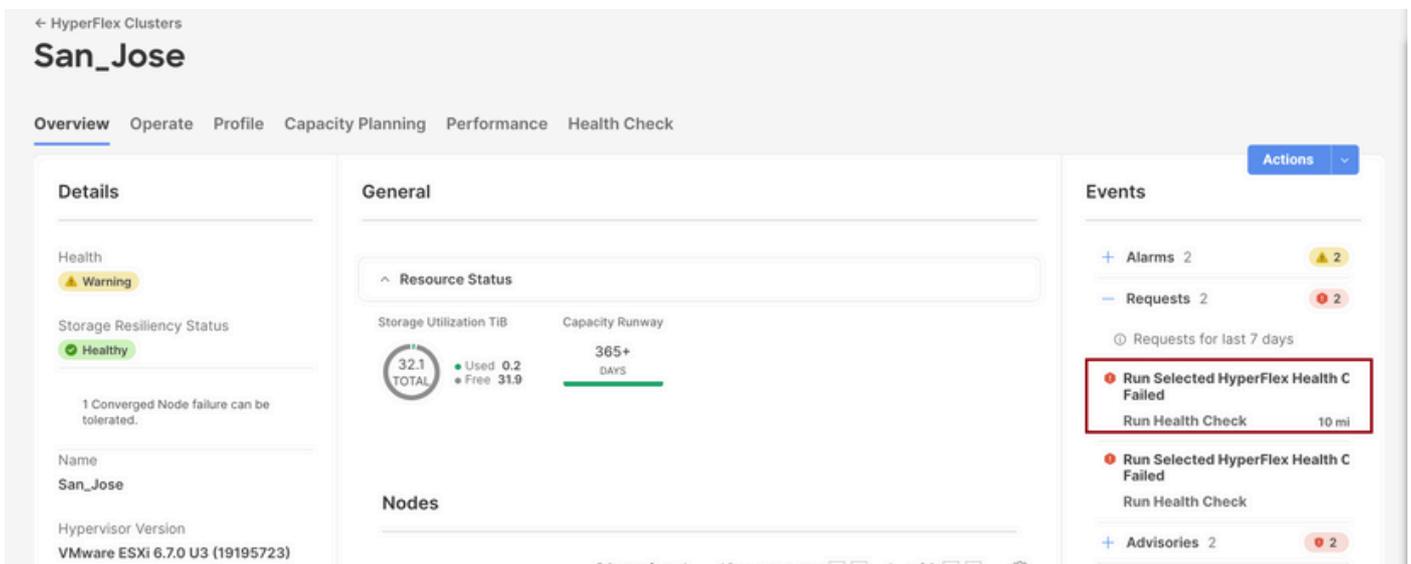
Schritt 4: Klicken Sie auf Betroffene Knoten, um die betreffenden Knoten zu überprüfen.



Aktivieren Sie auf der Registerkarte Overview (Übersicht) die Option Events (Ereignisse): Alarms, Requests (Anfragen) and Advisories (Ereignisse) (Warnungen, Anfragen und Ratgeber).

Erweitern Sie die einzelnen Veranstaltungen, um weitere Informationen zu erhalten.

Im Beispiel werden Anforderungen erweitert angezeigt. Klicken Sie auf Ausgewählte Hypercheck-Integritätsprüfungen ausführen fehlgeschlagen.



Es werden alle erfolgreichen und fehlgeschlagenen Prüfungen angezeigt.

Schritt 5: Klicken Sie auf den Umschalter für "Weitere Details anzeigen".

Run Selected HyperFlex Health Checks

Details

Status

● Failed

Name

Run Selected HyperFlex Health Checks

ID

64b083b7696f6e330121fbf8

Target Type

HyperFlex Cluster

Target Name

[San_Jose](#)

Execution Flow

Show Additional Details

❗ Validate and Update HyperFlex Cluster Health Check Execution State
3 HyperFlex health check(s) failed or completed with warnings.
For more information, please go to HyperFlex Clusters → San_Jose → Health Check tab.

✔ Invoke Check: ESXi to Controller VM Connectivity

✔ Invoke Check: /tmp Permissions

✔ Invoke Check: Controller Duplicate Folders

✔ Invoke Check: VFAT Disk Usage

✔ Invoke Check: SMART Disk Failures

✔ Invoke Check: ESXi HX User Account

Jede Aufrufüberprüfung kann erweitert werden, um eine detaillierte Ansicht der überprüften Elemente zu erhalten.

Es enthält detaillierte Informationen im JSON-Format für die Protokolle, Eingaben und Ausgänge.

Execution Flow

⚠ Invoke Check: VMotion Enabled

Jul 13, 2023 5:08 PM

[Logs](#)

```
1 {
2   {
3     "ConfigResCtx": {
4       "EntityName": "Jonah"
5     },
6     "Message": "VMotion is disabled on the ESXi host.",
7     "OwnerId": "{moId:64b083d8-...,instId:9d6ca46f-ae09-4eaf-...}",
8     "State": "Errored",
9     "Type": "Config"
10  }
11 }
```

[Inputs](#)

```
1 {
2   "HyperFlex Cluster M0ID": "6413a714-...",
3   "HyperFlex Cluster Name": "San_Jose",
4   "HyperFlex HealthCheck Definition M0ID": "63c057e-...",
5   "HxNode M0IDs": [
6     "6413a714-...",
7     "6413a714-...",
8     "6413a714-..."
9   ]
10 }
```

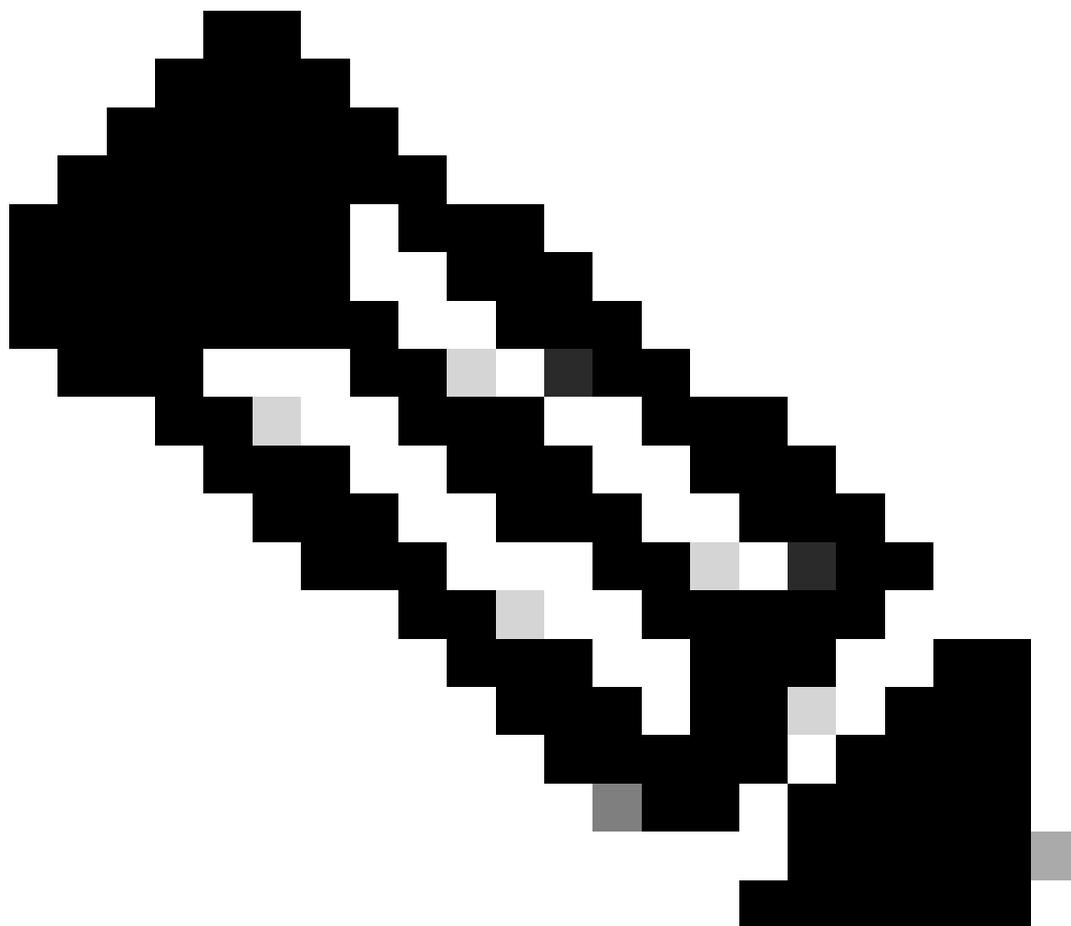
[Outputs](#)

```
4   "ConfigResCtx": {
5     "EntityName": "Jonah"
6   },
7   "Message": "VMotion is disabled on the ESXi host.",
8   "OwnerId": "{moId:64b083d8-...,instId:9d6ca46f-ae09-4eaf-...}",
9   "State": "Errored",
10  "Type": "Config"
```

Kursvideos

Hypercheck-[Video](#).

Intersight Health Check-[Video](#).



Hinweis: Bei einigen Korrekturen ist ein Eingreifen des Technical Assistance Center (TAC) erforderlich. Öffnen Sie bei Bedarf ein Ticket.

Wichtige Prüfungen

Nicht verwendete Pakete in UCSM löschen

Der UCS Manager-Firmware-Manager erfordert das Herunterladen der UCS-Firmware-Pakete in die Fabric Interconnect Boot-Flash-Partition. Überprüfen und löschen Sie alte Firmware-Pakete,

die auf den Komponenten nicht mehr verwendet werden, um zu vermeiden, dass die Boot-Flash-Partition der Fabric Interconnects mit unnötigen Dateien gefüllt wird.

Überprüfen Sie den Fabric Interconnect-Speicherplatz.

Schritt 1: Navigieren Sie zu Equipment (Geräte), wählen Sie Fabric Interconnects aus, und wählen Sie einen Fabric Interconnect aus. Das Beispiel zeigt Fabric Interconnect A (Primary).

Schritt 2: Wählen Sie im allgemeinen Bereich die Option Lokale Speicherinformationen aus, und erweitern Sie sie.

Equipment / Fabric Interconnects / Fabric Interconnect A (primary)

General Physical Ports Fans PSUs Physical Display FSM Neighbors Faults Events Statistics

Fault Summary

0 3 1 0

Status

Overall Status : **Operable**

Thermal : **OK**

Ethernet Mode : **End Host**

FC Mode : **End Host**

Admin Evac Mode : **Off**

Oper Evac Mode : **Off**

Actions

- Configure Evacuation
- Configure Unified Ports
- Internal Fabric Manager
- LAN Uplinks Manager
- NAS Appliance Manager
- SAN Uplinks Manager
- SAN Storage Manager
- Enable Ports
- Disable Ports
- Set Ethernet End-Host Mode
- Set Ethernet Switching Mode
- Set FC End-Host Mode
- Set FC Switching Mode

Physical Display

Properties

Name : **A**

Product Name : **Cisco UCS 6248UP**

Vendor : **Cisco Systems, Inc.**

Revision : **0**

Available Memory : **12.543 (GB)**

Locator LED :

PID : **UCS-FI-6248UP**

Serial : **[REDACTED]**

Total Memory : **15.770 (GB)**

Part Details

Local Storage Information

Advanced Filter Export Print

Partition	Size (MB)	Used
bootflash	16,329	79%
opt	3,877	4%
spare	5,744	6%
vsar_sysmgr	2,000	11%
vsar_tmp	600	1%
volatile	240	1%

Überprüfen der Aktivierung von Spanning Tree Port (STP) PortFast auf Upstream-Switches

Wenn der Upstream-Switch den Befehl STP PortFast unterstützt, wird dringend empfohlen, diesen zu aktivieren. Wenn Sie die PortFast-Funktion aktivieren, wechselt ein Switch oder ein Trunk-Port sofort oder bei einem Verbindungsereignis in den STP-Weiterleitungsstatus, wodurch der Status "Zuhören" und "Lernen" umgangen wird.

Die PortFast-Funktion ist auf Portebene aktiviert, und dieser Port kann entweder ein physischer oder ein logischer Port sein.

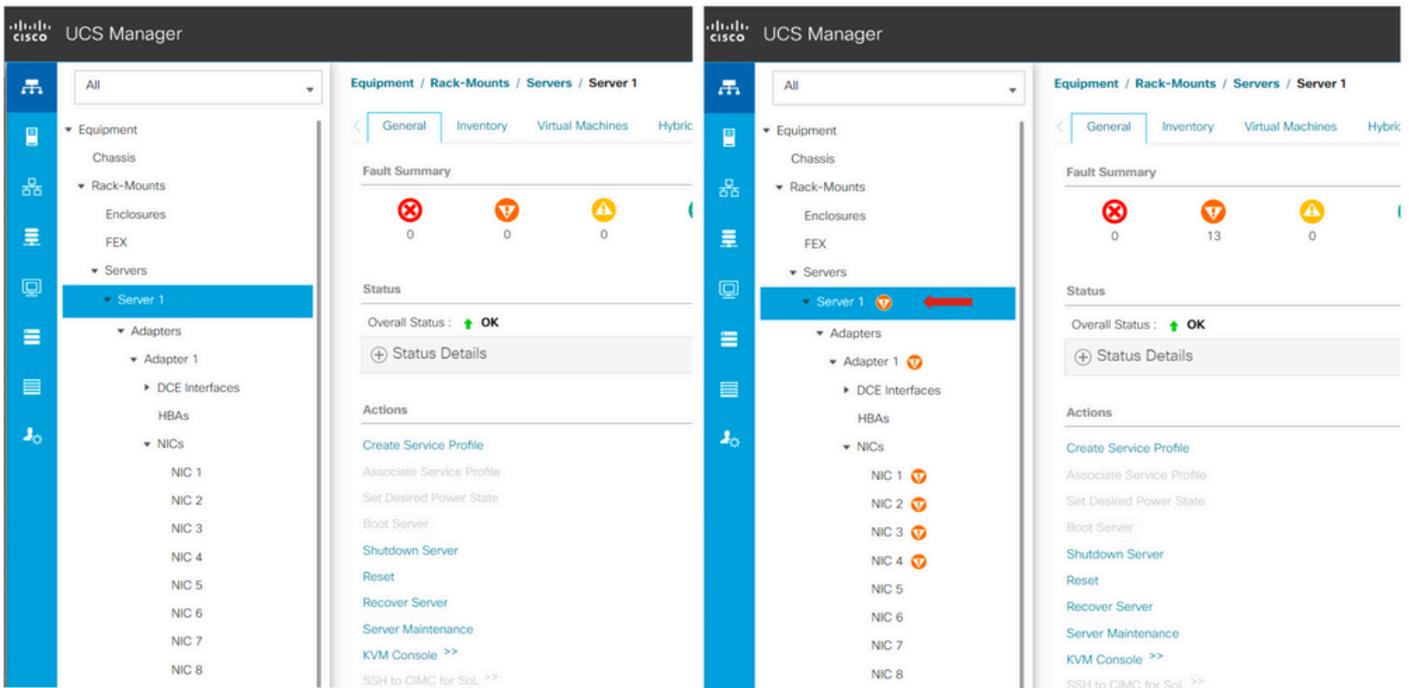
Physische Portfehler an Fabric Interconnect Ports oder Adaptern

Überprüfen Sie in UCSM alle Fehler in Verbindung mit Port-Fehlern an Uplinks oder Server-Ports, um Failover-Szenarien zu vermeiden.

Schritt 1: Melden Sie sich bei UCSM an, und navigieren Sie zur Registerkarte "Equipment" (Geräte), erweitern Sie "Rack-Mounts" und "Servers" (Server). Das Beispiel zeigt Server 1.

Schritt 2: Erweitern Sie Adapter, und erweitern Sie dann NICs.

Schritt 3: Überprüfen Sie, ob alle Netzwerkkarten (NICs) sauber sind.



Upstream konfiguriertes Speicherdaten-VLAN auf Standard- und gestreckten Clustern

Das VAN für Speicherdaten muss auf dem Upstream-Gerät konfiguriert werden, um sicherzustellen, dass bei einem Ausfall des Fabric Interconnects B ein Failover erfolgt.

Stellen Sie sicher, dass alle Anforderungen im HyperFlex-[Installationshandbuch](#) aufgeführt sind.

MTU und Failover

Stellen Sie sicher, dass die Netzwerkverbindungen für beide Pfade auf den Virtual-Machine-Netzwerkschnittstellenkarten (vmnics) funktionieren.



Hinweis: Um den Upstream-Verbindungstest durchzuführen, überprüfen Sie dieses [Video](#).

In diesem [Leitfaden](#) können Sie überprüfen, ob das richtige NIC-Teaming auf Basis der UCS-Richtlinien richtig konfiguriert ist.

Warten Sie bei einem Infrastruktur-Upgrade, bis die ESXi-Uplinks aktiviert sind, bevor Sie das andere Fabric Interconnect neu starten.

Qualifizierung für Test-Upgrade

Ab Cisco HyperFlex Version 4.0(2a) zeigt die Upgrade-Seite das Ergebnis des letzten Tests zur Qualifizierung für Cluster-Upgrades und die letzte getestete Version des UCS-Servers, der HX-Datenplattform und/oder ESXi an.

Melden Sie sich bei HX Connect an, um die Berechtigungsprüfung für das Upgrade durchzuführen:

Schritt 1: Wählen Sie Upgrade > Test Upgrade Eligibility (Upgrade > Test-Upgrade-Berechtigung).

Schritt 2: Aktivieren Sie das Kontrollkästchen UCS Server-Firmware, um die Berechtigung für Upgrades der UCS Server-Firmware zu testen.

Schritt 3: Geben Sie den vollqualifizierten Domänennamen (Fully Qualified Domain Name, FQDN) oder die IP-Adresse, den Benutzernamen und das Kennwort von Cisco UCS Manager ein. Klicken Sie im Feld "Current Version" (Aktuelle Version) auf Discover (Ermitteln), um die Version des UCS-Firmware-Pakets auszuwählen, die vor dem Upgrade validiert werden muss.

Schritt 4: Aktivieren Sie das Kontrollkästchen HX Data Platform, um die Upgrade-Berechtigung für die HyperFlex Data Platform zu testen.

Schritt 5: Geben Sie den vCenter-Benutzernamen und das vCenter-Kennwort ein. Laden Sie das Upgrade-Paket für die Cisco HyperFlex Data Platform hoch, das vor dem Upgrade validiert werden muss.

Schritt 6: Aktivieren Sie das Kontrollkästchen ESXi, um zu testen, ob ESXi für ein Upgrade qualifiziert ist.

Schritt 7. Geben Sie den Benutzernamen und das Kennwort des vCenter-Administrators ein. Laden Sie das Cisco HyperFlex Custom Image Offline-Paket hoch, das vor dem Upgrade validiert werden muss.

Schritt 8: Klicken Sie auf Validieren.

Schritt 9. Der Fortschritt des Qualifizierungstests für Upgrades wird angezeigt.

Validierung von Benutzern und Kennwörtern

Passwörter überprüfen für:

- vCenter-Administrator
- ESXi-Root
- Storage Controller Virtual Machine (SCVM)-Admin und -Root

Überprüfen des Eintritts in den Wartungsmodus

Stellen Sie sicher, dass virtuelle Systeme, die auf dem Host ausgeführt werden, im Wartungsmodus auf einen anderen Host migriert werden können. Wenn eine VM nicht migriert werden kann, muss sie ausgeschaltet werden. Wenn eine VM nicht automatisch migriert, aber manuell migriert werden kann, prüfen Sie, ob ein Problem mit DRS vorliegt.

Überprüfen Sie, ob DRS aktiviert ist, und stellen Sie diese Option auf vollautomatisiert ein, sofern eine Lizenz für DRS vorliegt. Wenn DRS deaktiviert ist, ist ein manueller Eingriff erforderlich, um die VMs manuell zu vMotion zu bewegen, wenn dies durch den Upgrade-Prozess angefordert wird.

Weitere Informationen finden Sie im VMware-[Leitfaden](#).

Überprüfen der vMotion-Konfiguration

Bestätigen Sie, dass vMotion ordnungsgemäß konfiguriert wurde, um nicht abgeschlossene Wartungsmodusaufgaben zu vermeiden.

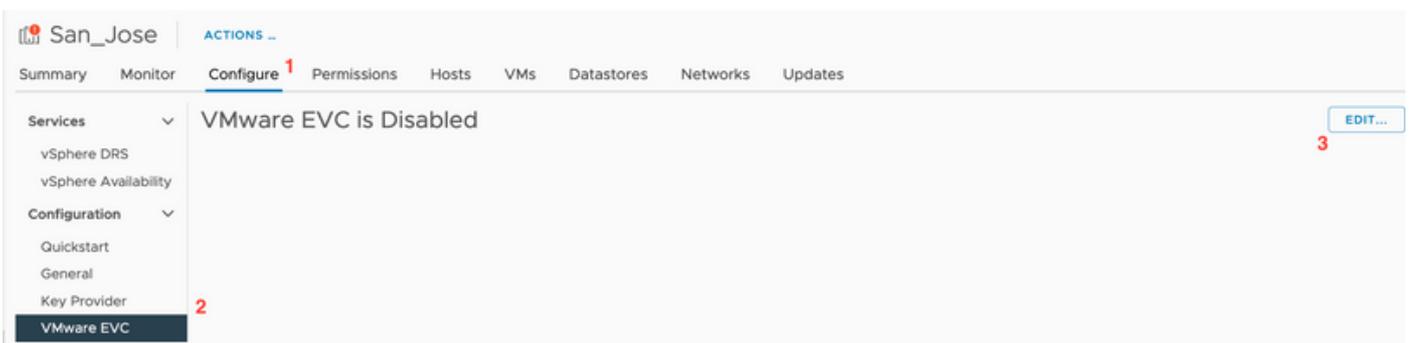
Weitere Informationen zur vMotion-Fehlerbehebung finden Sie [hier](#).

Überprüfen Sie, ob EVC (Enhanced VMotion Compatibility) auf dem Cluster aktiviert ist.

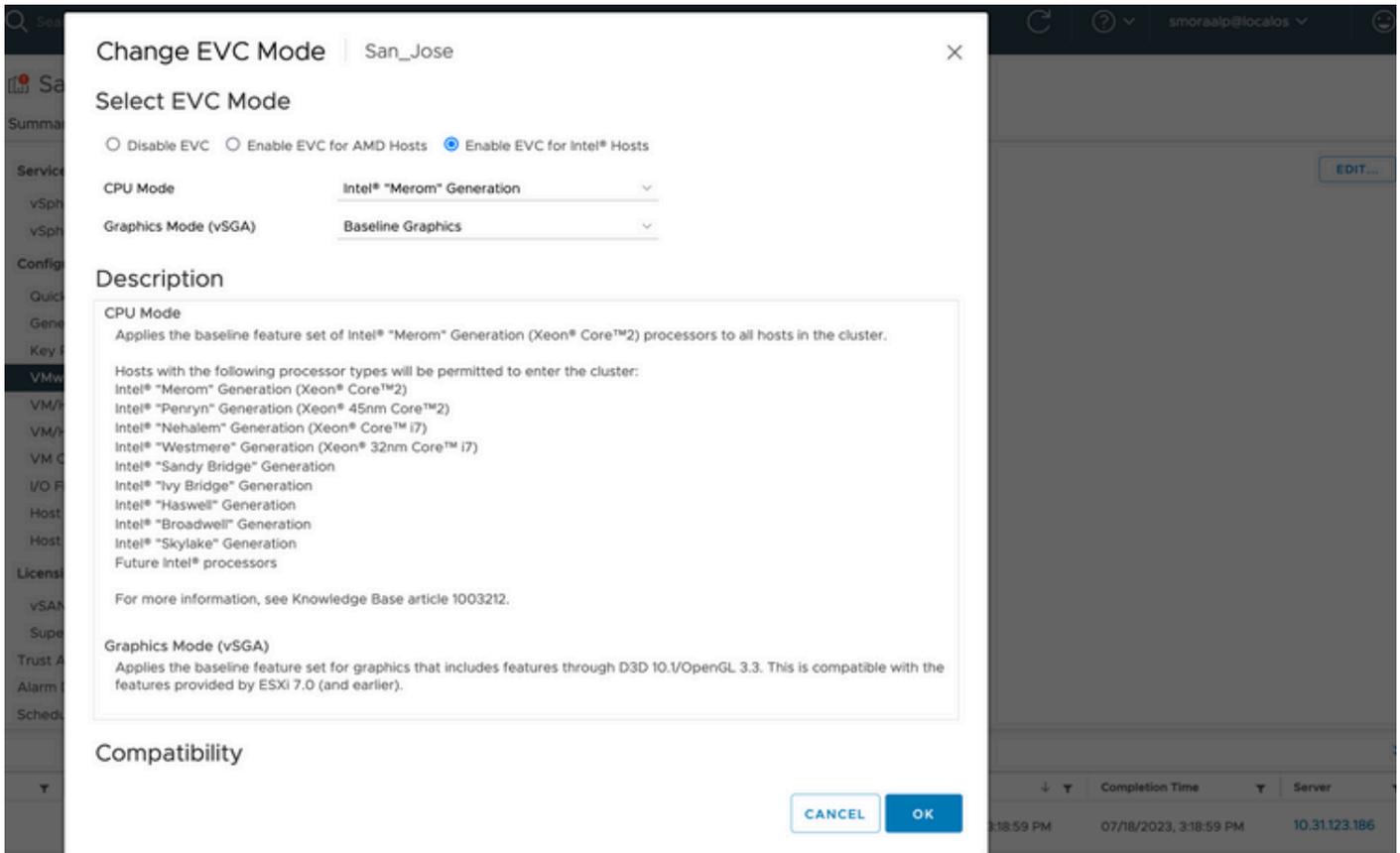
Schritt 1: Melden Sie sich bei VMware vCenter an, und navigieren Sie zu "Startseite" und "Cluster".

Schritt 2: Klicken Sie auf vCenter Cluster. Dieses Beispiel zeigt einen Cluster mit dem Namen San_Jose.

Schritt 3: Wählen Sie Konfigurieren, klicken Sie unter Konfiguration auf VMware EVC, und wählen Sie Bearbeiten aus.



Schritt 4: Stellen Sie sicher, dass Sie den EVC-Modus für den jeweils verwendeten Prozessor in Enabled (Aktiviert) ändern.



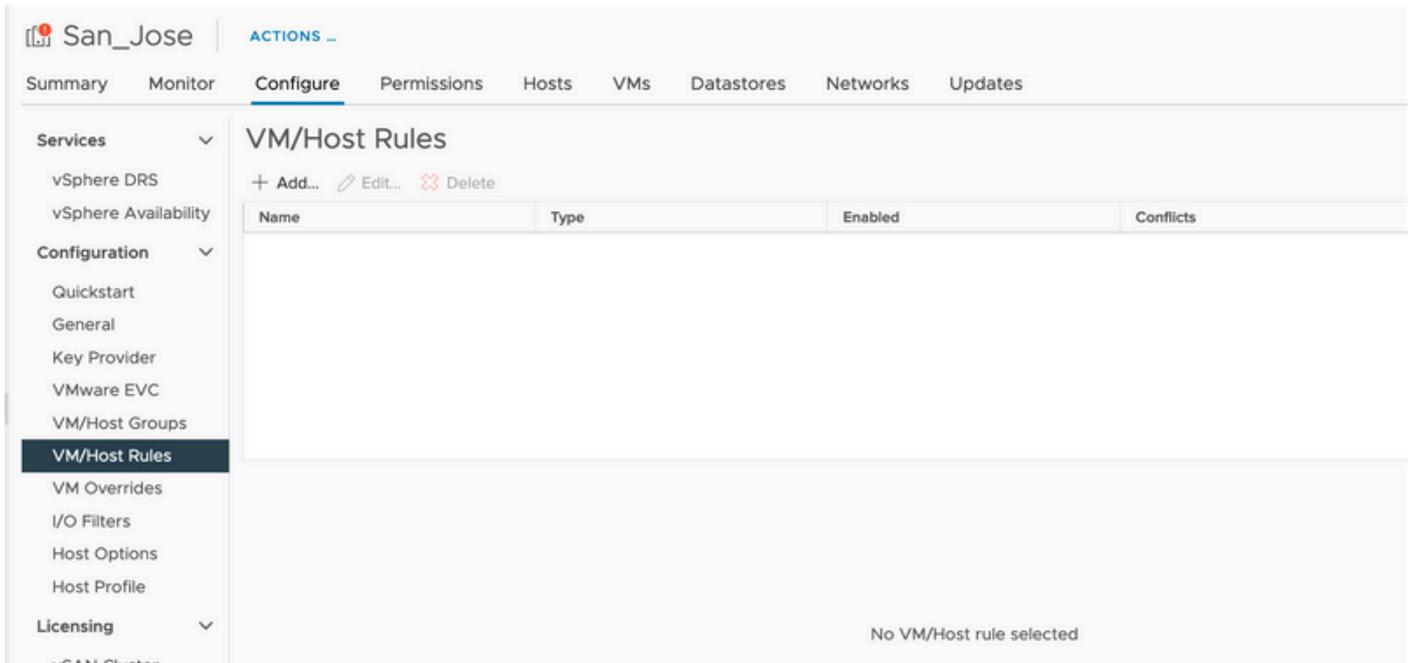
Überprüfen der Affinitätsregeln auf virtuellen Systemen

Überprüfen Sie, ob auf der Gast-VM eine Affinitätsregel erstellt wurde.

Schritt 1: Wechseln Sie vom VMware vCenter zum Cluster.

Schritt 2: Navigieren Sie zu Startseite und Cluster. Dieses Beispiel zeigt einen Cluster mit dem Namen San_Jose.

Schritt 3: Wählen Sie Konfigurieren aus. Wählen Sie unter Konfiguration die Option VM-/Host-Regeln aus, und überprüfen Sie, ob eine Regel erstellt wurde.



ESXi Agent Manager (EAM)

Ab HXDP 5.0(x) und höheren Versionen wird EAM nicht mehr auf den ESXi-Hosts zum Verwalten des SCVMs-Netzwerks und -Datenspeichers verwendet.

Ab HXDP 5.0(x) und früheren Versionen benötigen Netzwerke und Datenspeicher SCVM-Informationen.

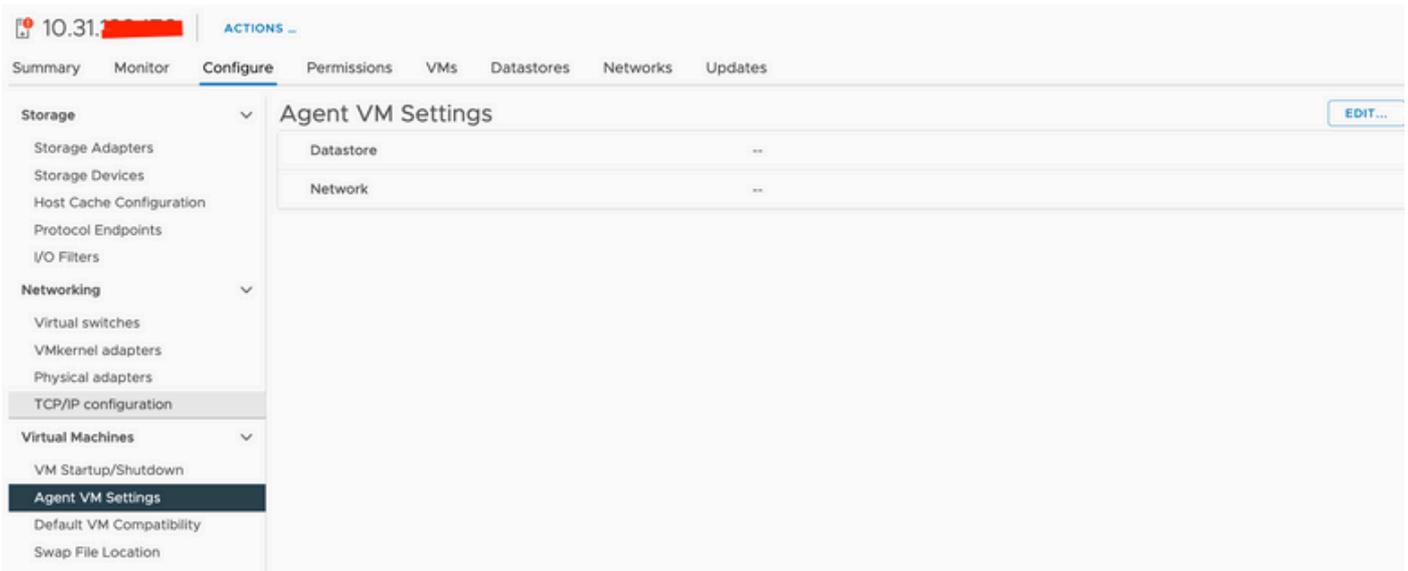
Überprüft, ob der ESXi Agent Manager (EAM)-Status normal ist.

Schritt 1: Bei VMware vCenter anmelden

Schritt 2: Navigieren Sie zu "Home" und "Clusters", und navigieren Sie zu jedem ESXi-Knoten.

Schritt 3: Navigieren Sie im VMware vCenter-Cluster zu Konfigurieren, und wählen Sie unter Virtuelle Systeme die Option Agent VM Settings aus.

Im Beispiel werden Leerzeichen angezeigt, da der HyperFlex-Cluster in 5.0(2c) vorhanden ist.



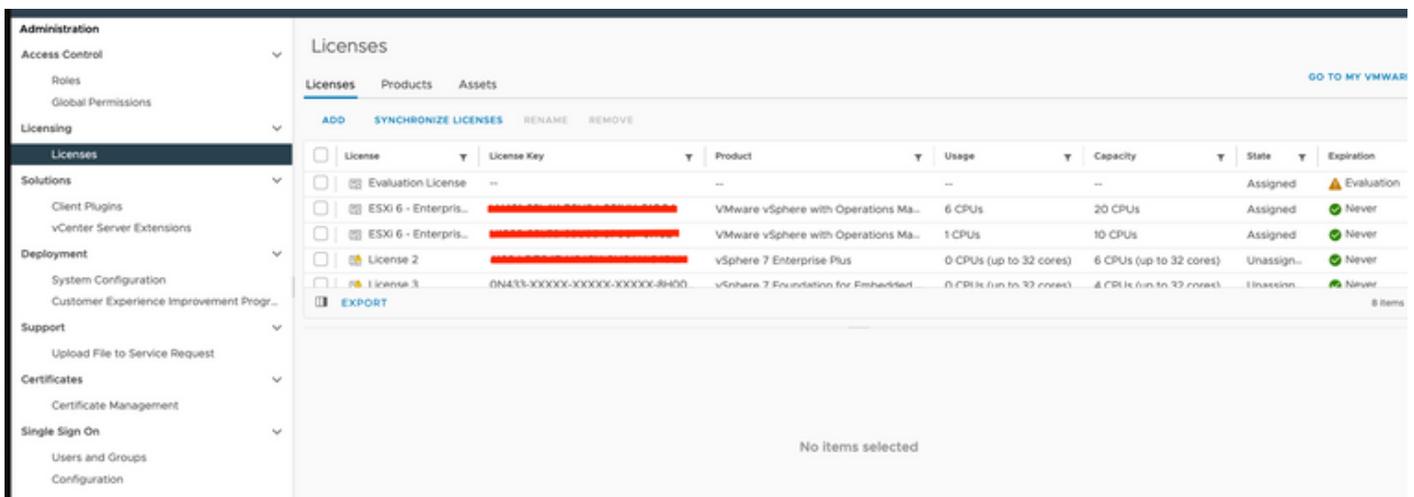
Wenn EAM verwendet wird, stellen Sie sicher, dass in vCenter keine Zertifikatfehler angezeigt werden.

Weitere EAM-Informationen finden Sie [hier](#).

vCenter- und ESXi-Lizenzen

Wenn Sie ein Upgrade von 6.x auf 7.0 durchführen, stellen Sie sicher, dass Sie vor dem Upgrade über die neuen Lizenzen verfügen.

Nach dem Upgrade haben Sie nur noch 60 Tage Zeit, sich im Evaluierungsmodus zu befinden.



SSH-Empfehlung

HXUSER-Sperre

Fehlgeschlagene Anmeldeversuche können dazu führen, dass ESXi-Benutzer gesperrt werden.

So überprüfen Sie den Benutzerstatus von "hxuser" oder "root"

Schritt 1: Öffnen Sie eine SSH-Sitzung als Root im ESXi-Knoten.

Schritt 2: Führen Sie `pam_tally2 --user hxuser` (oder `root user`) aus.

Schritt 3: Stellen Sie sicher, dass `hxuser` oder `root` gesperrt wurde.

```
[root@esxi1:~] pam_tally2 --user hxuser
Login Failures Latest failure From
hxuser 0
[root@esxi1:~] pam_tally2 --user root
Login Failures Latest failure From
root 0
[root@esxi1:~]
```

So entsperren Sie erwähnte ESXi-Benutzer:

Schritt 1: Führen Sie `pam_tally2 --user hxuser --reset` (oder `root user`) aus.

Schritt 2: Stellen Sie sicher, dass die Anzahl der Fehler auf 0 verringert wird.

```
[root@esxi1:~] pam_tally2 --user hxuser --reset
Login Failures Latest failure From
hxuser 0
```

```
[root@esxi1:~] pam_tally2 --user root --reset
Login Failures Latest failure From
root 0
```

Lockdown-Modus oder Beendet

Um die Sicherheit auf dem ESXi-Host zu erhöhen, müssen Sie den Lockdown-Modus aktivieren. Diese Konfiguration verhindert HyperFlex-Upgrades aufgrund des Sperrmodus, der für ein HyperFlex-Cluster-Upgrade deaktiviert werden muss.

So deaktivieren Sie den ESXi-Sperrmodus:

Schritt 1: Führen Sie SSH direkt auf dem ESXi-Host als Root aus.

Schritt 2: Drücken Sie F2 für die Ersteinrichtung.

Schritt 3: Geben Sie die Root-Anmeldeinformationen ein, um das DUCI-Setup zu öffnen.

Schritt 4: Wechseln Sie zu den Einstellungen für die Moduskonfiguration konfigurieren, und

ändern Sie sie in disabled (Deaktiviert).

Um den Sperrmodus in vCenter zu deaktivieren,

Schritt 1: Navigieren Sie zum Host im vSphere Web Client-Inventar.

Schritt 2: Klicken Sie auf die Registerkarte Verwaltung und dann auf Einstellungen. (mit 6.7, Klicken Sie auf die Registerkarte Konfigurieren).

Schritt 3: Wählen Sie unter System die Option Sicherheitsprofil aus.

Schritt 4: Klicken Sie im Bereich Lockdown Mode auf Edit.

Schritt 5: Klicken Sie auf Sperrmodus, und wählen Sie eine der Optionen für den Sperrmodus aus.

Weitere Informationen zum Sperrmodus finden Sie [hier](#).

Replikation

Wenn die Replikation konfiguriert und aktiviert ist, muss sie vor dem Upgrade angehalten werden.

Unterbrechen Sie die Replikation mit dem Befehl `run stcli dp schedule pause`, und aktivieren Sie sie nach dem Upgrade mit dem Befehl `stcli dp schedule resume`.

Laufwerksfehler

Laufwerksfehler führen zu einem Fehler beim Upgrade des HyperFlex-Clusters. So überprüfen Sie die HyperFlex Connect-GUI auf in der Sperrliste aufgeführte oder ignorierte Festplatten:

Schritt 1: Öffnen Sie die HyperFlex Connect-GUI unter `https://<HyperFlex-virtual-ip-address or fqdn>`.

Schritt 2: Gehen Sie zu Systeminformationen, und wählen Sie dann Registerkarte Systemübersicht.

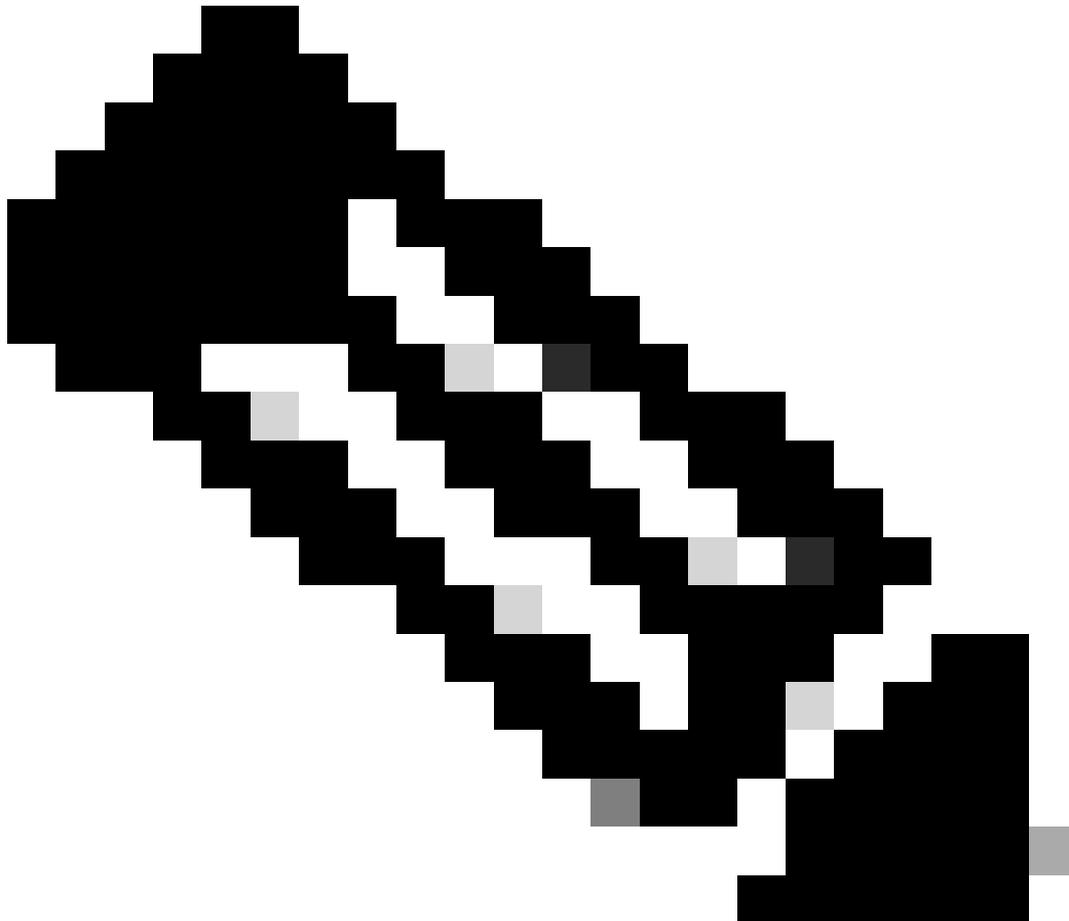
Schritt 3: Überprüfen Sie, ob Datenträgerfehler vorliegen.

The screenshot displays the HyperFlex Connect GUI. At the top, there are tabs for 'System Overview', 'Nodes', and 'Disks'. The 'System Overview' tab is active, showing details for a cluster named 'San_Jose' which is 'ONLINE'. Key information includes: License Type (Datacenter Advantage), License Status (In compliance), vCenter (https://...), Uptime (73 days, 6 hours, 9 minutes, 38 seconds), Hypervisor (6.7.0-19195723), HXDP Version (4.5.2e-39752), Total Capacity (32.14 TB), Available Capacity (31.94 TB), Data Replication Factor (3), DNS Server(s), NTP Server(s), and Controller Access over SSH. Below this, the 'Hyperconverged Nodes' section is visible, with a 'Disk View Options' dropdown. A 'Disk Overview' section is highlighted with a red box, showing a bar chart for 26 disks. The first 11 disks are green, indicating they are in use, and the remaining 15 are grey, indicating they are empty slots.

Festplattenprobleme müssen vom Cisco TAC behoben werden.

Austausch vorheriger Motherboards, Neubereitstellungen und Entfernen von Knoten

Durch den Austausch der Hauptplatine werden auch die vorherigen Host-UIDs durch die neuen IDs ersetzt. Wenn bei den Austauschaufgaben Probleme aufgetreten sind, kann die Nichtübereinstimmung der UIDs dazu führen, dass das HyperFlex-Upgrade fehlschlägt.



Hinweis: Intersight HealthCheck empfiehlt bei einer ID-Diskrepanz eine Verbindung zwischen dem HyperFlex-Cluster und Intersight und die Ausführung von HyperFlex Cluster HealthCheck.

Vergleichen Sie zum Austausch der Hauptplatine die stNode-UUID der ESXi CLI, um sicherzustellen, dass die UUID-Informationen mit der UUID im Hyperflex-Cluster übereinstimmen.

So erfassen Sie die UID:

Schritt 1: Öffnen Sie eine SSH-Sitzung mit dem ESXi-Knoten als Root.

Schritt 2: Führen Sie den folgenden Befehl aus: `hostsvc/hostsumm | grep -i uuid | grep -v inst`.

Schritt 3: Sammeln Sie die UUID-Informationen.

```
[root@esxi2:~] vim-cmd hostsvc/hostsumm | grep -i uuid | grep -v inst
      uuid = "1f82077d-6702-214d-8814-e776ffc0f53c", <----- ESXi2 ID
[root@esxi2:~]
[root@esxi2:~]
```

So rufen Sie die UUID-Informationen auf dem HyperFlex-Clusterknoten ab:

Schritt 1: Führen Sie SSH für die IP-Adresse des HyperFlex-Clusters aus.

Schritt 2: Ausführen des Befehls `stcli cluster info | mehr`.

Schritt 3: Erfassen Sie die Knoten-IDs.

```
hxshell:~$ stcli cluster info | more
stNodes:
-----
id: c4a24480-e935-6942-93ee-987dc8e9b5d9
type: node
name: esxi1
-----
id: 1f82077d-6702-214d-8814-e776ffc0f53c <----- ID for ESXi2
type: node
name: esxi2
-----
id: 50a5dc5d-c419-9c48-8914-d91a98d43fe7
type: node
name: esxi3
-----
```

Stellen Sie sicher, dass die `stcli` Cluster-Info-IDs mit den Informationen übereinstimmen, die auf den ESXi-Knoten angezeigt werden.

Diskrepanzen in HX und vCenter

Überprüfen Sie, ob vCenter-Informationen wie Rechenzentrums-, Cluster- und Datenspeichernamen auf dem HyperFlex-Cluster mit vCenter übereinstimmen. Wenn die Informationen nicht übereinstimmen, schlägt das HyperFlex-Cluster-Upgrade fehl.

Aktuelle Informationen finden Sie unter:

Schritt 1: Führen Sie SSH in der HyperFlex-Cluster-IP als `admin` aus.

Schritt 2: STCLI-Cluster-Informationen ausführen | `grep -i vcenter`.

Schritt 3: Sammeln Sie die registrierten vCenter-Informationen im Cluster.

```
hxshell:~$ stcli cluster info | grep -i vcenter
vCenterClusterName: vcenter-cluster
vCenterDatacenter: hx-cluster-name
vCenterURL: https://vcenter-ur1
vCenterDatacenterId: datacenter-name
vCenterClusterId: domain-c5124
vCenterUr1: https://vcenter-ur1
vCenterVersion: 7.0.2 Build-18455184
```

HyperFlex vCenter - Registrierung

Beachten Sie, dass bei Namen zwischen Groß- und Kleinschreibung unterschieden wird. Wenn der Name und die vCenter-Informationen aus der vorherigen Ausgabe nicht übereinstimmen, ist eine erneute vCenter-Registrierung erforderlich.

Um das vCenter erneut im Hyperflex-Cluster zu registrieren, sehen Sie sich das Video zur vCenter-Registrierung [hier an](#).

So registrieren Sie das vCenter neu:

Schritt 1: Führen Sie als Administrator SSH für die Cluster-IP-Adresse aus.

Schritt 2: Führen Sie den Befehl `stcli cluster reregister` aus.

```
stcli cluster reregister [-h] --vcenter-datacenter NEWDATACENTER --vcenter-cluster NEWVCENTERCLUSTER --
```

```
hxshell:~$ stcli cluster reregister --vcenter-datacenter MyData-Center --vcenter-cluster Cluster-Name -
Reregister StorFS cluster with a new vCenter ...
Enter NEW vCenter Administrator password:
Cluster reregistration with new vCenter succeeded
hxshell:~$
```

Zugehörige Informationen

- [HyperFlex-Cluster - Integritätsprüfung](#)
- [Ausführen von Hypercheck: Hyperflex Health & Pre-Upgrade Check-Tool](#)
- [Technischer Support und Dokumentation für Cisco Systeme](#)

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.