Cisco
Customer Experience

Ask the Experts

Day 2 運用：Cisco HyperFlex
(Day2 Operations : Cisco Hyperflex)

2024年6月18日

Disclaimer

This document is Cisco Confidential information provided for your internal business use in connection with the Cisco Services purchased by you or your authorized reseller on your behalf. This document contains guidance based on Cisco's recommended practices.

You remain responsible for determining whether to employ this guidance, whether it fits your network design, business needs, and whether the guidance complies with laws, including any regulatory, security, or privacy requirements applicable to your business.

免責

この文書は、お客様またはお客様の代理人である認定リセラーが購入したシスコサービスに関連して、お客様が社内業務において使用することを目的としてシスコが提供するシスコの機密情報です。この文書にはシスコが推奨するプラクティスに基づく手引きが記載されています。

お客様は、この手引きを使用するか否かやお客様のネットワーク設計および業務上のニーズにこの手引きが適合しているか否か、さらにはこの手引きが法律（お客様の業務に適用される規制上の要件、セキュリティ上の要件およびプライバシーに関する要件を含みます）に準拠しているか否かを判断する責任を引き続き負います。

アジェンダ

01 アクセス権限の管理 (Intersight)

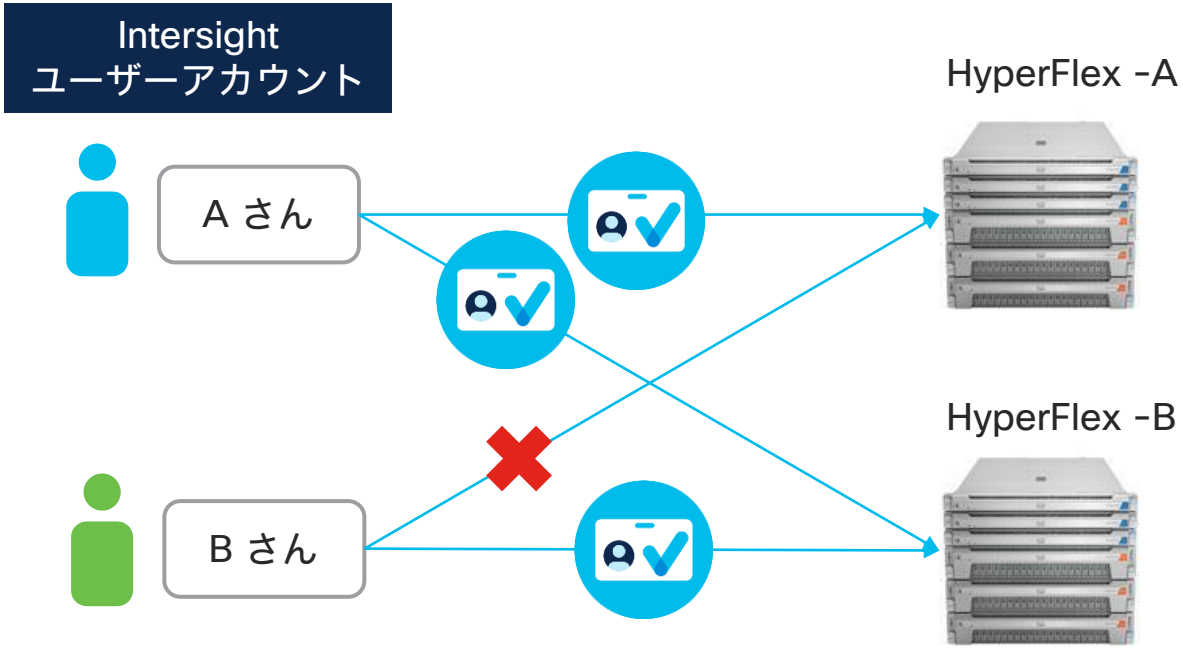
02 障害予防
・ハードウェア互換性リスト(HCL)
・アドバイザリ機能

03 障害対応
・Proactive RMA
・Connected TAC
・ログ取得機能 (マニュアル)

04 フィードバック機能

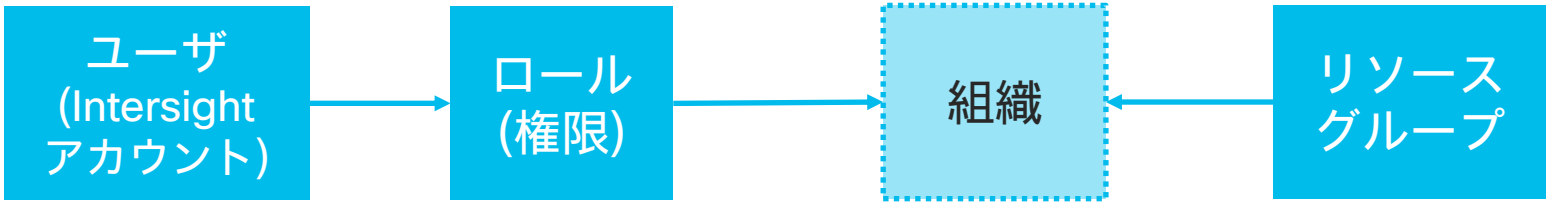
アクセス制御管理
(Intersight RBAC 機能)

アクセス制御管理



アクセス制御管理（組織とロール）

ロールベース アクセス コントロール（RBAC）



<定義済みのロール>
- Account Administrator
- Read-only
- Device Technician
- Device Administrator
- HyperFlex Cluster Administrator
- Server Administrator
- User Access Administrator

<組織>
ロールとリソース
グループの組み合わせ

<リソースグループ>
管理対象のグループ化

障害予防

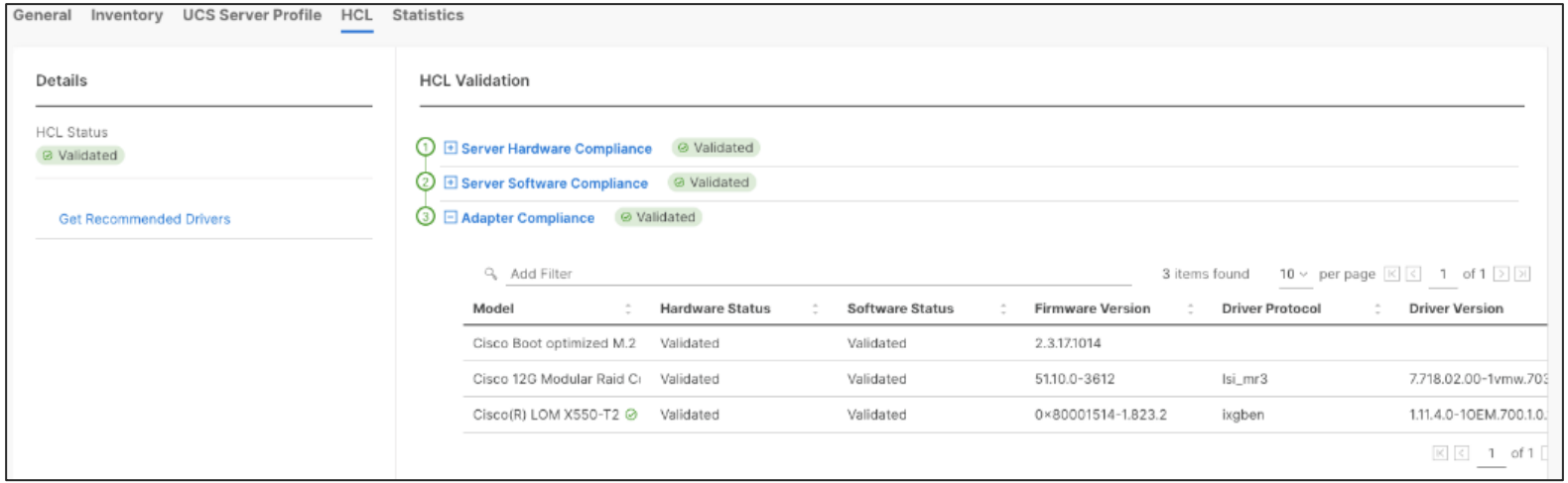
・ハードウェア互換性リスト(HCL)

ハードウェア互換性リスト(HCL)

概要

ハードウェア互換性リストとは、シスコ(パートナ)でテストおよび検証されたリスト
(ハードウェアとソフトウェアの組み合わせにおける動作保証)

- ハードウェア：UCS Manager / CIMC から情報を取得
- ソフトウェア：OS に導入されたモジュールによって情報を取得



ハードウェア互換性リスト(HCL)

概要

1 Server Hardware Compliance — Validated

Server Model
HX220C-M5SX

CPU
Intel(R) Xeon(R) Platinum 8160 CPU @ 2.10GHz

Server Firmware Version
4.2(3g)

2 Server Software Compliance — Validated

OS Vendor
VMware ESXi

OS Version
7.0.3 3

Server Software Compliance — Incomplete

Missing Operating System information. Learn

OS Vendor
-

OS Version
-

3 Adapter Compliance — Not Listed

Incompatible component firmware and driver for one or more components. Learn more at Help Center

Add Filter — 4 items found — 10 per page — 1 of 1

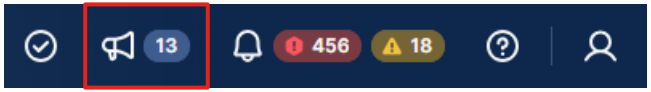
Model	Hardware Status	Software Status	Firmware Version	Driver Protocol	Driver Version
Cisco(R) LOM X550-T2	Validated	Validated	0x800016F7-1.826.0	ixgben	1.12.3.0-1OEM.700.1.0.15843807
Intel MLOM Quad Port 1Gb RJ45 NIC	Validated	Validated	0x80000E78-1.826.0	igbn	1.9.1.0-1OEM.700.1.0.15843807
Intel i350 Quad Port 1Gb Adapter	Validated	Validated	0x800011A4-1.826.0	igbn	1.9.1.0-1OEM.700.1.0.15843807
Cisco 12G Modular Raid Controller with 2GB cache (max 16 drives)	Validated	Incompatible Driver	51.19.0-4532	lsi_mr3	7.718.02.00-1vmw.703.0.20.19193900

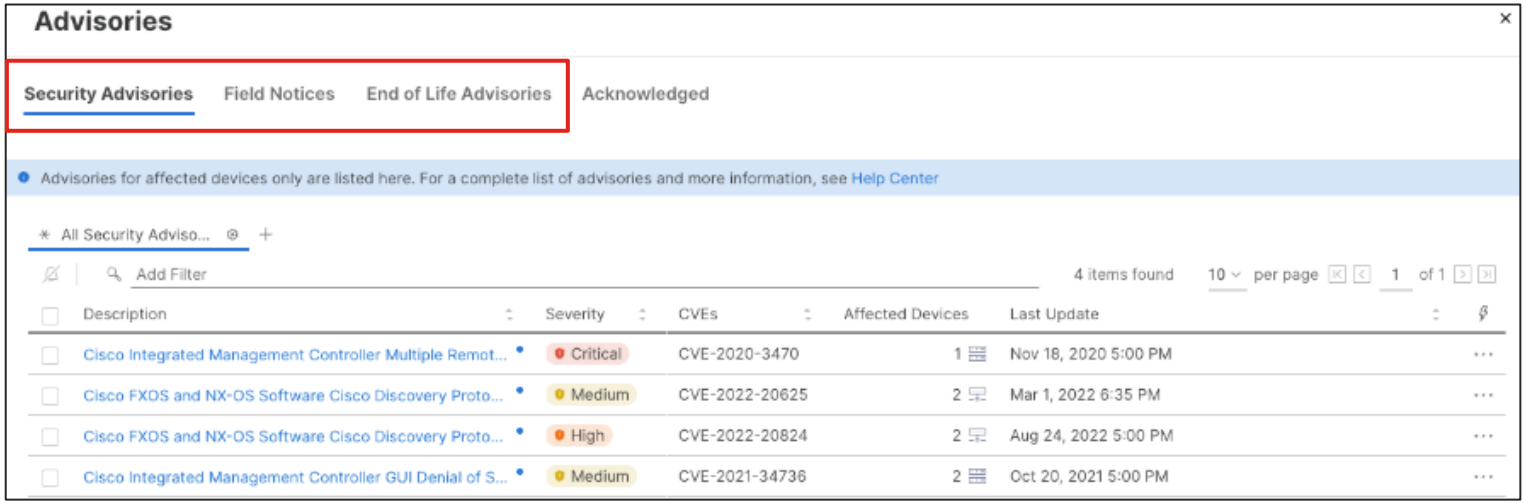
障害予防
・アドバイザリ

アドバイザリ

機能概要

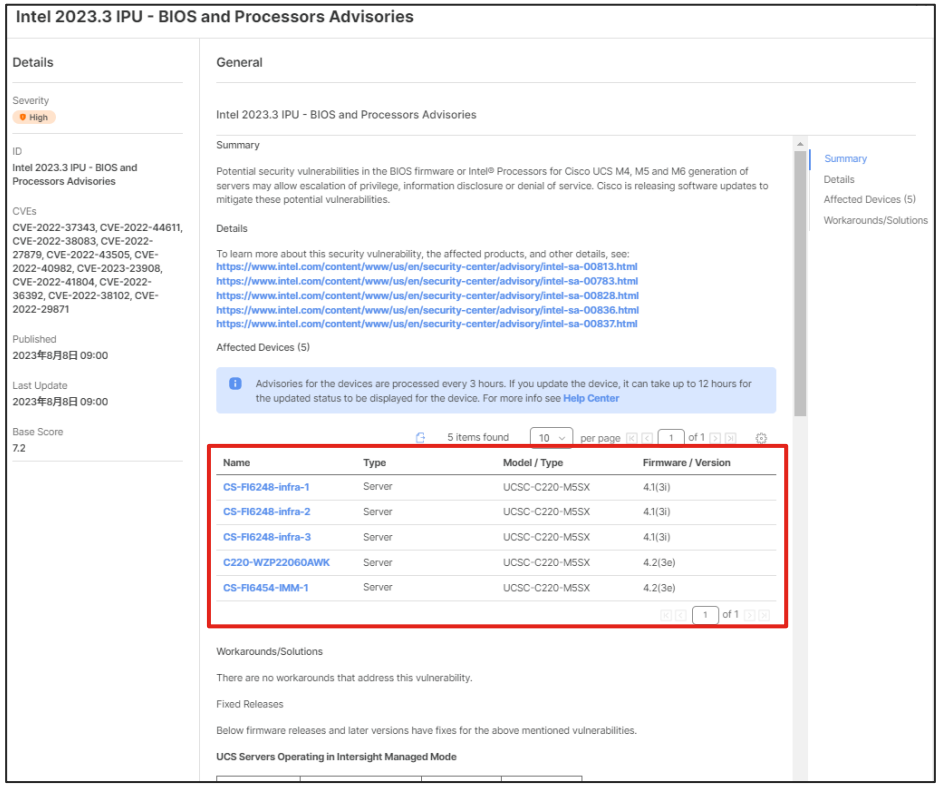
- アドバイザリ機能は３つの情報を提示
  セキュリティアドバイザリ、Field Notice、End of Life (EoL)
- 有償ライセンスが必要 (Intersight Essentials 以上)





アドバイザリ

脆弱性情報(CVE) の概要



Intel 2023.3 IPU - BIOS and Processors Advisories

Details

Severity
High

ID
Intel 2023.3 IPU - BIOS and Processors Advisories

CVEs
CVE-2022-37343, CVE-2022-44611, CVE-2022-38083, CVE-2022-27879, CVE-2022-43505, CVE-2022-40982, CVE-2023-23908, CVE-2022-41804, CVE-2022-36392, CVE-2022-38102, CVE-2022-29871

Published
2023年8月8日 09:00

Last Update
2023年8月8日 09:00

Base Score
7.2

General

Intel 2023.3 IPU - BIOS and Processors Advisories

Summary

Potential security vulnerabilities in the BIOS firmware or Intel® Processors for Cisco UCS M4, M5 and M6 generation of servers may allow escalation of privilege, information disclosure or denial of service. Cisco is releasing software updates to mitigate these potential vulnerabilities.

Details

To learn more about this security vulnerability, the affected products, and other details, see:
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00813.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00783.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00828.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00836.html
https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00837.html

Affected Devices (5)

Advisories for the devices are processed every 3 hours. If you update the device, it can take up to 12 hours for the updated status to be displayed for the device. For more info see Help Center

5 items found 10 per page 1 of 1

Name	Type	Model / Type	Firmware / Version
CS-FI6248-infra-1	Server	UCSC-C220-M5SX	4.1(3i)
CS-FI6248-infra-2	Server	UCSC-C220-M5SX	4.1(3i)
CS-FI6248-infra-3	Server	UCSC-C220-M5SX	4.1(3i)
C220-WZP22060AWK	Server	UCSC-C220-M5SX	4.2(3e)
CS-FI6454-IMM-1	Server	UCSC-C220-M5SX	4.2(3e)

1 of 1

Summary
Details
Affected Devices (5)
Workarounds/Solutions

Workarounds/Solutions

There are no workarounds that address this vulnerability.

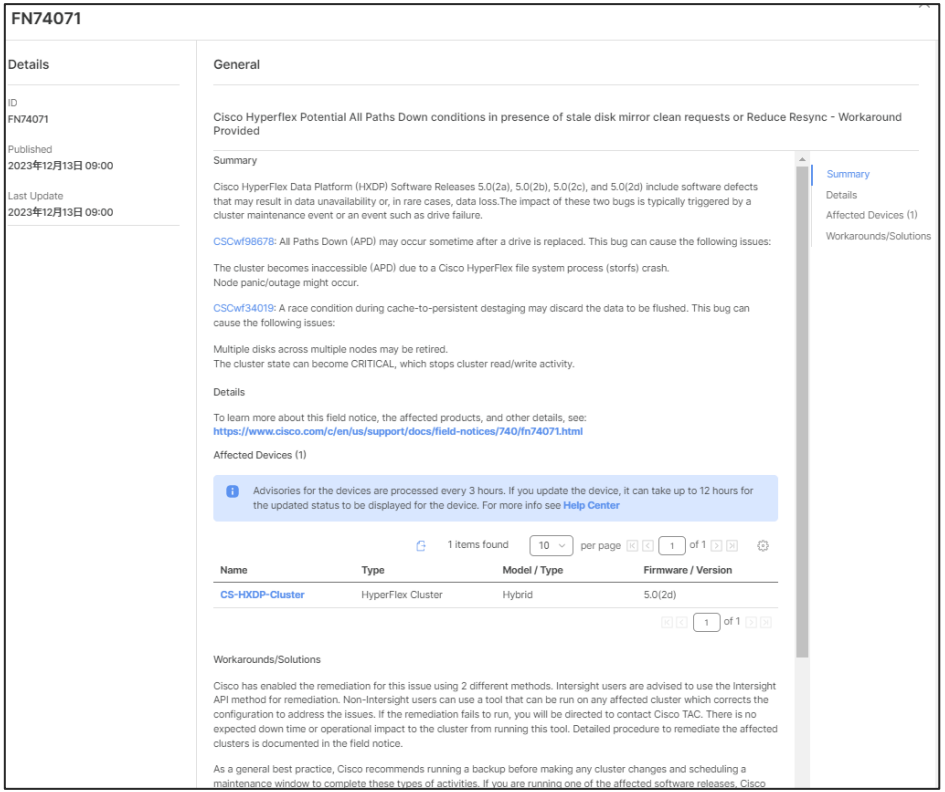
Fixed Releases

Below firmware releases and later versions have fixes for the above mentioned vulnerabilities.

UCS Servers Operating in Intersight Managed Mode

アドバイザリ

Field Notice 概要



FN74071

Details

ID
FN74071

Published
2023年12月13日 09:00

Last Update
2023年12月13日 09:00

General

Cisco Hyperflex Potential All Paths Down conditions in presence of stale disk mirror clean requests or Reduce Resync - Workaround Provided

Summary

Cisco HyperFlex Data Platform (HXDP) Software Releases 5.0(2a), 5.0(2b), 5.0(2c), and 5.0(2d) include software defects that may result in data unavailability or, in rare cases, data loss.The impact of these two bugs is typically triggered by a cluster maintenance event or an event such as drive failure.

CSCwf98678: All Paths Down (APD) may occur sometime after a drive is replaced. This bug can cause the following issues:

The cluster becomes inaccessible (APD) due to a Cisco HyperFlex file system process (storfs) crash.
Node panic/outage might occur.

CSCwf34019: A race condition during cache-to-persistent destaging may discard the data to be flushed. This bug can cause the following issues:

Multiple disks across multiple nodes may be retired.
The cluster state can become CRITICAL, which stops cluster read/write activity.

Details

To learn more about this field notice, the affected products, and other details, see:
https://www.cisco.com/c/en/us/support/docs/field-notices/740/fn74071.html

Affected Devices (1)

Advisories for the devices are processed every 3 hours. If you update the device, it can take up to 12 hours for the updated status to be displayed for the device. For more info see Help Center

1 items found 10 per page 1 of 1

Name	Type	Model / Type	Firmware / Version
CS-HXDP-Cluster	HyperFlex Cluster	Hybrid	5.0(2d)

1 of 1

Workarounds/Solutions

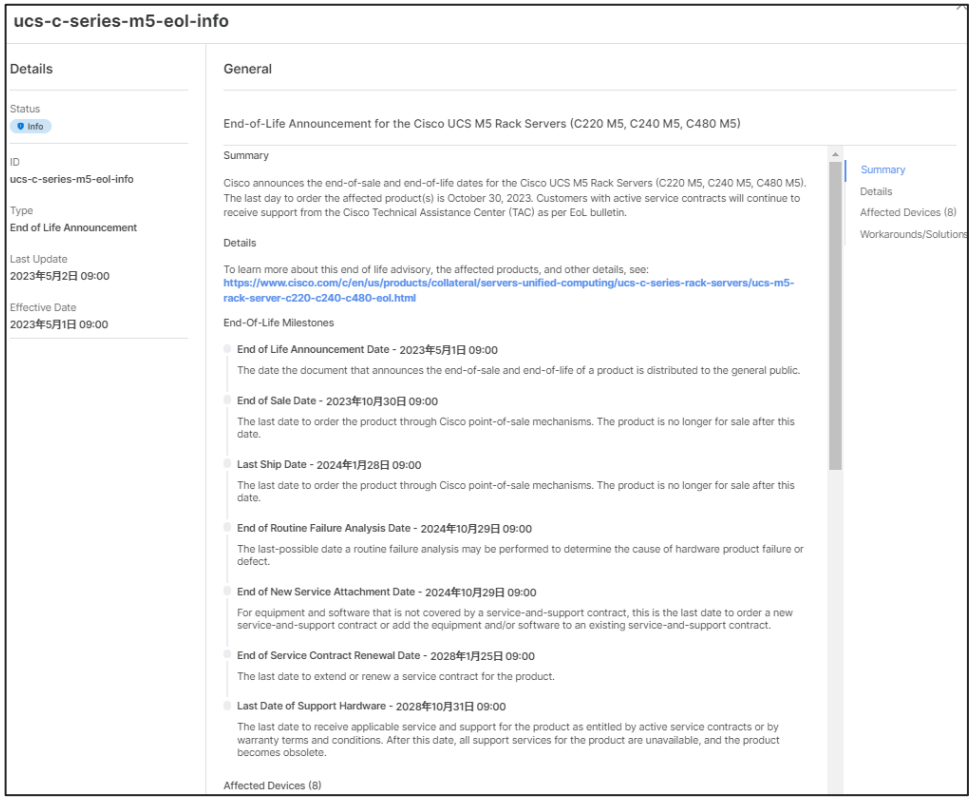
Cisco has enabled the remediation for this issue using 2 different methods. Intersight users are advised to use the Intersight API method for remediation. Non-Intersight users can use a tool that can be run on any affected cluster which corrects the configuration to address the issues. If the remediation fails to run, you will be directed to contact Cisco TAC. There is no expected down time or operational impact to the cluster from running this tool. Detailed procedure to remediate the affected clusters is documented in the field notice.

As a general best practice, Cisco recommends running a backup before making any cluster changes and scheduling a maintenance window to complete these types of activities. If you are running one of the affected software releases, Cisco

Summary
Details
Affected Devices (1)
Workarounds/Solutions

アドバイザリ

EOS/EOSL 概要



ucs-c-series-m5-eol-info

Details

Status
Info

ID
ucs-c-series-m5-eol-info

Type
End of Life Announcement

Last Update
2023年5月2日 09:00

Effective Date
2023年5月1日 09:00

General

End-of-Life Announcement for the Cisco UCS M5 Rack Servers (C220 M5, C240 M5, C480 M5)

Summary

Cisco announces the end-of-sale and end-of-life dates for the Cisco UCS M5 Rack Servers (C220 M5, C240 M5, C480 M5). The last day to order the affected product(s) is October 30, 2023. Customers with active service contracts will continue to receive support from the Cisco Technical Assistance Center (TAC) as per EoL bulletin.

Details

To learn more about this end of life advisory, the affected products, and other details, see:
https://www.cisco.com/c/en/us/products/collateral/servers-unified-computing/ucs-c-series-rack-servers/ucs-m5-rack-server-c220-c240-c480-eol.html

End-Of-Life Milestones

End of Life Announcement Date - 2023年5月1日 09:00
The date the document that announces the end-of-sale and end-of-life of a product is distributed to the general public.

End of Sale Date - 2023年10月30日 09:00
The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.

Last Ship Date - 2024年1月28日 09:00
The last date to order the product through Cisco point-of-sale mechanisms. The product is no longer for sale after this date.

End of Routine Failure Analysis Date - 2024年10月29日 09:00
The last-possible date a routine failure analysis may be performed to determine the cause of hardware product failure or defect.

End of New Service Attachment Date - 2024年10月29日 09:00
For equipment and software that is not covered by a service-and-support contract, this is the last date to order a new service-and-support contract or add the equipment and/or software to an existing service-and-support contract.

End of Service Contract Renewal Date - 2028年1月25日 09:00
The last date to extend or renew a service contract for the product.

Last Date of Support Hardware - 2028年10月31日 09:00
The last date to receive applicable service and support for the product as entitled by active service contracts or by warranty terms and conditions. After this date, all support services for the product are unavailable, and the product becomes obsolete.

Affected Devices (8)

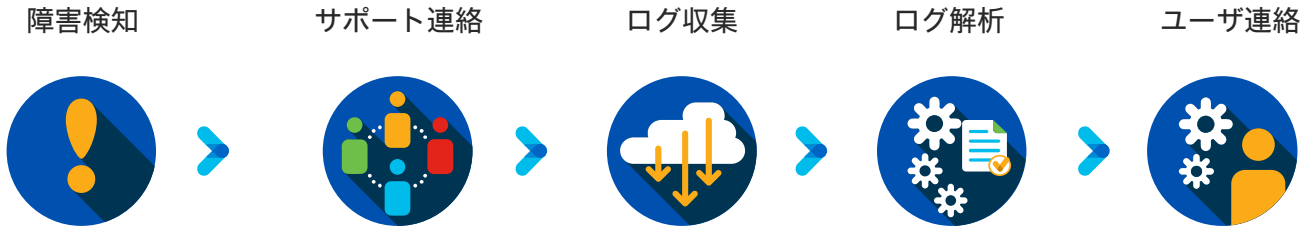
Summary
Details
Affected Devices (8)
Workarounds/Solutions

障害対応

・プロアクティブ RMA
・Connected TAC

サポート連携

- プロアクティブ RMA



- Connected TAC

プロアクティブ RMA

自動実行のポイント

プロアクティブ RMA が動作するには、下記の障害時に実行されます

- メモリ
  障害コード：F0185 (DIMM 動作不能)
- ディスクドライブ
  障害コード：F1732 / F0181 (DISK 動作不良、不能)
- ファン
  障害コード(ラックサーバ)　：F0484 / F0397 / F0794
  障害コード(ブレードサーバ)：F0484 / F0397

プロアクティブ RMA

送付されるメール

From: sherholm@cisco.com
To: XXXXXXXXXX
Cc: attach@cisco.com
Subject: [Action Required] SR XXXXXXXXX : Proactive RMA for HX Drive in HX Cluster: XXXXXXX, Triggered when disk in a HX cluster is in a hard black list and cannot be recovered. [Connected via Intersight]

Hello XXXXXX XXXXXX,

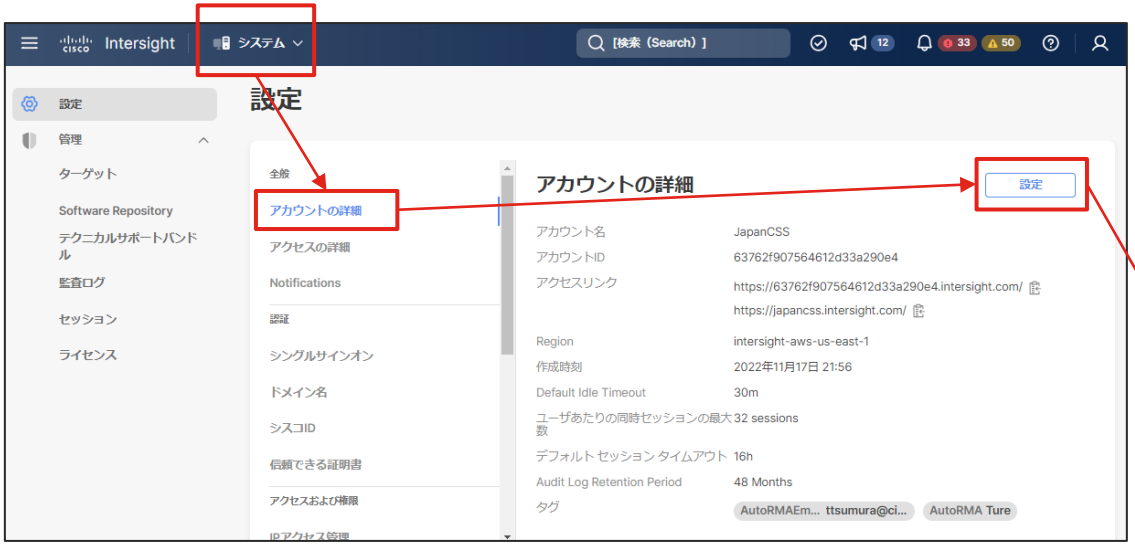
This email is to let you know that Cisco has received a fault message from your Cisco Hyperflex server connected by Cisco Intersight. The fault indicates a hard disk drive has failed and needs replacing. A TAC Case was created automatically (SR XXXXXXXXX) and draft RMA created to ship the replacement part. You need to open the RMA link to verify your shipping address and submit the RMA so the replacement part can be shipped out: https://ibpm.cisco.com/rma/home/?RMANumber= XXXXXXXXX
If entitled a Cisco Field Engineer can be requested on the above RMA form to complete the replacement.

Note: If you have difficulty loading the link above, please contact Logistics Support Center at one of the following manners:
https://www.cisco.com/c/en/us/buy/logistics-support-center.html

More information about the failed part and the server in which it's installed:
Hyperflex Cluster Name: XXXXXXX
Server Hostname: XXXXX
Server IP: XXXXXXXXX
Server Serial Number: XXXXXXXXX
Disk slot: 11
Fault Description: Triggered when disk in a HX cluster is in a hard black list and cannot be recovered.

プロアクティブ RMA

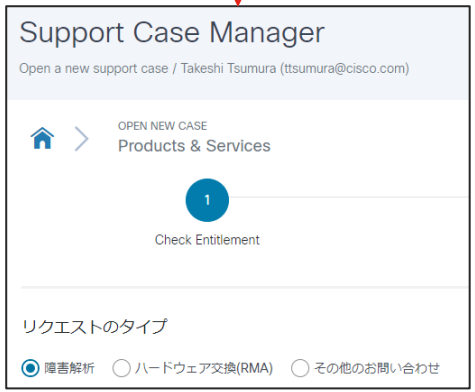
有効にする方法



sherholm@cisco.com から送付されるメールを受信するメールアドレスを入力下さい
例1：AutoRMA の送信先を test@cisco.local にする
AutoRMAEmail:test@cisco.local
例2：AutoRMA の送信先を test@cisco.local と group@cisco.local の複数にする
AutoRMAEmail:test@cisco.local,group@cisco.local

Connected TAC

シスコサポート連携



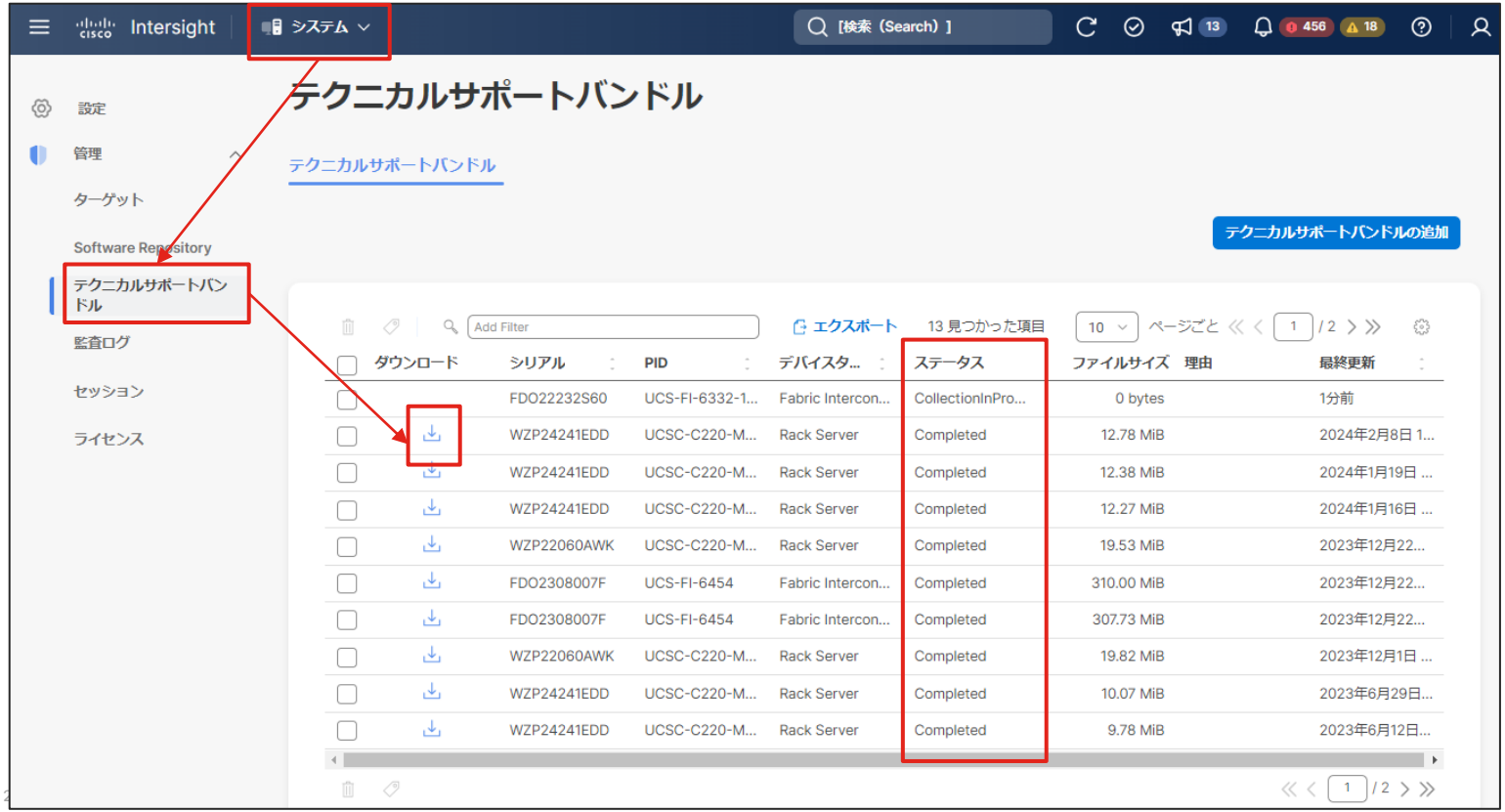
障害対応
・ログ取得機能 (マニュアル)

ログ取得機能 (マニュアル)

概要

ログ取得機能 (マニュアル)

概要



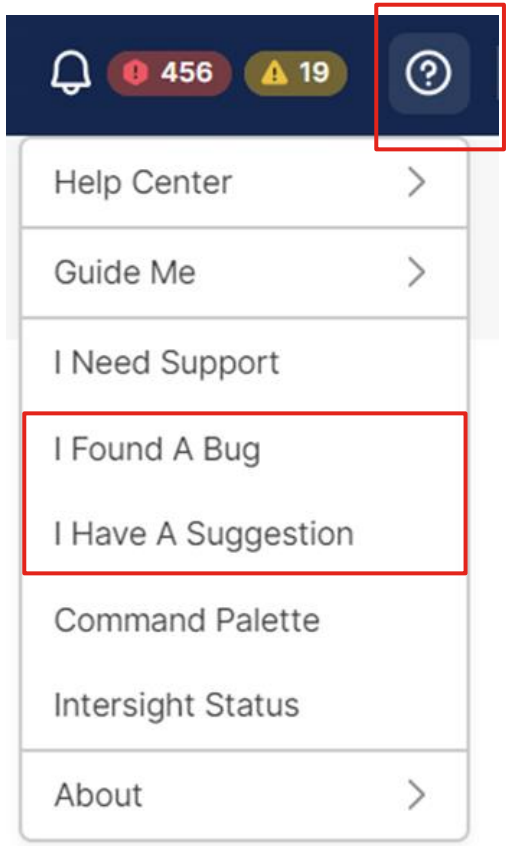
フィードバック機能

ユーザーフィードバック

概要

Intersight にはフィードバック機能があります。
右上のハテナマークをクリックしてください

- I Need Support
  シスコサポートに連絡する機能
  (サポートケースを開きます)
- I Found A Bug
  バグを報告する機能
- I Have A Suggestion
  機能改善や、新機能追加など
  皆様のご意見を投稿する機能



デモ#1:
Connected TAC

デモ#2:
アクセス制御管理
(RBAC)

覚えておくべき重要なポイント

01 Intersight は、アクセス制御が可能です。
定期的に権限の見直しを行ってください

02 障害予防には 2 つの機能があります
・ハードウェア互換性リスト
・アドバイザリ機能

03 障害対応の自動化にはプロアクティブ RMA です。
機能を有効にする事を忘れないでください

04 Connected TAC 機能により、障害対応にかかる
時間を短縮することができます

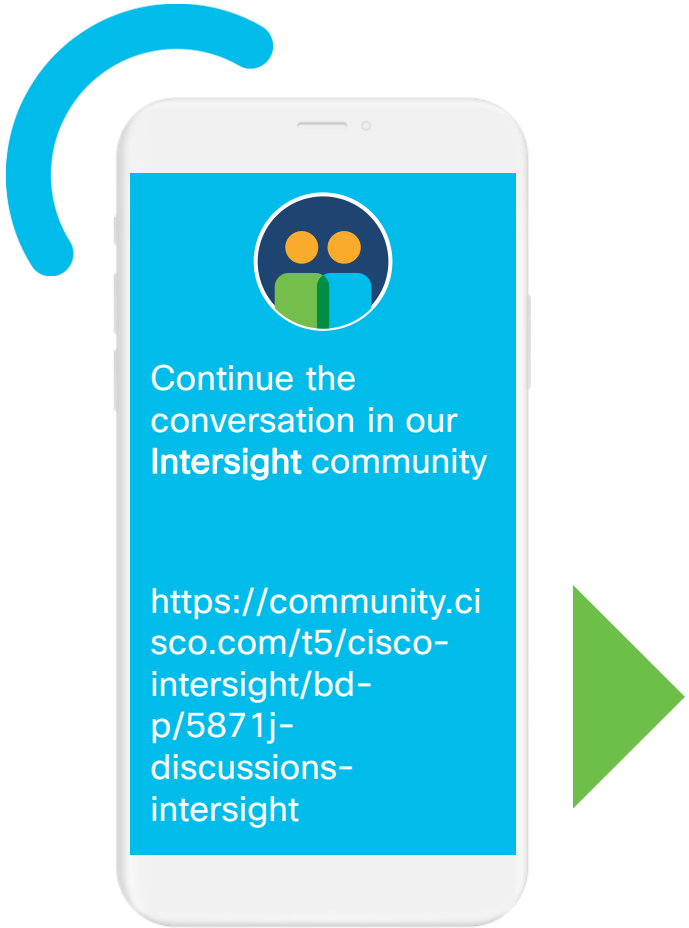
05 皆様のご意見をフィードバック下さい。
製品の改善 / 新機能追加を出来るだけ実施します

Resources

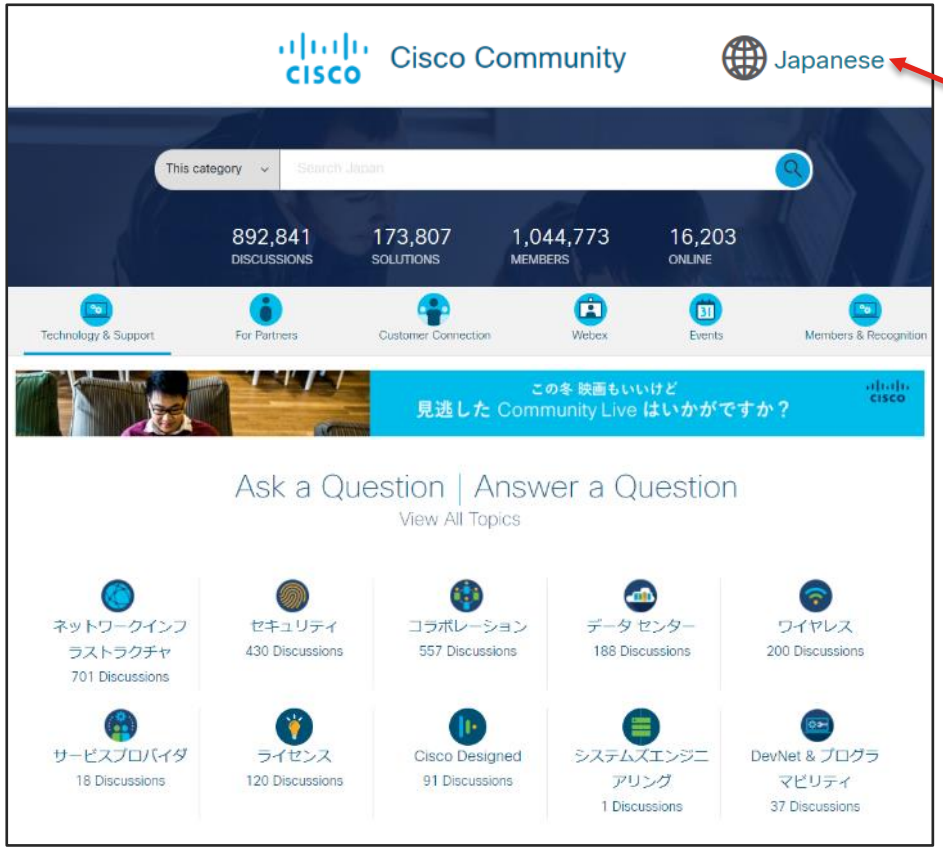
Ask the Experts リンク集: Cisco Hyperflex

https://community.cisco.com/t5/-/-/ta-p/4478213

※本日の ATXs 以外のリソースリンクも確認できます。



Cisco コミュニティサイトについて



日本語サイトがあります！
言語設定を変えるだけ。

・わからない事
・知りたい事
日本語でご質問下さい！

日本語コミュニティサイト
https://community.cisco.com/t5/japan/tkbc-p/japanese-community


Cisco
Customer Experience